LUND UNIVERSITY
School of Economics and Management

Department of Informatics

E-commerce and Information Security

Security controls in handling information and addressing security problems amid booming e-commerce.

Thesis 15 hp, course SYSK16 in Informatics

Authors: Nicole Engberg

Tove Larsson

Supervisor: Benjamin Weaver

E-commerce and Information Security: Security controls in handling information and addressing security problems amid booming e-commerce.

AUTHORS: Nicole Engberg, Tove Larsson

PUBLISHER: Department of Informatics, School of Economics and Management, Lund University

EXAMINATOR: Christina Keller, Professor

PRESENTED: May, 2021

DOCUMENT TYPE: Bachelor's Thesis

NUMBER OF PAGES: 103

KEYWORDS: Information Systems, Information Security, E-Commerce, Security Controls

SUMMARY: At a time when e-commerce is thriving and companies have to work with large quantities of data, there has been an increase of security risks. To stay current and afloat amidst and after the pandemic, the companies need to keep their consumers satisfied and safe. As threats to information systems become more advanced the companies need to stay on top of their game, and keep these risks from becoming incidents. They do this through the use of informal and formal controls within management, operational, and technical controls. To provide an overview of the methods and techniques that can be used to address security problems, specifically relating to the handling of personal data, a qualitative study was conducted. The aim of the study was to investigate what security controls companies have; which are most prevalent; and how they handle the data they store. The empirical data includes five interviews with employees at four different e-commerce companies, working in their respective security departments. The study established certain conclusions, mainly that the more common controls are ones that limit risk and access to systems and information; while less common controls are concerned with detail oriented solutions.

Contents

Tables

1 Introduction

In today's growing and ever-changing technological world, information has become increasingly valuable. Crume (2000) goes as far as to say that "information is the most valuable commodity on earth" (p.215). To keep up with the technological advancements, that information needs to be handled correctly, we need to understand security problems that can occur. E-commerce is a big industry that stores a considerable amount of sensitive information about a multitude of people and entities. E-commerce is growing, and in Sweden, there have been 40 percent more e-commerce purchases in 2020 than in 2019 (Postnord, Svensk Digital Handel & HUI Research, 2020). Furthermore, due to the Covid-19 pandemic, there has been a surge of online shopping from the consumer side. Since the pandemic has limited social contact and the number of visitors allowed in public spaces, people have turned to the socially safe method of shopping from the safety of their homes, namely online.

The aforementioned increase of e-commerce in turn issues a larger demand on information security in the cybersphere, as many customers require it to believe they are shopping safely. "A large body of literature suggests that e-commerce security is an important component of customer trust" (Fusilier & Penrod, 2009). This implies that e-commerce businesses need to take their information security practices seriously if they want to thrive in the information age. "The 'e-roads' must be safe enough to convince merchants that it's worth taking the risk" (Crume, 2000, p.201). A survey investigating security concerns of digital platforms showed that "44.5% of the respondents said they do not feel safe while ordering online amid COVID-19. Whereas, 54.5% of the respondents agreed they feel safe while using E-commerce in lockdown" (Galhotra & Dewan, 2020). Although the majority felt safe, 45% is still a large part of the general population, an untapped market that can be helped with a greater sense of security. Without information security, the e-commerce business would suffer from great mistrust issues. "If sensitive data is leaked, it may lead to significant business information loss or even affect the reputation of an enterprise" (Liu et al., 2020, n.p.). It is therefore crucial that security controls are constantly updated to refrain from security breaches that could compromise the integrity of people's information.

With the increase of e-commerce and the need for handling information in a correct and secure manner, companies need to be mindful of laws and regulations. It is especially important to be mindful today since there is such a large amount of information being handled. As protection for personal data, GDPR was implemented in 2018 and a new chapter of society began where personal data and information has to be more strictly prioritized by companies than it was before (European Commission, n.d.a). According to GDPR Chapter 6, Article 85, when a personal data breach has occurred, the controller has to inform the supervisory authority of the data breach within 72 hours, at the most (European Commission, n.d.b).

Consequently, proper management of security controls can be seen as an important factor in the management of confidential information. An understanding of which methods work results in more secure systems with a lessened necessity of expansive resources in the long run. The security controls frequently evaluate the security risks within the organization and decide what efforts are needed to address the risks (IBM Cloud Computing, 2019).

Implementing the correct procedures leads to relevant preventative measures being taken and resultantly having fewer aspects that need to be covered by detection and recovery controls (Stallings & Brown, 2018, p.513). By using security controls, companies can implement best practice solutions that are kept up to date with the relevant regulations, and then furthermore optimize this implementation by educating the companies' employees about security guidelines.

Having a better understanding of functional and reliable security controls is an invaluable asset considering that security controls or safeguards "can be used to improve security of IT systems and processes" (Stallings & Brown, 2018, p.511). Secure systems would entail a minimal amount of vulnerabilities, and operative counter strategies at the first sign of an incident. Every company has unique variables to consider for their system and therefore has different requirements for it to be an optimal one. Be that as it may, in e-commerce the companies have, for the most part, similar weaknesses and pitfalls in the case of information security. This study, of what practices the varying organizations implement, provides insight into what security controls or safeguards seem to be most commonly used. With this, the study would contribute to a current understanding of what methods and techniques can be utilized in security practices and processes, specifically in information security within e-commerce.

1.1 Scope

In relation to the rise of e-commerce, "the security of e-commerce transactions ... is a critical part of the ongoing success as well as growth of E-commerce" (Hussain, 2013, p.8). With the growing e-commerce, risks arise and parts of the e-commerce transactions can be compromised which can lead to leakage of private information (Hussain, 2013). A study by Sangeetha and Suchitra (2016) determines that e-commerce companies can implement an alternative third-party service as a security control to handle security risks and the personal data the company stores. Moreover, Ji (2018) expresses that the security issues, in the existing security systems of e-commerce companies, need to be detected and located. A study by Ji (2018), about the information security issues in e-commerce, presented solutions by using "information encryption technology", strengthening "protection management of websites", and establishing a "set of systematic, comprehensive and specialized laws of e-commerce" (p.3-4). To successfully secure e-commerce systems, Badotra and Sundas (2020) conducted an analysis of e-commerce systems and presented a literature survey containing common attacks. Studies have shown that existing e-commerce systems store and handle critical and sensitive data, which makes them vulnerable and easy targets for malicious attacks (Badotra & Sundas, 2020; Gehling & Stankard, 2005; Sangeetha & Suchitra, 2016). Defined measures to protect sensitive data exist, such as confidentiality, integrity, availability, authentication, and non-reputability (Badotra & Sundas, 2020). Beyond this, there are defined approaches to secure data, as presented in Badotra and Sundas' (2020) study, which are encryption, digital signatures, and digital certificates. Another study by Hussain (2013) also stressed the importance of using these approaches to prevent security threats. For e-commerce companies to successfully handle security risks, security controls have been implemented, such as authentication, authorization, auditing, confidentiality, integrity, availability, and encryption (Gehling & Stankard, 2005; Sangeetha & Suchitra, 2016). Defining where vulnerabilities lie in the systems can define controls that can counter malicious attacks on parts of the systems, such as sensitive personal information that e-commerce companies store and handle (Gehling & Stankard, 2005). Furthermore, Kuruwitaarachchi et al. (2019) present frameworks

consisting of combinations of security controls that can be used to secure information systems. They claim that the main parts of information security concern transactional security, system security, privacy, and cybercrime. The frameworks they present contain an array of controls that aim to protect information systems concerning the aforementioned four parts.

Existing research has established that security threats exist, and defines some specific ones and their corresponding impact in regards to e-commerce companies. The existing research also determines what security controls and measures exist and how they can be used. This thesis study complements existing frameworks with what is most commonly used and classifies the security controls, providing an opportunity for efficient combinations of controls. Beyond this, there is a significance in theoretical research to evaluate if the common ones, most of which are presented in frameworks from previous research such as Kuruwitaarachchi et al. (2019), are actually implemented and valued. This study also defines where there are gaps in the usability and range of certain controls that are less commonly used, contributing to theoretical research in the need for development.

1.2 Objective

To facilitate customer trust, e-commerce companies have to ascertain that they work with reliable and secure methods. With the increase of e-commerce business, there is a corresponding increase in the data that needs protecting from malicious actors. Thus, a strong security system, and suitable methods to address risk and incidents, are paramount in information security.

Using existing research and literature along with a tailored interview study of e-commerce, the objective is to provide an overview of methods and techniques that can be used to address security problems, specifically relating to the handling of personal data. Thus adding to the research on security controls by presenting a current-day analysis of e-commerce businesses, presenting common techniques in varying trades. These aspects will be discussed in accordance with the data collected from interviews with people in the business of e-commerce.

1.3 Research Question

The aim of this thesis is to explore security controls in e-commerce security systems. Following the objectives, the research question, therefore, reads: In the face of the current e-commerce boom, what security controls do e-commerce companies most commonly use to handle information and address security risks?

1.4 Delimitations

For the clarity and feasibility of this study, some limitations have been defined. The primary limitation is that this paper focuses on companies in the e-commerce industry. This implies that the companies need to provide online sales of goods or services to consumers on an electronic platform. Additionally, the companies are business-to-consumer (B2C), considering that the thesis aims to investigate the handling of personal data. The geographical scope has

been limited to Europe, specifically companies in the European Union (EU), meaning the companies interviewed have offices that follow EU rules and regulations. This was defined for the sake of minimizing the risk of overgeneralizing the results, as well as being able to analyze GDPR in relation to security.

2 Literature review

To get a better understanding of how security controls can address security problems the authors have studied literature and related articles within the field. The literature and the articles presented are to give a deeper understanding of the topics, and pave the way for future research that can be conducted within the area. The different chapters chosen from Stallings and Brown (2018) are to give a foundation for how security problems will be addressed through managerial, operational, and technical security controls later in the discussion. The other books give different perspectives on security issues that can be present in information handling, along with proposed preventive measures and solutions for such cases. The articles delve into specific topics and aspects that give insight into why security controls are relevant and how they function.

2.1 Management Controls

Management controls focus on matters that the management handles and refers to “security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization’s mission” (Stallings & Brown, 2018, p.513). Johansson et al. (2021) presented in their journal, that by understanding how, for what, and for whom the managerial controls are used, an organization can learn how to apply these controls and use them as support.

2.1.1 CIA Triad

One approach to ensuring security is by adhering to the CIA triad, which is 'confidentiality, integrity and accessibility.' These three aspects are key in the creation of security policies and generally secure systems. The CIA triad also points to the difficulties that come with big data, which is exactly what e-commerce is concerned with. This theory can be used to show the value of security in this field, as well as where there are shortcomings (Stallings & Brown, 2018). Confidentiality means that only authorized users are allowed to access the information, and is used to control technical and physical access to the system (Cabric, 2015). Integrity is used to assure that the information “remains intact and unaltered” as it can be subject to frauds and be compromised (Cabric, 2015, p.185-186). Accessibility or availability entail that the information should be accessible when needed. According to Cabric (2015, p.185-186), there should not be anything that “block[s] legitimate and timely access to information.”

2.1.2 Four-eyes principle

The four-eyes principle entails that two individuals need to approve an action before taking it, thereby verifying the legitimacy of it before implementing it. An alternative name for the principle is the two-man rule or the two-person rule (CROS-European Commission, 2019). Bodenschatz and Irlenbusch (2019) present in their study that the four-eyes principle “reduces

corruption when [an] interaction is repeated" (p.194), which can help benefit companies when working with their internal information. Companies can use the principle as a control mechanism to achieve top-level security, and is commonly seen as the additional control at the top of the system to achieve a higher level of security (Osaci et al. 2018).

2.1.3 GDPR

GDPR (The General Data Protection Regulation) is applicable throughout Europe and its purpose is to protect individuals' personal data in a standardized and equal manner, as well as protect the fundamental rights and the freedoms of individuals (IMY, 2021). The reason for applying this regulation is its relevance to the subject of information security, and the manner in which companies adapt to the regulation in their work with it. Therefore it has also been included in the study, to get a better picture of how companies work with it. According to 39§ GDPR "the personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed." In accordance with the GDPR companies have had to adapt what information is gathered, how much information is needed, and the purpose for gathering the information. According to GDPR Chapter 2, Article 5(1) the category and quantity of personal data a company can gather to use depends on the reason for gathering the data and the predetermined use of the data. GDPR Chapter 2, Article 5(1) also states that there are fundamental rules a company has to follow. These are that (1) the personal data should be processed "lawfully, fairly and in a transparent manner;" (2) there has to be "purpose limitation" with a specific reason for processing the data, and the company has to be transparent to the individuals about this; (3) the company can only gather what is necessary to achieve the wanted result, so called "data minimisation;" (4) the company has to make sure the personal data that is gathered is up-to date and has "accuracy;" (5) the company cannot store the personal data longer than what is needed, and has to make sure there is "storage limitation;" (6) the company must also make sure the data is protected and handled with "integrity and confidentiality."

2.1.4 Informal Controls

Informal controls are needed to help form the security structure within the organization by helping with training and awareness programs in order to align employee behavior in information security matters (Sindhuja & Kunnathur, 2015). Informal controls treat the human-related errors, and to prevent these from occurring the open communication between managerial and security personnel is needed to ensure information security (Sindhuja & Kunnathur, 2015). An open line of communication can help identify possible vulnerabilities and mitigate destructive discrepancies that might arise between employees (Sindhuja & Kunnathur, 2015).

2.1.5 Risk Management

Risk management consists of making calculations and assessments of known and unknown risks, as well as taking appropriate risk control measures in relation to the risks. The process of risk management is to make sure that the risks are within reach of the enterprise, at a reasonable price (Li & Li, 2020). Risk management is used in relation to IT systems as a "process that helps in balancing operational necessities and economic costs associated with adequately handling information" (Dhillon, 2007, p.157). Berger, Shashidhar and Varol (2020) presented in their study that "how a business handles risks is crucial to its continued

success" (p.4), and through risk management the organization is efficiently handling its risks. Risk assessment is an essential factor to risk management for successfully implementing ITSM (Information Technology Service Management), and also for the organization's survival (Berger, Shashidhar & Varol, 2020).

A response approach to dealing with risks is for companies to use a CIRT. A CIRT (computer incident response team) or a CSIRT (computer security incident response team) is "set up for the purpose of assisting in responding to computer security-related incidents that involve sites within a defined constituency" (Stallings & Brown, 2018, p.563). A CIRT has the responsibility to respond when a security breach has occured, when viruses have been detected, or when other potentially disastrous incidents in the organization. The group consists of technical specialists qualified to deal with the specific threats and experts that can help guide the companies managers in a suitable manner in the wake of such incidents (Gartner, n.d.). Often in risk management the aim is to determine whether to accept, avoid, mitigate, or share a risk (Stallings & Brown, 2018). Depending on the impact a risk threatens to create, the CIRT can see which is the most plausible solution with minimal damage and low cost.

Another approach to help with risk management is to use CVE lists, the common vulnerabilities and exposures catalogue. CVE "is one of the largest publicly available source[s] of software and hardware vulnerability data and reports" (Blinowski & Piotrowski, 2020, p.5). Blinowski and Piotrowski (2020) presented that the CVE list can be used by companies to list the information security risks and vulnerabilities they face, where the purpose is to give them "common names for publicly known problems" (p.5). The reason for doing this list is to make it easier to share data across different vulnerability means. According to Blinowski and Piotrowski (2020), the CVE list has become a standard for sharing information about the risks and vulnerabilities for many companies.

2.1.6 Standards

2.1.6.1 NIST

NIST (National Institute of Standards and Technology) (2020) helps support technologies in all forms, from small companies with simpler technologies to big companies with complex technologies. NIST's portfolio includes standards, measurements, and legal metrologies that can help with traceability and quality assurance (NIST, 2020). In 2018 NIST published an updated version of their "Framework for Improving Critical Infrastructure Cybersecurity" which was originally published in 2014 (Barrett, 2018). This framework is a guideline that NIST put forward to complement their standards with a specific focus on cybersecurity practices (Shen, 2014). The framework allows companies to assess their cybersecurity systems and to identify potential vulnerabilities (Shen, 2014).

2.1.6.2 PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) offers security practices that can be used to protect the company's information assets (Yulianto, Lim and Soewito, 2016). It contains 12 high-level requirements to be met as well as information security best practices that must be adopted and enforced to "any merchants and payment card processors" (Yulianto, Lim and Soewito, 2016, p.65). The current PCI DSS implementation can be used by companies to effectively achieve the 12 requirements (Yulianto, Lim and Soewito, 2016). The companies have to define the internal and external weaknesses in the early stages of implementing PCI DSS to avoid possible risks (Yulianto, Lim and Soewito, 2016).

2.1.6.3 ISO

ISO (International Organization for Standardization) is an independent and international organization with more than 160 national standardization authorities as members (SIS, n.d.). ISO has over 22 000 standards published globally and one of the most famous standards is ISO 9001, which is for quality (SIS, n.d.). The standards are developed and studied regularly to assure the quality of the standardization process (SIS, n.d.). According to Stallings and Brown (2018), ISO "promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services" (p.49). ISO standards can help and benefit enterprises; raise customer confidence by presenting the products as safe and reliable; make sure regulations are met; reduce costs within the organization; and attain access to the market all over the world (ISO, n.d.).

The ISO 27000-series is focused on helping organizations achieve good information security, and the standards are flexible and suitable for all sizes of companies (Eriksson, 2016). In the ISO 27000-series there are two documents that can be useful to companies: the ISO 27001 and ISO 27002 (Eriksson, 2016). The ISO 27001 focuses on policies and processes within an organization (Eriksson, 2016). It also focuses on how to create a safe environment for the information the organization wants to protect and help the company improve its risk management (Eriksson, 2016). ISO 27002 focuses instead on recommendations (Eriksson, 2016). The documents help list the companies' wanted goals and the controls needed to achieve these goals, which can vary depending on the organization's needs and resources (Eriksson, 2016).

2.1.7 ITIL

ITIL (Information Technology Infrastructure Library) is a set of best practices to help manage security (Berger, Shashidhar & Varol, 2020). The ITIL is a part of the ITSM (Information Technology Service Management), a service management philosophy many organizations use (Berger, Shashidhar & Varol, 2020). Security incidents can affect the sensitivity of information, which can complicate the management of the security, but it can still be managed in an appropriate and efficient way (Berger, Shashidhar & Varol, 2020). ITIL 4 is the newest update since 2019 which includes a Service Value System (SVS) (Berger, Shashidhar & Varol, 2020). SVS references all the organization's activities and components that create value by working together, which is essential when you wish to generate value in service offerings as well as for security incidents (Berger, Shashidhar & Varol, 2020). Service Value Chain is the core part of SVS and is a flexible process of creating, delivering, as well as improving services that can easily adapt to ITSM needs such as security management (Berger, Shashidhar & Varol, 2020).

2.2 Operational Controls

Operational controls focus on the processes and operations implemented by people, instead of systems. The controls "address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies," which can help improve the security of a system, or several systems, within the organizations (Stallings & Brown, 2018, p.513).

2.2.1 Access Controls

Access controls are used to limit the admittance to information systems to authorized users or processes initiated by authorized users, as well as limit access to functions that only authorized users are allowed to perform (Stallings & Brown, 2018). The mechanisms used to implement these limitations can be applications, operating systems, firewalls, routers, files, and databases (Stallings & Brown, 2018). The system checks a user that seeks access to the system, and then it can determine if the user is allowed to access the system (Stallings & Brown, 2018). A security administrator manages the authorization database, which consists of what type of access to which resource the user is allowed to get (Stallings & Brown, 2018). Access controls can use this database to grant or deny access. The user access to the system resources is recorded by an auditing function (Stallings & Brown, 2018). A company can use an Access Control Policy (ACP) to determine the different levels of confidentiality of data; what processes there are for managing the data and resources; as well as the classifications of security requirements for these resources (Saracino, 2020).

Another way to determine access control levels is through least privilege (Stallings & Brown, 2018). Least privilege is a principle that every user, or every process of the system, is only given the least set of privileges essential to perform (Stallings & Brown, 2018). To identify and outline the roles of users and processes, the organization's system security policy can be used, thereby only permitting authorized roles access to perform certain functions (Stallings & Brown, 2018). By only permitting people with approved access to a resource, the system can manage and control that the resources are limited to only necessary users and processes (Stallings & Brown, 2018). The least privilege principle can also temporarily give access to system programs or administrators when it is deemed necessary, but when usual tasks resume the access should be withdrawn (Stallings & Brown, 2018).

Furthermore, separation of duties is used by companies so that people working with specific tasks are not the same as the people who check the task (Stallings & Brown, 2018). Separation of duties is needed to make sure that the people working with finding inappropriate use are not the same as the ones that can perform the inappropriate use (Stallings & Brown, 2018). Therefore all the security functions and auditing should not be performed by one person, since it could lead them violating security policies that no other person can see or be informed about (Stallings & Brown, 2018).

2.2.2 Authentication and Authorization

Authorization, according to Stallings and Brown (2018), is “the granting of a right or permission to a system entity to access a system resource” (p.130), and that authentication is the “verification that the credentials of a user or other system entity are valid” (p.129). When a user uses the system, an authentication process begins (Stallings & Brown, 2018). The system first authenticates the user and eventually approves or denies authorization to the user (Stallings & Brown, 2018). To be allowed access to the wanted information in the system, the user has to show credentials such as a token or possession that can verify the user is authorized to access the information (Stallings & Brown, 2018). Authentication and authorization are essential to an organization's infrastructure in being able to protect the sensitive data and information from getting infiltrated by attackers (Anna et al. 2020). When a system detects an attack it sends out security warnings and blocks the attacker from entering the system, thereby ensuring the system cannot be entered by unauthorized users (Anna et al. 2020). Anna et al. (2020) presents different methods for different degrees of confidentiality.

They explain that depending on what the damage can be to the organization there are different methods for protecting the information, such as multiple passwords, one-time passwords, and additional verification when trying to access different areas within the organization (Anna et al. 2020).

2.2.3 Formal Controls

Formal controls are often associated as a form of policy or document that dictates how technical controls help manage information security within an organization (Sindhuja & Kunnathur, 2015). Formal controls can be seen as the foundation for the shaping and implementation of technical controls (Sindhuja & Kunnathur, 2015). The formal controls can help an organization when regulating how responsibilities should be allocated, by establishing the consequence of misinterpretation of data and misapplication of rules within the organization (Sindhuja & Kunnathur, 2015). The use of formal controls in the organization is required to define the guidelines for internal transfer of information (Sindhuja & Kunnathur, 2015). This suggests implementation of standardization of the organization's security policies (Sindhuja & Kunnathur, 2015). This will provide transparency and visibility of the activities in the organization (Sindhuja & Kunnathur, 2015). Formal controls are, however, not enough to block out miscreants that want to access sensitive information (Sindhuja & Kunnathur, 2015).

An instance of a formal control includes logging, which is “the act of collecting event records into logs. Examples of logging include storing log entries into a text log file, or storing audit record data in binary files or databases” (Chuvakin et al. 2013, p.31). There are different types of logging, and one of those is security logging, which detects and responds to attacks, malware infections, data theft, and other security issues that can occur in a system (Chuvakin et al. 2013). Security logging can log when users authenticate to log in to a system, as well as other access processes which are logged and analyzed (Chuvakin et al. 2013).

2.2.4 Testing

According to Watkins and Mills (2011, p.11), “testing is any activity aimed at evaluating an attribute or capability of a program or system and determining that it meets its required results.” They also describe it as being “the process of executing a program or system with the intent of finding defects” (p.11). They say testing can be used by companies to make sure a system doesn't have any defects; does what it is supposed to do; conforms to the expectations put on it; and performs satisfactorily. There are many testing methods, each with a different purpose, and some common ones include: developer testing, user acceptance testing, system testing, and penetration testing.

Developer testing is when developers test their code while they write it. This testing method has been identified as essential to improve software reliability since the defect can be located early in the software development life cycle (Xie et al. 2010). This creates trust in the program unit during testing, and it decreases the costs usually spent on fixing faults by catching them early in the process of development (Xie et al. 2010). According to Xie et al. (2010), developers can use existing testing frameworks to develop test inputs automatically. Thereafter they can use their developer skills to understand the tools, and the difficulties they can come to face, and thus help guide through the difficulties and prepare. Xie et al. (2010, p.175) asserts that “developer-testing activities typically include generating test inputs, creating expected outputs, running test inputs, and verifying actual outputs”.

According to Ganesh et al. (2014), user acceptance testing (UAT) is a testing method that the user performs when the code has been delivered to the user. They say that in preparation for the handover to the user, the user acceptance plan should be set up and the code ready to be tested to perform in accordance with the user acceptance plan. Deviations that occur are logged and investigated thereafter, depending on the fault (Ganesh et al. 2014). For example, an error in the code or a need to adapt to changes made in business requirements (Ganesh et al., 2014).

Another testing method is system testing, which can be used to investigate "firmware, OSs, and system services for implementation flaws, insecure system settings, and other known vulnerabilities" (Chen et al. 2018, pp.82-83). System testers generally test a system without having prior knowledge of the system, therefore a common method they apply is the black-box method (Chen et al. 2018). According to Watkins, J. and Mills, S., Black box testing is designed "without the knowledge of how the system under test is constructed" (2011, p. 18-19), the testing method is usually applied later in the development and the tester does not have prior knowledge about the software used to create the system.

Yet another common testing method is penetration testing, which applies offensive attack techniques to find vulnerabilities within an organization (Chen et al. 2018). The testing method can generally be said to complement the defensive security methods (Chen et al. 2018). By improving penetration testing coverage, malicious attacks can be avoided and not given the chance to attack since it only needs one exploit to be successful (Chen et al. 2018). There are three specialized penetration testing methods that can be used, which are interface testing, transportation testing, and system testing.

2.2.5 Auditing

An information systems audit is a method of evaluating the effectiveness of an information system's controls (Zwass, 2016). Auditing is used by companies because they should "provide assurance that systems are adequately controlled, secure, and functioning as intended" (Petterson, 2005, p.41). Petterson states that a good report should contain the following elements: the current condition; the criterion of what the audit compares the condition to; the cause of the condition; the effect of the condition on the organization; and a recommendation of what to do to resolve the realised situation. However, he points out that a main challenge for IT auditing is that the technology is quickly changing, meaning new controls need to be set in place to achieve best practice.

According to Herath and Herath (2014, n.p.), "information security and systems audits for assessing the effectiveness of IT controls are important for proving compliance". They state that an audit is very valuable to a company, if they have the resources, as it costs both time and money. CSI's (2011) Computer Crime and Security Survey showed that audits are essentially the top technique used to evaluate effectiveness of information security. The survey was conducted annually over 15 years, 2011 being the last, and they consistently showed that auditing was a top practice, but this final year the percentage of audits conducted by companies had decreased slightly.

2.3 Technical Controls

Technological controls are measures that help secure critical and sensitive data, information, and IT systems functions within an organization. The technical controls "involve the correct use of hardware and software security capabilities in systems" (Stallings & Brown, 2018, p.513).

2.3.1 Zero-Trust

"Trust is the bidirectional belief established between two entities that the other entity is what it claims to be and that it will behave in expected ways during the duration of the interaction" (Ahmed et al. 2020, p.4). This trust is what enables quick access to networks from known devices, but skips a thorough vetting that checks if the device is actually harmless. The zero-trust concept was developed to protect the integrity of a network from malicious activity. Protecting from malicious activity is the basis for many security measures, but what sets zero-trust aside from the masses is that it grounds itself on that "all users, devices and applications outside and inside the perimeter [of a network] will be treated in the same way" (Ahmed et al. 2020, p.2). This entails that the initial reaction of a network is to not trust an entity that is trying to gain access, whether they are in a known area or not. Ahmed et al. (2020) explain that an otherwise common method to provide network security is by having protective measures at a perimeter level. This separates trusted networks and untrusted ones by exhibiting trust to the networks within the perimeter but allocating zero trust to those outside. The problem with this is that it gives unchecked access to the entities already within the network. If there happens to be a malevolent entity within the perimeter then there would be much less protection within the network. Zero trust is therefore a strategy that makes this problem redundant. Choosing not to trust any entity until it is proven trustworthy is a defensive technique that creates a more secure environment. This is a valuable strategy in protecting a network as it eradicates the idea of a trusted versus untrusted network, making it a non-issue.

2.3.2 SaaS

SaaS, or software-as-a-service, is when software is rented rather than purchased.

> The NIST Reference Architecture for Cloud Computing clarifies that the SaaS provider is responsible for deploying, configuring, maintaining, and updating the operation of the software applications on a cloud infrastructure. (Simmon, 2018, pp.9-10).

With this comes responsibility, on the part of the provider, as they need to assure their consumers that their systems are secure. Feher and Sandor (2019) claim that a SaaS solution has the potential to be secure through the use of Cloud-IPS, Cloud Firewall, and Cloud SIEM solutions. Liu et al. (2018) also mention that there is a wide variety of security solutions based on SaaS, on top of traditional network security technology. However, they also bring up that there are some points lacking in SaaS security, such as easily manipulated access controls considering that several users log in to the systems with the same credentials. SaaS serves a good purpose for companies who need short-term solutions, as it enables easy management of business activities (Liu et al. 2018).

2.3.3 Cryptography

Cryptography is a way to turn legible text into indiscernible information, and vice versa (Kurd & Besli, 2020). The two main types of encryption are symmetric and asymmetric (public-key) encryption (Stallings & Brown, 2018). With symmetric encryption one can complete specific safeguards, such as message authentication and creating secure hash functions (Stallings & Brown, 2018). Meanwhile, asymmetric encryption is used predominantly for digital signatures and key management (Stallings & Brown, 2018). "Protecting digital data and maintaining information security have been achieved through the use of cryptographic algorithms" (Kurd & Besli, 2020, p.1). For instance, the MD2 hash makes a unique string of characters of 128 bits based on a text, and then, with a checksum, one can ensure that the text has not been corrupted (Gauravaram et al. 2010; Meylan et al. 2021). Hajny (2020) also goes into how "security and privacy in communication networks is usually provided by cryptographic means" (p.87). Confidentiality, integrity, and availability are the three points to achieve, and to do this there exists algorithms, for example Advanced Encryption Standard, Secure Hash Function, and Digital Signature Algorithm (Hajny, 2020). Hajny (2020, p.87) states that the "protection of user data is still very low" in environments such as industrial networks, IoT networks, or sensor networks. This statement supports that it is necessary to look into the protection of data and what security controls companies actually have in place when it comes to security.

2.3.4 Backups

A data backup is a copy of defined data stored in another place. Having backups is a common practice that people use to avoid losing all of their information in the case of a security attack (Crossler, 2010). Knowing how valuable data is, paired with the negative impact of losing this valuable data, are some of the reasons why backups are often implemented (Crossler, 2010). In the grand scale that companies store data, it is extra important to have backups and secure the information that is quite often sensitive. There are several ways of backing up data via physical solutions and virtual solutions alike, including but not limited to data centers, servers, decentralized solutions (Mathew & Mai, 2018), and node backups (Zhiyong et al., 2018). Although, Mathew and Mai (2018) mention that there are still some weaknesses in these solutions as they do not uniformly protect against all possible external threats. There is room for improvement in security effectiveness but that is why there are backups to begin with.

Two common ways of storing data, to begin with, are cloud storage and local (on-premise) storage (Adshead, 2021). "To prevent the leakage of sensitive information and to ensure data security, a secure storage method is needed to store real-time sensitive data, including equipment locations, safely and without affecting data availability" (Liu et al. 2020, n.p.). Liu et al. (2020) go on to say that the choice of cloud services versus local are dependent on the type of data stored and how you want to access and use it. They say that cloud computing has high storage capacity and computing power, while local storage provides low-cost and high-efficiency data protection. With the different methods of storing data also comes different ways of securing the data, and in turn possibly different levels of protection.

2.4 Summary

The different concepts studied in the literature review were chosen due to their relevance with the use of security controls in businesses. As a summary of the literature review chapter, a table with an overview of the themes and concepts investigated is presented below. The overview will provide clarity over the relationship between the literature and the interview questions formed (Appendix A), hopefully ledning an understanding of the purpose of the research paper's study.

Table 1: Literature Overview

Perspective	Category	Factors	Literature	Example Questions
Management Controls	CIA Triad	Confidentiality, integrity and accessibility	Stallings & Brown (2018) Cabric (2015)	In handling people's private information, do you feel there are more security concerns in comparison to other confidential data in the company? Have you experienced that data or information that you work with has not been available?
	Informal Controls Four-eyes principle	Legitimacy Human-related errors Employee Behavior	CROS-European Commission (2019) Bodenschatz & Irlenbusch (2019) Osaci et al. (2018) Sindhuja & Kunnathur (2015)	Does the company require you to work from a secure VPN? Are there policies regarding BYOD (bring your own device)? How do you limit human errors in the development of the systems?
	GDPR	Protect personal data Adequate, relevant and limited purpose	IMY (2021)	How has GDPR affected your work with information security? Do you have any authorization controls that limit who can access personal data? What routines, if any, are used to make sure the data that is gathered is necessary?

	Risk Management	Calculation and Assessments Response Approach	Li & Li (2020) Dhillon (2007) Berger, Shashidhar & Varol (2020) Stallings & Brown (2018) Gartner (n.d.) Blinowski & Piotrowski (2020)	How do you categorize risks? What does your company value as high-level vs low-level threats? What process do you have in response to risks?
	Standards	Traceability and quality assurance Internal and external weaknesses definition Quality of the standardization process	NIST (2020) Yulianto, Lim & Soewito (2016) Stallings & Brown (2018) Eriksson (2016) Barrett (2018) Shen(2014) SIS (n.d.) ISO (n.d.)	Do you have to follow any defined security standards? If so, which standards?
	ITIL	Security incident managements	Berger, Shashidhar, & Varol (2020)	Do you have a strategy for handling and countering an attack on your service or application?
Operational Controls	Access Controls	Confidentiality Limited access based on necessity Reduction of personal agenda	Stallings & Brown (2018) Saracino (2020)	How do you limit human errors in the development of the systems? What methods are in place to discover if there has been a breach or if someone has accessed information/data they are not authorized to see?
	Authentication and Authorization	Credentials Verification	Stallings & Brown (2018) Anna, K. et al. (2020)	Do you have any authorization controls that limit who can access personal data?
	Formal Controls	Manage information security Define guidelines	Sindhuja & Kunnathur (2015) Chuvakin et al. (2013)	Does the company keep a log of each employee's activities? How do you allocate the resources in your department?

	Testing Auditing	Software reality Quality Assurance Software investigation Vulnerability techniques Effectivity assurance	Xie et al. (2010) Ganesh et al. (2014) Chen et al. (2018) Zwass (2016) Petterson (2005) Herath & Herath (2014) CSI (2011) Watkins & Mills (2011)	How is your security system managed? Do you have a set security system that is maintained or do you actively update and change it? Do you periodically check controls for relevance and intended functionality?
Technical Controls	Zero-Trust	Integrity	Ahmed et al. (2020)	If your service or application would have an intrusion by an unauthorized person, what preventative measures do you have in place?
	SaaS	Operation solution	Simmon (2018) Feher & Sandor (2019) Liu et al. (2018)	What does your IT environment look like?
	Cryptography	Data protection Authentification	Kurd & Besli (2020) Stallings & Brown (2018) Gauravaram et al. (2010) Meylan et al. (2021) Hajny (2020)	What measures, if any, are in place to protect the confidentiality, authenticity, and/or integrity of information?
	Backups	Data storage	Crossler (2010) Mathew & Mai (2018) Zhiyong et al. (2018) Adshead (2021) Liu et al. (2020)	What happens in the case of a systemwide crash, or mistaken delete of an important part of the system?

3 Method

To gain knowledge about how e-commerce organizations work with security controls when handling delicate information, we conducted interviews. Interviewing is a qualitative method that provides a way to investigate "how another person thinks and feels about a specific topic, event, or phenomenon" (Alvehus, 2013, p.81, own translation). In this case, it concerns the topic of information security and controls. With this method, we were able to speak with experts in the field and gain insight into how theories are implemented in a practical setting.

3.1 Research Approach

The interviews were conducted digitally, which benefits the consistency of the method, as we observed that many variables can then be controlled. These variables include, but are not limited to, the interview's setting, structure, time frame, and media usage. For instance, we could ensure that we were always in a quiet and controlled environment where we would not be disturbed. Both Zoom and Microsoft Teams acted as platforms for the interviews, which lasted an hour each, allowing for multiple interviews in a day.

By choosing interviewees in organizations with varying consumer target markets, we were provided with varying perspectives for the study. With these perspectives, we procured an understanding of what controls and methods are used to keep information secure under different circumstances, and with differing company needs. The interviewees were chosen carefully to ensure they were equipped with adequate knowledge of the security systems and practices of a company, thereby providing relevance to the study. By this, we mean that their roles in their respective companies give them the relevant knowledge for the scope of the study. For instance, they all work in an IT department, with work tasks relating to information security.

3.1.1 Interviewee Selection Process

The interviewees selected have roles in the security sectors of companies that provide an e-commerce function. They were found through our private and professional network. Some of the people contacted chose not to partake in the study due to not wanting to share security details. This was an expected issue, as a study into companies' security practices can be seen as a security threat in itself. One person mentioned that we would have a perfect social engineering attack if we manage to get answers to all of our questions. Despite this, a few interviewees were keen to participate with the allowance of not answering all questions or answering some vaguely.

Furthermore, all the people contacted in our "interest check" work at companies that have a connection to e-commerce. We also know that "through a well-thought-out strategic selection, one can access the parts of the organization that can be assumed to be interesting to receive information from" (Alvehus, 2013, p.67, own translation). Accordingly, the people contacted

all have roles within IT and security, also considering that “a homogenous selection makes it easier to make direct comparisons between the people” (Alvehus, 2013, p.69, own translation). Nevertheless, we chose this as our target group in our selection process because, generally, people working in these departments have the knowledge and expertise to answer the questions we pose, while also having the authority to share information they deem harmless. Moreover, we deliberately approached companies in different trades with the endeavor to attain a reliable overview of the e-commerce industry as a whole. Hence, the interviewees work at companies that are within the retail, travel, food and health, and fintech trades. Retail is understandably within e-commerce, considering online shopping is mainly for material goods, but the others may not be as obvious as how they match with the target group. Food and health are currently, especially with the pandemic, a big market for online shopping, as it allows people to buy groceries and medicine without having to leave their homes, keeping many people from becoming sick. FinTech fits into the target group because the company provides the service of handling the sale process for other businesses, which means they handle all of the transactional information and have responsibility over problems related to it. Lastly, we have a travel provider who fits into this study because, although they do not sell tangible goods, they sell tickets to consumers on an online platform, meaning they still have to deal with information handling concerning private people’s data.

Table 2: Interviewee overview

Interviewee	Name	Role	Company size + trade	Interview Date and Time	Appendix
1	Göran Roseen	Solution Architect	FinTech > 2000 employees	20.04.2021, 11:00-12:00	B
2	Person X	Security engineer	Retail ≈ 4000 employees (in department)	20.04.2021, 13:00-14:00	C
3	Andreas Krohn	Head of IT	Travel < 1000 employees	22.04.2021 14:00-15:00	D
4	Jan-Olof Andersson	Data Protection Officer	Retail of food and health ≈ 23 000 employees	23.04.2021 10:30-11:30	E
5	Tomas Gerdin	IT Security Manager	FinTech > 2000 employees	10.05.21, 9:00-10:30	F

3.2 Research Design

3.2.1 Interview

To enable comparable answers between the interviews we designed a semi-structured interview. A semi-structured interview entails that the interviewers follow a structure of having "a few open questions or wider themes that the conversation is based on" (Alvehus, 2013, p.83, own translation), but also allowing the option of follow-up questions. The possibility for follow-up questions in this structure means that clarifications can easily be made, and intriguing answers can be delved into.

Prior to the interviews, we conducted a primary literature study. This was the basis for the questions as we were able to use our knowledge of some theories to tailor them to be as relevant as possible to the study. Having background information on these theories and practices within information security meant that we could have more effective and conducive interviews. Albeit this preparation, we still adopted a form of abductive reasoning. "Abduction refers to an inferential creative process of producing new hypotheses and theories based on surprising research evidence" (Timmermans and Tavory, 2012, n.p.). By this we mean that although we conducted a literature study in preparation for the interviews, we altered the theories analyzed based on new information mentioned by the interviewees. This meant that we could get more relevant and contributing analyses.

We structured the interview by having questions relating to the different types of controls: management, operational, and technical. Within each type of control, we had main questions, follow-up questions, and probes.

> Main questions begin a discussion about each separate part of your research question. Follow-up questions seek detailed information on the themes, concepts, or events that the interviewee introduces, while probes help manage the conversation ... asking for examples or clarification. (Rubin & Rubin, 2012, p.116)

During the interviews we made sure to ask all of the main questions, trying to keep as close to the wording as possible. They were designed to be quite open, as to not manipulate the interviewees towards a specific answer, and allow them to answer as freely as possible. We also wrote down some possible follow-up questions and probes in case the interviewees mentioned something of interest, or if they were unsure what we meant by our main questions (Appendix A). We also placed follow-up questions in addition to, and outside of the scope of, the prepared questions.

3.2.2 Interview Guide

An interview outline was created based on the literature findings to investigate how e-commerce companies do, or do not, utilize security controls. Each question in the interview outline is meant to investigate a certain aspect from the literature, as a way to get an overview of what extent the different security controls are used. The interview followed a structure of 6 categories, with different concepts and interview questions following the concept theme. The first two categories as well as the last category were to give us general information and understanding of the companies. In Table 3: Interview guide, the structure is presented.

Table 3: Interview guide

Category	Concept	Interview question (Appendix A)
Consent	Integrity	1.1, 1.2, 1.3, 6.2
General	Organization IT environment Information security Covid-19	2.1, 2.2 2.3 2.4 2.5
Managerial Controls	Risk management Security Standards Device control GDPR	3.1,3.2, 3.3, 3.4, 3.5 3.6 3.7, 3.8 3.9
Operational Controls	Authorization Security Access Controls Testing Logging Data handling	3.9.1 4.1, 4.2 4.2 4.2 4.3 4.4, 4.5
Technical Controls	Cryptography Detection controls Backups	5.1 5.2, 5.3, 5.5 5.4
Closing	Industry	6.1

3.2.3 Data Collection Method

With the consent of the interviewees, we were able to utilize the recording tools on Zoom and Microsoft Teams for the interviews, which eased the transcription process afterward. Alvehus (2013) mentions that being recorded may make some people feel uncomfortable, which could affect the outcome of the interview, but in this case, none of the interviewees expressed any concern or hesitation to the method. Alvehus (2013) also expresses that in some cases it can even be a comfort to be recorded as they are ensured that what is said will be noted word for word.

Microsoft Word Online was used to help transcribe the recordings, along with some manual edits and corrections, to ease the legibility. Additionally, some parts of the interview steered into topics irrelevant to the study, so these parts were omitted from the transcripts (Appendices B, C, D, E, F). In some cases, there was a request for anonymity, so redactions were made to respect the interviewees' privacy. We also sent the transcripts to the interviewees to check that they were accurate. As well as this, the recordings were deleted after the transcription process, as per some of the interviewees' requests. In the transcripts, we refer to the interviewer as one participant and the interviewee as a second, despite the fact that there were two interviewers present. We chose to do this as a simplification, as we deemed it to have no significance in the study.

3.3 Data Analysis

In the analyzing process, we started by sifting through the data. Reading through each interview and picking out all of the mentions of theories, controls, or methods used in the interviewees' security practices. Once that was done we sorted them thematically, by the different types of controls that they correspond to, while also noting the frequency by which they all were mentioned across the different interviews. At this point, we reduced the findings by grouping similar themes together. With this organization of the data, we were able to analyze and evaluate what types of practices and theories are commonly implemented in information security.

3.4 Validity and Reliability

Validity and reliability are crucial in setting the value of a study in the scientific community. Ensuring that the data gathered is appropriate and relevant to the study leads to validity. Ensuring that the data gathered is correct and trustworthy leads to reliability.

By interviewing people working with e-commerce and security we received pertinent insight for the scope of our study, establishing validity in the interviewees. As a result of having relevant interviewees, we can deduce that the information they shared in the interviews are also accordant with the study and provide a valuable understanding of how they work with security controls. As well as this, conducting interviews as our method for this research led to a quite open conversation on the topics investigated. This means that we could get information from our research participants, the interviewees, that is as true to the industry as we can get. The interviews are also replicable in the sense that the environment was controlled and that a semi-structured interview was conducted. The same questions can be posed to new participants with similar backgrounds to ours, and the answers would be expected to be of a similar nature, save for the chance that new adaptations may arise over time. The questions created are all based on the literature reviewed in this paper. They are designed to question the companies' in which controls they use. Some questions may not be directly linked to a specific theory but that is because we wanted some open questions so as not to guide the answers too strongly. Having literature based questions helps us investigate security controls in companies, and thus shows validity in the study. A method other than interviewing may have restricted the information offered to us, and not allowed for follow-up questions, which turned out to be crucial in gathering the data we needed for this study.

Reliability is largely showing that the study is trustworthy. Throughout the research process we have documented our approaches and methods to both designing the study as well as conducting it. All of the steps taken are presented in the method, along with the reasoning behind the decisions. "Reliability can be enhanced … by employing a good-quality tape for recording and by transcribing the tape" (Creswell, 2013, p.253). Before the interviews, we asked the participants if they were okay with being recorded, and they all agreed to it. We transcribed the interviews shortly after they were conducted, while they were still fresh in our minds, to get as reliable a transcription as possible. To further check the reliability of the transcription we implemented member checking. This "involves taking data … back to the participants so that they can judge the accuracy and credibility of the account" (Creswell, 2013, p.252). Having the affirmation by the interviewees verifies that our interpretations were

legitimate, resulted in increased authenticity. The interviewees all approved of the transcriptions which in turn established both the reliability and validity of the data. Additionally, in the presentation of the results we included all of the interviewees statements on each topic to achieve fair comparisons.

3.5 Ethics

Transparency is very important in conducting ethical research. Creswell (2013) emphasizes that it is "important to disclose the purpose of the study to the participants" (p.57). Therefore, when reaching out to people to check interest in participating in our study we provided an initial overview of who we are, what we are researching, and why we reach out to them, specifically. Out of the 15 people contacted five declined, six didn't answer, and four accepted. Through one of the participating interviewees we also got a new contact leading to a fifth interview.

We sent out more detailed descriptions of what the purpose of the study is to the people who chose to participate and answered any clarifying questions they had. A week prior to the interviews, they were sent the main questions from the interview outline (Appendix A) so they could look through the questions beforehand and let us know if they had any questions or concerns.

Before the interviews started we asked if it was okay to record the interview, and they were all okay with that. Once the recording started we asked them some questions of consent (Appendix A). Starting with the question of anonymity, only one participant chose to keep themselves and their company anonymous. For this person, we adopted an alias from them as Person X and the company as Company X. Offering the option of anonymity is important in terms of ethics because the participants need to feel their privacy is respected, otherwise, it is very difficult to build trust between the interviewer and interviewee (Creswell, 2013).

Subsequently, we informed them of their rights as participants in our study. They were informed that the information gathered during the interview will only be used in regards to this thesis study; that they may choose to stop the interview at any time; and that we will send our findings and final report when it is done. Being aware of these rights, the participants can be confident that they are represented fairly, and that they are not bound by anything if they choose to retract from the study. Additionally, "it is the interviewee that has to have the final say in how [their discourse] is registered" (Alvehus, 2013, p.85, own translation), which is achieved by having the interviewees approve of the transcripts before publication. As a final step, we deleted the recordings of the interviews, so the interviewees could be confident that all the information from them is what is presented in this thesis.

3.6 Method reflection

There were an array of limitations and challenges faced while conducting this study. The main involuntary limitation faced was that Covid-19 restricted travel. This was not a hindrance for the study, however, as there are many tools to enable online interviews. The interviews therefore went well and we had the advantage of being allowed to record them. The digital interview method in turn made it possible to interview people outside of our geographical region, widening the scope of what organizations we could consider.

Despite these conditions, we got many rejections when looking for participants in our study. Some companies simply did not have an IT department, so smaller companies were hard to get a hold of. Some companies did not want to participate due to security concerns, since we are investigating security practices.

We were also faced with some time restraints while conducting this study. To begin with, we had just over two months to create, conduct, and analyse this study. Two months is not very much time to gather interview participants while still allowing time to write an in-depth and coherent report. Therefore, with more time, another researcher could, for instance, conduct more interviews to look at trends across a larger number of companies. What's more, is that we were given a contact for a complementary interview with one of the companies we interviewed, but this interviewee only had time the week before the paper's deadline. This had the effect that more information could be integrated into the results and analysis, but that it could have been done more thoroughly without the time limit.

A final factor that may have affected the interviews' outcomes is language. We wrote the interview questions in English, considering that the research paper is written in English, but all of the interviewees are Swedish. Three of the interviewees did the interviews in English, answering very well and being able to use terminology that we could easily pinpoint in relation to the literature review. The other two answered in Swedish during the interviews, so then it became a bit trickier flagging specific terminology, and we have to trust that we made correct translations. However, it was good that the two who chose to conduct the study in Swedish did so. If they had been uncomfortable during the study due to a language barrier then we would not have gotten as thorough answers as we did.

An improvement that can be made to the study is also to re-evaluate the questions posed. They have literary ground, but there could surely be more clear and effective ways to get the answers we were looking for.

4 Results

The rise of e-commerce has affected the manner in which companies work with security and data handling. To better understand how e-commerce companies have used security controls in their companies and what types of security controls they have used, we chose to do a quantitative research in the form of interviews. We have presented our findings in accordance with the perspectives management, operational, and technological controls; and divided them into categories within the perspectives.

Information and direct quotations from the transcript are cited or referenced in the following form: ApB/00:01:20, this references to Appendix B, time 00:01:20.

4.1 Presentation of interviewees

Following are the interviewees and their respective companies presented for context.

4.1.1 Interviewee 1

The first interviewee is Göran Roseen who works for SveaEkonomi, a company with over 2000 employees (SveaEkonomi, 2021) that focuses on financial technology (FinTech). They have seven teams in their security department, and one aspect of their job is to help their customers with the payment facilitation on their e-commerce sites. Göran works with designing the systems and the future systems, orchestrating how the development is being done (ApB/00:02:24, ApB/00:07:29). The role Göran has is that of a solution architect (ApB/00:01:20).

4.1.2 Interviewee 2

The second interviewee works for a retail company that reaches an international market. The interviewee chose to keep the company and themselves anonymous for this study. Therefore, the company will be referred to as Company X, and the interviewee as Person X. Company X's security department has about 4000 employees (ApC/00:01:29). Person X works in this department, which supports "a wide range of both information as an object and information down to a data point" (ApC/00:01:29). Their role in the organization is that of a security engineer (ApC/00:01:29).

4.1.3 Interviewee 3

The third interviewee is Andreas Krohn who works at ForSea Ferries. ForSea is a company with 750 employees (ForSea Ferries, 2021), that provides transport across Öresund between Helsingborg, Sweden, and Helsingör, Denmark. They sell tickets online for travels on their ferries, but also package deals for events and stays at either side of the water. They have a small IT department that handles the security of their systems. The role Andreas has at the company is as head of IT (ApD/00:01:32).

4.1.4 Interviewee 4

The fourth interviewee is Jan-Olof Andersson who works at ICA. ICA Group AB is a prominent retail company, with approximately 23 000 employees, that concentrates on food and health (ICA, 2020). The company is located in Sweden, Estonia, Latvia, Lithuania (ICA, 2020). The role Jan-Olof has is as a Data Protection Officer in the IT Department at ICA Sweden (ApE/00:00:44).

4.1.5 Interviewee 5

The fifth interviewee is Tomas Gerdin who works at SveaEkonomi, like Göran, Interviewee 1. Göran put us in contact with Tomas, because Göran figured Tomas could answer some of our questions more correctly and detailed considering Tomas works more hands on with the operations (ApB/00:07:29). The role Tomas has is as IT Security Manager (ApF/00:05:08).

4.2 E-commerce

E-commerce is everywhere, as Interviewee 2 said: “Which company is not an e-commerce company anymore?” (ApC/00:50:23). What is quite noticeable in e-commerce is that it is “very fast-moving, and you need to be able to come up with new features very quickly” (ApB/00:52:59). Interviewee 1 goes into how threats are moving very quickly in e-commerce and that you need to be “prepared so you’re not building something that is full of security holes” (ApB/00:52:59). Interviewee 4 sees that the aspect that makes e-commerce unique from many other industries is that it handles a lot of sensitive information, and that the platform has to be accessible all the time, 24/7 (ApE/00:48:22). Additionally, he states that the option for changing data on the side of the consumer is very important, in case they wish to edit an order or their personal information. This, along with the fact that they store information on their consumers to increase efficient purchasing, in turn puts high security requirements on the company to do all of this safely while also protecting the data from unauthorized persons. On the other hand, Interviewee 2 states that e-commerce is probably not too different from other industries in terms of information security and digital information security, but that “it’s just how you fine-tune it, how much you investigate it” (ApC/00:50:23). Interviewee 5 is also along the same lines, saying that there is not a big difference between how they approach security concerns in e-commerce versus finance (ApF/01:19:24). While Interviewee 3 states that they are “not mainly an e-commerce business, [but] an operator that sells tickets online” (ApD/00:48:39), so it is more generally web security for them and thus security around web payments that’s the unique factor.

The threats are also different now, at least according to Interviewee 1 who states that the threats are more commercial now rather than “hacking kids” (ApB/00:52:59). Therefore the companies have certain standards to regulate some of their processes. Interviewee 1, 4, and 5 bring up PCI DSS, which is a certification their developers need to work with card payment systems (ApB/00:16:13, ApE/00:21:26, ApF/00:39:34). Interviewee 5 says it is the strictest regulation they have to adhere to (ApF/01:22:04). In addition to this, Interviewee 1 mentions that they follow PSD2, Payment Services Directive, which monitors the rights and obligations for payment providers and users (ApB/00:16:13). Interviewee 4 expands on their use of ISO standards 27001 and 27002, which covers the management system itself and the safety measure that should be taken for data protection (ApE/00:39:45). Compared to them, Interviewee 5 said they do not use ISO 27001 set out by the Data Protection Authority but

instead have regulations set by the Financial Supervisory Authority (ApF/00:39:34). The interviewee claims that their regulations are stricter than the ISO so it is not seen as a detriment. On top of the financial authorities they also follow EBU, the European Bank Union, who apparently toughen their requirements yearly (ApF/01:22:04).

Interviewee 2 says that they work with NIST standards "in the whole process from requirements until compliance" (ApC/00:19:01). The interviewee says that although there are many standards, they all have a different scope, so "NIST is very general, but deep dives in a good way" (ApC/00:19:39). They see it as a suitable standard for them because it works for both on-premise as well as cloud systems, and they have many systems to secure. As well as the fact that "the ones that have worked with it are some of the greatest names in security" (ApC/00:19:39).

In contrast to the other interviewees, Interviewee 3 mainly has requirements set by "Swedish, Danish and international authorities when it comes to maritime law" (ApD/00:22:39). He explains that the regulations are mainly concerning physical safety, but that "cyber threats, cybersecurity, and so forth are becoming more and more a part of that naturally", but that the requirements of cybersecurity are still quite vague (ApD/00:22:39).

Interviewee 5 said they work with invoices and collections of payments, as well as financing of web services. The company takes over the process for e-commerce websites as soon as the customer is going to pay, this means the e-commerce website "takes no risks and it grows very much" (ApF/00:01:09).

4.3 Information Security

4.3.1 Value

Information security has value, but people see the aspects of it differently. When the interviewees were asked what they see as the most important part of information security they all initially responded that it was a very broad question, as it covers so much and there are many aspects of information security that are important. Interviewee 2 answered that the most important part of information security is "knowing what information you have and where you store it" (ApC/00:05:02). They specify that knowing what you are protecting is key in security, so you can properly protect it. Interviewee 1 said that finding the correct level of risk mitigation is the most important (ApB/00:04:55). This helps them to handle their risks and also keep from expensive measures to protect their data, as they can dampen the effects of the risks and keep them from becoming troubling incidents. Interviewee 4 expressed that they value information security based on the CIA triad (ApE/00:04:52). This is the confidentiality, integrity, and availability of the information they have, which includes valuable financial information, and also their consumers' personal data. They say that it is important to them with information security to uphold confidence in how they handle the information they collect and handle. This includes their own employees' data as well as information on their distributors on top of the customers' data. Similarly, Interviewee 3 also values safety and confidence in that their systems are working as they should (ApD/00:05:15). They were, however, referring to their systems physically, meaning that the mechanics of their systems are safe, as their company is in the business of transport. Interviewee 5 brought up the fact that having information on financials makes them a target (ApF/000:10:52). The most

important thing to them in information security was to be aware of these threats and to also inform vulnerable parties about it.

4.3.2 Structure/software

The software used by the companies varies depending on what's needed and wanted. Interviewee 1 said what he does as a solution architect is orchestrating how the development works and how to apply it in their business area. He said that the company uses web-based payments and that they "consist of seven teams which are working on different services that all together form this business area, and each of the systems has their product owners that are driving development for their systems" (ApB/00:02:24). He continued saying that the allocation of people is very important, such as keeping them in the same teams since that will lead to good teamwork. Therefore the company tries to put "people in teams and then hire new people" so as not to move people around (ApB/00:36:55). According to Interviewee 3, the IT department's job is to make the other departments' job easier since it all depends on the system working properly.

The IT environment that the companies have ranges from having data on the cloud to having a blend of both cloud and other solutions, as well as their own solutions without using the clouds. Interviewee 1 and 5 said they have nothing in the cloud, Interviewees 2 and 4 said they have a hybrid, and Interviewee 3 said they have everything on the cloud. Interviewee 2 mentioned that they both have a hybrid cloud solution and data server holes, the hybrid "are mainly into vendors of the big vendors, so [they] do not act as small cloud supporters or cloud vendors" (ApC/00:03:36). Interviewee 2 said they have a lot of in-house development and workforce, as well as consultants and SaaS solutions, which is when "you have software as a service" (ApC/00:04:33). Interviewee 4 also said they have a hybrid solution. They store locally and on the cloud, and also use external resources for the operations. Interviewee 3 said they have partners that help with all their IT infrastructure since they have everything on the cloud. Interviewee 5 explained they don't have cloud services considering that, as a financial company, they do not want to have personal data on the cloud since they are not aware where it lands, which is an impasse for the company. He explained that they are in business with many American operators and often use Microsoft, which means the banking information can be located in other countries which can be a problem for the company.

The software used depends on what the organization needs, some use older software and others newer. Interviewee 1 said they use both old and new, which means that when changes in the software are needed the coordination is performed by the solution architects on different levels. He also said that the company has to make sure nothing is thrown away that is working well for the company, and that they only replace systems when they are no longer performing efficiently. When they do get new software, it could be a combination of off-the-shelf software and new standard systems, but Interviewee 1 mentioned that their company "always strive[s] to take ready-made software" (ApB/00:29:56).

Interviewee 2 works with several security systems, and said they have a responsibility to update and maintain them. This is both the responsibility of the SaaS vendor and the company, but ultimately the company has responsibility for the security system. Interviewee 3 said that "in a perfect world, I would just scrap them and have something else," about changing old systems (ApD/00:33:51). He lamented that it isn't a perfect world and legacy systems cannot be easily rid of, and that any company that's been in business for more than 5 years has a legacy system.

Another difference between the companies is that they work in different manners within their organization. Interviewee 4 said they work agilely throughout the whole organization. They make yearly plans that are broken down into 4 month periods, and goals are set up for different parts of the organization on how to achieve the plans. He said they design risk analyzes, treatment analyzes, information classification, and development of safety requirements within the different developments; and that there has to be communication about the resources that need to be allocated (ApE/00:36:23). The requirements mentioned are decided in the feasibility study in projects, as well as the use of other requirements such as PCI DSS and data protection. According to Interviewee 4 the need for different resources can be allocated when developing new solutions within the company. If competences are needed from other departments then this assessment is made in the feasibility study and if one chooses to proceed (ApE/00:38:23).

The companies also work with technologies in many different ways. Since some of the technologies are complex, the companies can use internal resources that help with these technologies, but they can also bring in consultants. Interviewee 1 said they use consultants to help with "analyzing the threats," and that they have services they subscribe to for checking possible threats to their systems (ApB/00:11:31). Interviewee 2 said they use CVE lists to check if something is happening on the market, and take it into account when developing their systems. This is a similar approach to Interviewee 1, who uses databases to search for abnormalities to see if someone else has already seen the same problem. Interviewee 1 mentioned that the threats today are global and professional, and that "to work against them you need to be cooperating" (ApB/00:11:31). Therefore, using the database can be helpful for several companies as they can see if the same malicious code has happened in other countries and companies across the globe.

When it comes to storing data, it is located in data centers, which can be located at different places and be functioned by one or several centers. Interviewee 1 said they are working in two systems at the same time, and have exact copies of their data in both places. In the case a system shuts down, they "would just switch over to [use] service just from one place" (ApB/00:51:04). Interviewee 3 said they have their data centers located in Malmö, and have most of their servers there. Interviewee 3 works at ForSea Ferries, and said there are servers on the ferries since if the internet connection goes down then the infrastructure needs to be on the ferries as well. Interviewee 5 said they have a data center with their own servers, where they store all their customer data, which can be very sensitive information. Interviewee 5 mentioned that since they have a lot of personal data that is collected, they are required to maintain good protection. They do this by having the highest protection of data as possible, which is also important when handling and keeping the data (ApF/00:07:34).

Interviewee 4 said that in a security system many components are needed to protect the information. For instance, having network components, system authorization, and logging as well as other components. Thereby, he mentioned that in their infrastructure they need to administrate authentication in applications and have security rules for the infrastructure, which can be operated by the whole organization within the company or from a team. According to Interviewee 4 they have security operation centers that manage the security components in their infrastructure to secure the information during storage, communication and so on (ApE/00:30:38).

Interviewee 5 said they use the heaviest encryption, for the short data since they have HSM which is hardware that is encrypted. There are different levels and encryptions that are not as

tough, but are bought from external parties as certificates. Interviewee 5 said that everything that has to do with the web today is a certificate, and that they have no web-traffic that does not go through HTTPs (ApF/01:04:50). These certificates have an expiration date of 2 years.

4.3.3 Strategy

The companies have strategies that they use in their organizations. Depending on the size of the company and what they want to achieve, they have different means and resources to do so. Interviewee 1 said that they have to be a bit secretive about the strategies they use but that there are several, and that they have ways of monitoring the systems. There are "people monitoring the systems 24 hours a day, and we have a lot of logging and ways of finding anomalies in the logs" (ApB/00:14:52). Interviewee 1 said that they often have to make compromises and prioritize things. For instance, teams that have several tasks have to prioritize what task should come first and make a "time-wise separation" (ApB/00:38:10). Interviewee 3 didn't want to go into detail in their strategy for handling and countering an attack on their service, but they admitted to having a strategy. He said they have penetrative tests to see what needs to be focused on, for example. This is done by external experts that help test the security and can inform what needs to be prioritized. This is helpful since they can inform where there are problems and how to handle them. Interviewee 4 said that they follow the PCI DSS regulation, and evaluate what happens in an incident, and how they can learn from this and compare it with other incidents. He also said they have desktop simulations, discussions, and perform risk analyses to see if possible attack and risks can occur, as well as how they can work to prevent this (ApE/00:17:34).

Interviewee 2 said that when talking about information security, it is important to know what information you have and where to store it. The important step is knowing what you are protecting. Interviewee 2 mentioned that they use the zero-trust strategy, which entails that "you don't trust anyone: you don't trust the homepage; you don't trust certificates; everything is verified again" (ApC/00:06:26). This is something that has arisen during the pandemic since everyone is working from home, and they want to connect to the network from new places. Interviewee 2 said that they traditionally secure their network at their place of work since everyone works from the same place. This way they could focus on putting up firewalls, detectors, and connectors to secure their network, but now, during the pandemic, an endpoint is outside the network, which is a problem. The employees cannot rely on the company's sphere, instead they each "need to also see that each endpoint stands alone securely" (ApC/00:06:26).

Interviewee 5 said that they have four aspects when working with information security. The first aspect is information security that manages the wiring system; the second aspect is IT security; the third aspect is cybersecurity and other investigations regarding cyber threats; and the fourth aspect is physical security. According to Interviewee 5, the physical security can be safeguards such as alarms, fire alarms, controls, and protection of persons (ApF/00:05:08). These four aspects form the security operation within the company he works at, and they try to make sure the company is safe by working with these different aspects.

Furthermore, the companies are working with finding better means of working with prioritizing standards and policies. Interviewee 1 said they have OKRs (Objectives and Key Results), which are defined business objectives and key results they want to achieve. Interviewee 1 said: "during the first part of 2021 we want to achieve something that is more limited in scope so that it's possible to achieve" (ApB/00:39:10). For each key result they try

to create tasks that will work towards achieving the OKR, and they try to change their OKRs every half year or quarter depending on the company's situation . Interviewee 1 said that the OKRs are delegated from the business area manager who decides what the objectives would be, and the employees can give suggestions for objectives to the business area manager. After this the objectives are divided into teams that then decide the key results. There is a lot of cooperation between the different teams in this process since they have different resources. The manager and employees work together to decide what needs to be done and the teams thereby can decide which tasks need to be done to reach the key results. Interviewee 1 said that there needs to be "different levels of setting up goals and defining what to do in order to come to those goals," thereby teams can decide amongst themselves how to reach the key results (ApB/00:40:38).

Interviewee 2 said that since they work with strategic security, they help application teams secure their environments and can recommend to them what strategy to use. The company Interviewee 2 works at has detective and reactive measures, both from buying tools and using in-house tools. Interviewee 2 said that their way of getting solutions is, from a security standpoint, very personal in a way. The company has new people coming into the company with new experiences and competences, which is a focus for the company, but it is also important to have security tools that are important resources to the company. The interviewee added that they invest in people and how to use their competences in the most useful way. Interviewee 2 pushed on the fact that "when you look from a people perspective, you usually talk about personas and customer journey," which is the most useful for building applications, and it seems like the company has gained a lot from this (ApC/00:40:00).

In the case of a systemwide crash, there are strategies to handle this, all companies have a plan of what they should do if it happens. Interviewee 1 said they have a plan in case of a crash by having two data centers. The data centers have the same data stored, which means they are exact replicas of each other, and if one crashes then the other takes over. If it is instead a mistaken delete, then good backups are necessary but that would mean that the company loses a lot of tasks already performed, and this is something the company wants to avoid. In the case that both data centers crashed, the company that Interviewee 1 works for hasn't planned for, and the company data would be completely gone in that case. Interviewee 2 said that they need to have a disaster recovery plan put in place to protect information, but especially the applications that controls warn to have high-security classification. In the case that a crash happens, the company can mirror it out and shift to another application or region and run from there instead. In the case an application has an intrusion from an authorized person, Interviewee 2 said they have tools for it, and processes are started to find out how it happened and how they can prevent it. Interviewee 4 said they have recovery plans within IT, which is a part of their continuity plan since they have to have a plan in the case they need to recover from an incident or a crash.

4.3.4 Human factor

The human factor when it comes to errors in systems seems to be a very common problem. All of the interviewees mentioned some form of concern over the human factor, or that it is the most common cause of errors (ie. ApD/00:37:16). Interviewee 2 stated outright that "usually, you say that humans are the biggest security risk" (ApC/00:35:35).

Interviewee 1 explained that they have a thorough process for testing software and even have a dedicated Quality Assurance department consisting of experts on finding problems in their systems (ApB/00:30:30). By completing these various tests they aim to eradicate any errors

made by the creators of the system, and also to verify that the system works as it should and is properly protected by security measures. He specifically mentions that they perform tests such as developer testing, system testing, user acceptance testing. Interviewee 5 corroborates this (ApF/00:21:21). Similarly, Interviewee 3 says that they perform tests where they can. However, most of their development is done by external parties, so they do not have a great number of controls in place to control for human error (ApD/00:34:53). Moreover, Interviewee 4 also backs up that performing tests is a method of minimizing human error (ApE/00:32:08). He specifies that they have auto-generated tests for the code, and then more detailed tests to check the functionality and performance. Additionally, he says that it is organized through the four-eyes principle, so the testers of an application did not write the code and have another role in the organization. In a similar manner over being checked, Interviewee 5 mentioned that they reduce 'deliberate' human error through constant logging, so they can see if someone does something unusual or harmful in a system, and who it was (ApF/01:00:39).

Interviewee 2 differs a bit from the group as they go a bit more into the fact that human error originates from an actual person. The interviewee says they're partial towards ITIL, where "you define your processes in a very fine-tuned way and that you can also add security features down to it" (ApC/00:35:35). They then express that it is more than just security to limit human error, though, but also security awareness, This entails that every developer at the company has to be a part of the process, "because if they don't know what security is, we cannot maintain it" (ApC/00:35:35).

4.3.5 Workplace measures

In terms of workplace measures, the interviewees were asked about BYOD policies and whether their companies implement a secure VPN for remote work. These interviews varied in how detailed answers the interviewees felt comfortable with divulging. For instance, Interviewee 2 had no comment on whether they work from a VPN, and could answer that they have a policy on BYOD, but not what the policy contains. However, Interviewee 1explains that they have "rules about not having any copies of the software in your local computer at home" (ApB/00:17:18), which is where the VPN is implemented to allow them to work in a type of virtual machine environment, by "remoting into computers inside the company" (ApB/00:17:18), which Interviewee 5 confirms (ApF/00:37:20). Interviewee 4 also says they work via VPN, and seems to be quite happy with the solution (ApE/00:22:26). In contrast, Interviewee 3's company does not use VPN, but instead a solution called Citrix (ApD/00:24:03). He explains that VPN connects two networks, but they do not want anyone to connect to their work network. Therefore, they use Citrix which allows you to log in remotely to a computer, "basically working in a virtual machine that's hosted on [their own] network" (ApD/00:24:03).

On the topic of BYOD, all of the interviewees said they have some form of policy for it. The three that elaborated said they were quite informal and not very strict, however. The main thing they have in place is there is a guest Wi-Fi network for people to connect their private devices. Interviewee 3 said that there are not any technical hindrances keeping you from connecting to the work network, however (ApD/00:25:05). Interviewee 1 seemed to be a bit more strict in that they have an unofficial policy that you are not allowed to work on your private device for anything that can be deemed sensitive information (ApB/00:20:38). One struggle with this unofficial policy is that they do not have defined what is considered sensitive data (ApB/00:23:07), which can become cumbersome (ApB/00:22:10). Interviewee

5 adds to this that they, at the same company, also do their best to make sure everyone at least has virus protection, but that it is tough to ensure on peoples' private computers (ApF/00:35:44). Meanwhile, Interviewee 4's company allows you to use a device at work as long as it can be 'managed' by the company, meaning that the company has access to anything regarding work tasks performed on it (ApE/00:23:30). They do have controls in place to classify information, with help from, for example, Microsoft 365 (ApE/00:08:29). Through this, they can encrypt information that is taken out on devices that are not set up to have access to it.

4.3.6 Covid-19 Pandemic

The Covid-19 pandemic has affected many industries and one of those is e-commerce. The interviewees all said that the companies they work at have been affected in some way, whether it be sales or internal work habits. Interviewee 2 could not comment on the sales of their company but mentioned that they have a lot more to do now than they did before (ApC/00:05.46). They explained that moving to remote work makes it more difficult to implement a zero-trust strategy (ApC/00:06:26). Working remotely implies employees wanting to connect to the work network remotely, which makes it harder to ensure secure connections. In contrast, Interviewee 4 did not feel like the network security was an issue, as they had just two years ago changed location and changed work habits along with that (ApE/00:06:38). By this, they mean that they had the infrastructure to support remote work and that everything was already 'on the net', with smaller issues such as having to handle physical documents. They work from a VPN and have also implemented various other measures due to the pandemic (ApE/00:08:29). Interviewee 1 also mentions that they have a VPN for working from home, and that they were a bit reluctant to have people working from home, due to security concerns, but that they have seen that they can make it work (ApB/00:17:18). Interviewee 5 says that they even looked into buying all of their employees new computers to use when they work from home, but that it was materialistically unrealistic, they instead tried to ensure that everyone had decent tools to work with (ApF/00:35:44). Although the call center had to stay on location due to systematic restraints, it also had the space to spread out due to fewer people on location (ApF/00:32:39).

Looking at sales, it has affected Interviewee 1's company with "a huge increase in sales because … people have changed to ordering on the net" (ApB/00:06:30). However, the increase in sales has not affected the work in information security "because that's just the volumes and you must still do the same work whether you have large or small volumes" (ApB/00:06:30). Interviewee 5 saying that in his department there is more to do due to the increase in sales (ApF/00:32:39). In response to an increase in distant consumerism on the part of Interviewee 2's company, they mention that there is more to do in general as they have to adapt to also making everything available for previously reluctant customers who were not early adopters of e-commerce. Compared to the other companies, Interviewee 3's company focuses on travel, and although they offer online purchase of tickets they have had a decrease in consumers due to the travel restrictions following the Covid-19 pandemic (ApD/00:06:20). They, therefore, do not have more work, actually less, but they have managed to use the lessened workload to focus on IT security (ApD/00:06:20).

4.4 Data storage and handling

How data is handled and stored is very different depending on what company you look at it in the sector. Some of the companies interviewed have their own environments, like Interviewee 1, and use their own internal cloud, and other companies, like Interviewee 2, 3, 4 and 5, use the cloud but in different constellations. Interviewee 2 said that they use a hybrid, some of the instances are in the cloud, which are vendors of big companies, and some are on-premises. The same is for Interviewee 4 where they use a hybrid of storing their data locally as well as on the cloud, and in some instances they put their operations externally. Differing from the others, Interviewee 3's company has everything on the cloud and has partners that help them with their infrastructure.

Data is handled in many different ways since information is often stored on many devices. Interviewee 1 mentioned that you're allowed to work with sensitive data, but not on your own personal device. If the information is work-related but not sensitive or concerning personal data, then you can work from your own device and talk openly in meetings between colleagues about the work you are doing. However, as soon as you are delving into sensitive information you are not allowed to use your own device. This also applies when using cloud services. Interviewee 1 mentioned that they are "not using cloud services for anything sensitive;" and this only refers to sensitive information such as code and actual systems interconnections (ApB/00:20:38).

When handling sensitive data such as bank accounts and other personal information, Interviewee 1 mentioned that "certain actions will have to have what we call duality, or four eyes, which means that two people need to perform the action" (ApB/00:33:13). This can be used specifically when the actions can have financial effects on the system. There are different processes when the four-eyes method is used. These include when a payment to a customer has to be to the correct account; when changing a bank account; and granting access to a new user into certain sensitive areas. This can differ from other companies where the organization does not gather sensitive data since it is not needed for the company's operation. Interviewee 3 said they "have very little data about [their] customers" since they do not need a lot of data about their customers when they use their services (ApD/00:18:09). Depending on how the transaction of payment is made and where the service is conducted, different information has to be given and saved about the customers.

Interviewee 3 mentioned that they have data centers in Malmö, where they have most of the servers. The physical machines are located in Malmö and on the ferries in case the internet connection goes down. Interviewee 5 said they have a data center with their own servers where they store all their customer data, which can be very sensitive information. Interviewee 5 mentioned that they have a lot of personal data that is collected, and this requires them to maintain good protection by having the highest protection of data as possible, but it is also important when handling and keeping the data (ApF/00:07:34).

Information security is applicable to a whole company. Interviewee 5 said that the management system steers the direction the company works towards. The government requires that the company has a management system and that the company follows it. Documentation of the management system is important, but it is equally important to do what you document and not use the documentation as a way of showing you achieve the requirements when it is not the case. It is better to write the reality of how the management system is used and thereafter expand or change the items in the management system. According to Interviewee 5 they have controls from Swedish Financial Supervisory Authority,

as well as an internal audit every year at the request of the board. This internal audit is performed by an external party, who checks what financial tools are used and what the IT looks like. They make sure the company follows the management system and do what has been presented there.

4.4.1 Data loss and tampering prevention

Interviewee 5 said that he is always trying to prevent malicious attacks. The company uses an intelligence system to try to prevent unauthorized users from entering the company's system. This tool searches the web and dark web to see if the company's name is mentioned anywhere suspicious. This is useful if the company's name suddenly appears on the dark web, then they can see where logins or other data is being sold to infiltrate the company's system. Interviewee 5 said that by using the intelligent threat analyzing tool they can find a lot of information that is being published about the company on the web. This can be serious since some of the threats give instructions on how to enter the system or if the company has a weakness. This can often be detected before the incident and can then be prevented. Interviewee 5 also said that this can be by accident. There have been cases when an employee posts code online to get help to solve something without realizing how dangerous it can be to the company. This is prevented by having the intelligence system, thereby removing the code immediately when detected. The tool can also be used to find the company's clearing number. This way they can see if their customers' account numbers are online and unprotected. An event like that needs to be prevented and detected early, to make sure they can stop it from hurting the company and customers. The tool can be expensive but is useful and needed if the company wants to work preventatively, according to the interviewee.

Checking for data loss and tampering is something that the companies were a bit secretive about, but gave us general answers and some hypothetical answers, too. According to Interviewee 1, tampering in their company is detected by checking a list of orders. If the sum from different lists is the same then the order is correct, but in the case of tampering one of the lists might differ and that is a way of detecting it. Interviewee 1 referred to this as redundancy. Redundancy has in the past been avoided since it was expensive with data storage, but since today's data storage is cheaper, the data can be stored in several different formats and not be too expensive. This is something that has improved the companies performance since the data can be in different forms to make them accessible when needed. “You can save the data in one form where it's easy to get it out for one purpose and you can store it in another form where it's easier for another purpose” (ApB/00:45:49).

In the case of system-wide crashes or system downtime, the system can be shut down or the data not available for the companies. Interviewee 1 said that in the case that the data is not available, they “keep working on bringing up the system again” (ApB/00:35:51). When a system-wide crash happens, most companies have a plan for this, although this is something that has a very small chance of happening. The companies have their data stored in data centers, some have several in different locations and some have one or two. In the case where companies have several, the data centers would store the same data at both locations, but in the case one shuts down then the other would still have the data available. Interviewee 1 mentioned that a more difficult situation would be if there would be a mistaken delete, and their way of dealing with this is to have a good backup and if necessary restore the backup. This could be a difficult situation since there is “a time difference between when you detect something and when you have your last backup”, which would indicate the company would have to redo several processes to regain the lost data (ApB/00:47:40).

Interviewee 5 said that if the data was not available because the system was down, it would be a nightmare for the company. They work a lot with load balancing, meaning that all systems should be duplicated or more. The more the load increases, the more web servers are activated. The load balancing distributes the power, and it is therefore important to build a system that can handle the pressure. The system being down would cost the company a lot of money, which is something that cannot happen. Therefore the duplication is needed in case one of the systems is down, which hopefully happens without the customer's knowledge. Interviewee 5 said that this is also a way to maintain the systems. They can turn one off to update and then turn it on without having to pause their services. He said this is done continuously all the time with all their systems (ApF/00:47:59).

Interviewee 4 said that in the case of a defect or disruption in the information system, an assessment is made of the severity, and what priority the handling of this should have (ApE/00:43:38). One of the companies uses the ITIL framework, which has four classifications, which helps decide what department in the company will handle the disruption. Interviewee 4 handles it themselves when it is on the lowest classification, and in the case of the highest classification it is handled by a department that will try to get the information going quickly. He also said that in the case it is security-related, another process is needed and the security department handles the incident. Using a similar approach with security classification, Interviewee 2 presented that to handle security disruptions, controls are put in place and a disaster recovery plan is used. Interviewee 2 said that "you have it mirrored out so you can just shift," which helps to shift to another region, for example, if there is a discrepancy in the region you are working in and the company tries to "keep it so super general so everyone can apply it depending on their business criticality" (ApC/00:43:53). In the case of discrepancies in the system, Interviewee 3 said they try to make sure that it is only the user who should have access to the system but beyond this, the company cannot do much more than that.

There is data the companies do not want to be stored, for instance, toxic data. This is data gathered that the company might not use or have a necessity for. Interviewee 3 said they actively avoid toxic data, for example in the form of facial recognition. This is data that they do not want to have and Interviewee 3 said that it "will go wrong if [they] have that ability and that data stored somewhere" (ApD/00:15:29). The company can use other companies to handle toxic data, such as credit card numbers, by using banks or Klarna. Risks will be reduced if companies look at what data they have and only gather what they need since this reduces the chance for data leakage and minimizes the risk of someone using the information against the company.

4.4.2 Confidentiality, Integrity, and Availability

To protect the confidentiality, availability, and integrity of information, there are different methods the companies used. Interviewee 1 mentioned using validations to make sure the information is correct and hasn't been tampered with. Through the use of API calls and checksums, the company can make sure the messages from the customers are not tampered with. Interviewee 1 said that "protecting the databases, that's the data addressed, and the checksums are protecting the data in transit" (ApB/00:42:21).

Interviewee 5 said that they have a big responsibility to inform their customers about the work they do and the data they store and handle. They also have a responsibility to inform the consumers what they can be expected to hear from the company. For example, inform them

that they do not ask for certain types of data, and that if they get a call like that it is most likely a fraud or scheme. Interviewee 5 added that they work closely with the police as well as other companies, such as Telia, to try to trace where the calls are coming from and prevent more similar events.

One aspect of data storage is that the data handled should be removed regularly. Often it is done automatically by schedules and rules, depending on the data which can be determined by its type and what process should be applied to it. This is a preventive method against human errors, since the system makes sure that they "remove the data when it's supposed to be removed," according to Interviewee 1 (ApB/00:49:02). The exception to this is the GDPR, where a person has the right to be forgotten. This was also brought forward by Interviewee 4, who stated that since a person has the right to be forgotten the company has automatic functions that remove information (ApE/00:29:17). This is something that is done for all applications such as Outlook and many others, in this way the company does not have to think about when as well as what information has to be removed, save for specific cases. Interviewee 1 said that they handle specific information removal requests on a case-to-case basis.

To make sure the systems are working the way they should and are not doing anything wrong is important, therefore companies can have different approaches for checking this. Interviewee 1 mentioned that they have yearly audits that make sure regulations are followed, such as GDPR, and that the systems processes are functioning correctly. He also mentioned that their company does not "have any routines in day-to-day work" since most of their systems are already implemented and only incremental changes are made, but routines could be different if the systems were to be built up from scratch (ApB/00:25:59). Additionally, he said there is a data protection officer at their company that can help when needed if employees are unsure about what they can and cannot do. There are other ways of testing the systems, such as testing in different forms and in different parts of the system. Interviewee 3 said that they use penetration testing which "is a good way to verify that everything has been done;" if something has been missed from a policy; and to make sure their system works (ApD/00:43:20).

4.4.3 Testing and Logging

Interviewee 5 said they do penetration tests, which they buy from other companies. They hire people who try to enter their system and find vulnerabilities, to see if the controls put in place will stop them. This is expensive but the company thinks it is a necessity, partly for regulatory reasons as well as for their own gain. They have many different systems and it is hard to scan all these systems, so they try to vulnerability test them. This is not only done automatically or through systems that check them, but physically testing them by having people trying to enter the system. Interviewee 5 said there will be more demands for this in the future, and you can already see it now that the regulations are creating requirements for this (ApF/00:26:21). Therefore there will probably be requirements from the EU in the future to have penetration testing.

Testing can be used by companies to detect abnormalities that can occur in the security systems, "when you're coding you can see your code and then you run it through and set it to that application testing system" (ApC/00:30:06). This helps note where the company can have security flaws in the system. This can be done by using different tools such as the open-source tool SaaS, a tool that was used by one company, and can generally be used when companies

have different languages when developing. Interviewee 2 mentioned a CVE list that they use to see what risks are happening in the market, and that way when they "see that something is happening, [they] can draw it in and detect it already in line when ... developing" (ApC/00:30:06). The companies said that the tools they use depend on the size of the company and the complexity of the security solutions needed. One interviewee said that when they worked at a smaller company they never looked at their security system, and now working at a big company they have big teams that can help with different security issues, and the responsibility is not only on one person.

Logging was something the companies didn't want to discuss in detail, they gave a more general answer to the questions regarding this. Interviewee 2 did not want to comment on logging and Interviewee 1 went into parts of it. According to Interviewee 1, there are people working with monitoring 24 hours a day, and they "have a lot of logging and ways of finding anomalies in the logs" (ApB/00:14:52). The data logged in the system can show when personnel does something or changes are made. There are back-office functions that log what happens when it happens, and who does it. Interviewee 3 said that they log depending on "how critical it is, and what critical data it might contain" (ApD/00:35:30). Therefore no comprehensive logs are done on everything in the systems, albeit some key systems are monitored. This is a similar approach to how Interviewee 4 said they do at their company, which is that not all personnel is monitored but the company may monitor specific systems.

Interviewee 4 mentions two different perspectives to logging. The first is to find faults and to manage a discrepancy or crash in the system. The second is that someone has broken the security rules. There are rules for logging towards the sensitivity of the user and system, such as classification of information, which puts higher expectations on logging. According to Interviewee 4 there is logging both in "applications, servers, and other functions" (ApE/00:33:41). From a data protection perspective the information logged in the different places has to specify how long it can be managed. The usual time presented from the interviews for how long information can be logged is around a year's time. Interviewee 4 said during his interview that if a security risk hasn't been detected during that time, the organization has problems, which reflects the importance of having relevant logging functions (ApE/00:33:41).

Interviewee 5 said that the key is to look for patterns in the loggings. They use an AI engine to look through the data and find discrepancies, and then a technician can look through it. When a discrepancy is detected by looking through the pattern, an alarm is activated that sends out a signal. Interviewee 5 said that logging is used to help handle risks. They log a large quantity of data, about 50GB, every day from their systems that they analyze. They have a SOC that looks through patterns in the logs 24/7 and activates an alarm if they find anything that sticks out in the pattern. Interviewee 5 said that this alarm can detect something within the operation, but it can also detect something to do with the security. The alarm lets the company know that someone is trying to enter the system and in that case the SOC has the mandate to shut the system down and try to prevent the intruder from entering the system. By looking through patterns on all different types of systems, such as firewall and virus programs, vulnerabilities can be found. Interviewee 5 said it is an informant factor to logg what has gone wrong, since the more they logg, the more they can detect threats before they occur. In the case an attack happens, the company will detect it early, and be prepared and able to turn off the system that is attacked. Interviewee 5 said time is of the essence, since the earlier they detect the attack the faster they can reduce its impact on the company (ApF/00:52:50).

Logging the employees work is something that companies do, but they have to be careful when handling this information. According to Interviewee 5 they log some information when an employee uses a system, but mostly the logs contain behavior from the company's side. This means that they mainly check that the company has done the correct actions to detect discrepancies in the software. Interviewee 5 said logging can be a useful tool when working with fraud or crime, since they follow a pattern and the company can see what pattern a user has. What the user does in the system and where they log in from is all logged by the company firewalls that can see where the traffic is coming from. If this is done by a criminal, the logs can be useful for the police and be used in a criminal investigation since there is an electronic track to the user. According to Interviewee 5, it is also important to log the employees activities since they can monitor that they do not mess with the system. They trust their employees, but the biggest threat would be if an employee would have a grudge against the company and would do something hurtful to the company. This is the reason why it is important to log all activities in the systems, to see how it is using the systems, and to use the SOC to see if someone has accessed a system with sensitive information.

Interviewee 4 mentioned that the components of infrastructure in Microsoft 365, such as firewalls, IPS registers, and other functions, have logging functions. Ones that trigger alarms when someone tries to break the security rules put in place. In every component in the infrastructure, there are types of kick-start effects and mechanisms that trigger the effects if someone tries to go outside of their access (ApE/00:19:21). Interviewee 4 gave the example when an employee often works from home and suddenly there is traffic coming from another place, an alarm will be triggered.

4.5 Authorization and Access

All of the interviewees mentioned that the companies they work at use some form of access and authorization controls. The main reasons being to reduce errors in the system, and to protect data. For access controls, all of the organizations explained that they use the idea of least privilege. "That means that you should only know what you need to know" (ApC/00:38:03). Basically meaning that a person should not have access to more information than is necessary. Interviewee 1 mentioned that one way of doing this is by having "a specific role assigned to you in order to be able to perform certain actions" (ApB/00:33:13). This also implements the concept of separation of duties, which entails that you do not have the power to manipulate data that you work with for an analytical purpose. For instance, "normal users or developers won't have access to the production data so that they can change it" (ApB/00:42:21). Interviewee 5 affirms that they do not allow access to information that is not necessary for your defined work tasks, and that all workers have a certain clearance level within the systems (ApF/01:00:39).

This also links into authorization as it checks that the right person is accessing secured data.

> If you should have information on objects that are very highly classified, you need to have these security controls in place, and that limits of course who has access and how you authorize that page or to the application itself - Interviewee 2 (ApC/00:25:07).

Interviewee 1 specifies that they use Active Directory, a Microsoft Authorization solution to manage many of their controls (ApB/00:24:52). Interviewee 5 also said this, and added that to access certain systems you need more than a password to access them (ApF/01:00:39). You

apparently have to access a specific system to then be granted access to the extra secure systems. These secured systems are also under constant surveillance by logging to ensure that they know who does what, in the case that someone acts maliciously. Moving on, Interviewee 4 follows the 27002 ISO regulation that helps indicate what length their passwords should be, and whether two-factor authentication is needed (ApE/00:39:45). Two-factor authentication is also used by Interviewee 5's company (ApF/00:15:31). They implement that a QR code comes up to scan, this way they can be sure that it is the right person trying to gain access to whatever it may be. He even goes as far to say that usernames and passwords are becoming obsolete, and that nowadays it is either Bank-ID, SMS codes, or the like. Furthermore, a unique detail he mentioned was that they implement access controls on their users as well (ApF/01:04:50). Perhaps not in the traditional way, but by limiting which web-browsers can be used to access the company's services. By this he explains that they are not compatible with certain older browsers, and that if it were up to him they would only be compatible with the latest versions, because it is more secure, but that is not realistic when you want people to be able to use your services. Overall, the interviewees expressed that they have authorization controls that follow the restrictions set by the access control level.

Accordingly, a few of the interviewees mentioned that the access controls are placed in accordance to what information is stored. For instance, Interviewee 3 said that how they decide which processes they set up to limit access "depends very much on each system as well because [the data is] not all in one big database" (ApD/00:27:15). The more classified information is the more restricted access it has and vice versa. Interviewee 2 said that if they have "customer data, then [they] classify information highly, that it needs to be confidential, has integrity, and is always available" (ApC/00:25:07). Interviewees 1, 3, and 4 mentioned that they employ several technical solutions that limit access, but not going into much detail about which ones. Interviewee 4 explained that they have some general solutions but also some built-in functions based on the requirements set for the specific application (ApE/00:28:20). For instance, through the use of Microsoft 365, they can classify information and then encrypt it if the device trying to download it does not have the necessary access rights (ApE/00:08:29). They did, however, not want to specify much more because then an attacker could use this knowledge to counteract the controls (ApE/00:41:29).

4.6 Risk Management

When looking at risk management there is a general consensus that you want to avoid a risk actually becoming an incident. Interviewee 2 says that they usually do classification through assessments and go from there (ApC/00:42:26), while both Interviewees 1 and 4 mention a type of sliding scale to assess the level of a threat (ApB/00:07:29, ApE/00:09:52). Interviewee 4 expands on this, saying that they have a scale from 0 to 5, and the higher the number the greater the damage a certain risk can cause (ApE/00:09:52). They calculate the impact of possible incidents via risk analyses, which are most commonly performed by a CIRT throughout the year and the board annually, considering that they have a governance structure connected to risk management (ApE/00:09:52). Based on the results from the analyses they can evaluate if there are risks that are too high-level within a certain area or development phase. He says that they perform risk analyses regularly throughout the whole company, during the development and realisation of projects (ApE/00:12:05). One that they do, in particular, is a Data Privacy Impact Assessment, to see what risks exist in relation to the customers, on top of the company.

Similar to the risk analyses mentioned, Interviewee 2 said that they have an impact probability model to see how probable a risk is of becoming an incident, and then the impact of this event (ApC/00:10:23). On top of this, they perform a business impact analysis to "look at what can happen in the business if something is breached or if something happens" (ApC/00:42:42). They check to see what the impact is and how they can handle it, which tells them how confidential it is and how they should classify it. At Interviewee 3's company they also perform a type of impact analysis, combined with an evaluation of the likelihood of the risk taking place, to help categorize the risks into different levels of threat (ApD/00:11:58). For instance, "some things are very likely, but there's basically no impact and other things are unlikely, but the impact is [they] could lose passenger or employee lives, which must be taken very seriously" (ApD/00:11:58). Creating a risk matrix they have a company-wide overview, and then break it down into more detailed threats that need to be handled. Interviewee 5 also talked about having to weigh the value of likelihood against impact, and then make a decision of what kind of action needs to be taken, if any (ApF/01:08:58). A factor that can affect the likelihood and impact is for instance, that a solution for an attack exists, but that it is a very advanced one that only few can figure out how to implement, then there is a low risk that an incident will take place (ApF/01:11:44).

Interviewee 1 mentioned that the first step they take in risk management is essentially monitoring the environment. (ApB/00:05:37).

> Keeping up to date with current threats and development in this area, and then looking into our systems and seeing how the current threats could be applicable to us and then suggesting changes to our processes and systems. - Interviewee 1 (ApB/00:05:37)

Interviewee 3 describes a similar method of looking at what can happen and putting that in perspective for how to handle the risks (ApD/00:07:05). Mainly being concerned that there does not come any ransomware into their systems. Two of the interviewees, 2 and 4, said that they classify risks based on the CIA triad. Based on the classification made through those three perspectives (confidentiality, integrity and availability) they look at what protective measures they have or need to have (ApC/00:15:35). Interviewee 4 said that they then have certain legislations they implement, considering how important all of these aspects are for the trustworthiness of their company (ApE/00:04:52).

Furthermore, Interviewee 4 expressed that it is very important to know who the risk owner is (ApE/00:13:36). Usually, it is the head of IT when a risk has to do with IT, but privacy concerns or company-wide risks can sometimes be delegated to the CEO if it is serious enough (ApE/00:09:52, ApE/00:13:36). The interviewee accentuates that there needs to be a clear dialogue, in any case, so the risk owner is aware of their responsibility to ensure it gets handled (ApE/00:13:36).

When it comes to handling the risks, Interviewee 3 said that they prioritize prevention (ApD/00:41:14). Interviewee 1 also expressed that the most important thing to them in information security is "finding the correct level of risk mitigation" (ApB/00:04:55). The aim is to dampen the effects the risks can have. Interviewee 4 mentions that they have measures in place to automate information classification and that they encrypt data when it leaves their network of trusted devices (ApE/08:29). This helps with security as you take away easily avoidable risks. They also perform security training to raise security awareness amongst their employees, especially when handling incidents (ApE/00:17:34). Interviewee 3 also uses employee training, along with policy change, or technical solutions, or a combination, to mitigate risks (ApD/00:13:42).

In identifying risks Interviewee 1 explained that they have a reporting system (ApB/00:09:45). The reporting system works by creating tasks or issues, with a special category for risk-related issues. This way "if any employee sees something that they think could be a risk" they can flag it as a possible risk (ApB/00:09:45). Then they analyze the flagged risks depending on the type of report, and in some cases use external resources to see the risk and consequences (ApB/00:10:46). These external resources can include consultants, as well as services that perform checks and detect anomalies and threats in the systems (ApB/00:11:31). The advantage of these external resources is that they are aware of problems across different companies, so they can look at these aspects more closely, and they have specified resources for these purposes (ApB/00:11:31). The drawback is that a subscription is needed for these services, so "you need to have a company that can pay for it in order to access it" (ApB/00:11:31). Interviewee 5 also mentions that they even do vulnerability tests to find weaknesses in their systems that they can then work on securing (ApF/00:16:45). Similar to the reporting system, Interviewee 2 says that they have "responsible disclosure programs in IT" where they can inform of possible risks, and even "consumers and customers can reach out" (ApC/00:12:14).

When it comes down to realizing a risk, the interviewees seem unison in having detective controls in place at their companies. They have controls to detect if something out of character is happening in their systems, and then they try to figure out what they're trying to do in there (ApD/00:47:15). Interviewee 2 explains that once you identify a risk, and then detect an incident connected to that risk, they have an array of processes (APC/00:13:15). The interviewee says that they have a dedicated workforce for risks, but that when these risks turn into incidents then "it's in detection or response mode" (ApC/00:13:51). Interviewee 3 adds to this in general terms that they have ways to identify malicious actors in their network, and then they determine how serious the threat is, depending on if the malicious actor is in low vs high classified systems or information (ApD/00:21:18). Either way, they have means of identifying an intruder, knowing what they're doing, and then limiting their access. Once they limit these accesses they also check to see that the intruder "didn't leave anything behind" (ApD/00:47:15). This ensures that the intruder does not have an 'in' to the company systems and information. Interviewee 4 also explains a very similar process in their system. They start by logging and checking what type of attack has taken place, and what the intruder has done with or to the system (ApE/00:46:11). They can then deduce what the consequences of this intrusion are. Throughout this process, the company works to shut down the effect of the attack and restore the system. Having a segmented IT structure makes it more manageable to handle intrusions as the intruder does not have access to the whole IT environment at the initial breach, and they can therefore be shut out of the system quickly (ApE/00:47:33). Interviewee 5 describes how they have a SOC, Security Operations Center, that sits constantly looking at the logs they keep of the systems (ApF/00:44:04). The SOC has people working day and night to monitor the systems and look at the systems patterns, this way when an incident occurs they are there and can determine if immediate action needs to be taken, or if they can wait and delegate the task (ApF/00:46:21). An interesting aspect was that they make sure to have extra developers on call on Black Friday and around Christmas time, considering that the online shopping increases exponentially these days (ApF/00:46:21). Besides that, Interviewee 3 also explains that there are certain laws and procedures they must follow when it is, for example, GDPR related incidents (ApD/00:13:42). They do not have laws for other incidents but they do have plans on "how to handle that incident together with [their] infrastructure partner" (ApD/00:13:42).

Interviewee 5 also mentioned some interesting scanning techniques. He said that they do intelligence scans outside of their systems, including the dark web, on their company name, as

well as the bin numbers for their bank (ApF/00:18:41, ApF/00:22:25). This way they can see if there is anything suspicious about them out on the web, or if they have had any leaks. This allows them to counteract possible incidents and protect their consumers' information much faster than if they did not actively search for it.

Interviewee 5 said they have many controls that detect attacks early, therefore they have never had any intrusions that haven't been stopped by the controls. If someone sends a malicious email to the company, the system looks through the email to find suspicious information. Everything that is malicious is detected by the system and stopped from entering further into the company, which is very important for the company. it is a very expensive system and a lot of the company's resources are needed for it, but since the reality is that there are a lot of threats, it is needed.

4.7 GDPR

Overall, the companies interviewed were familiar with GDPR before its implementation, and when it was enforced companies had to adapt to the regulation and value privacy in a new way. Many companies were forced to modify their data gathering methods and policies to act in accordance with the regulation. GDPR has vastly affected how companies work with information security and digital security. One of the companies interviewed mentioned that "you often need a price tag on things in order to make them important, and GDPR is a big price tag" (ApB/00:24:26). Several of the companies interviewed mentioned that since there is now a fine attached to indiscretions with information handling, they have to work hard to assure that they follow GDPR.

Generally, the companies have different methods of controlling that they are in alignment with the requirements of the regulation. Interviewee 1 said they have yearly audits of their system to find faults and make sure that the processes are done correctly in line with the regulation (ApB/00:25:59). Processes have been adapted to make sure that the companies work accordingly with GDPR, thus the structuring of data in their systems has improved security wise.

Interviewee 2 acknowledged that "even when [GDPR] was released it wasn't clear what was expected", which meant that for companies it has been a continuous process to figure out how to work in accordance with GDPR (ApC/00:24:05). Most of the companies interviewed seemed to agree that the GDPR can be very vague, but also at times specific, making it hard to interpret. They say it is hard to be in complete alignment with the regulation since it depends on what data you are dealing with and in what situation. Interviewee 4 said that in terms of resources, GDPR has affected some parts of the work in having sufficient resources to implement all of the security controls needed to adhere to GDPR (ApE/00:25:30). He says this has been a necessity for the company to be able to continue working, but at the same time work accordingly with the GDPR .

According to the GDPR, the personal data gathered has to be necessary to the organization. The companies mentioned that they are aware of this in data collection, as they also have a lower burden if they do not have unnecessary information on their consumers. They also acknowledged that measures are taken to make sure the data gathered is not kept longer than necessary. Some companies used systems with automatic cleaning of information, that makes sure the information and data gathered is cleared as soon as possible.

Interviewee 5 said that their management system has different levels, the highest levels consist of policies from the board which are fuzzy, which is why they only need to look over these policies once a year to approve them. According to Interviewee 5 these policies are sweeping and it is enough that they express that the company has good information security. He says that there are, however, also documents such as instructions and manuals that they comply with, which consist of what the systems precisely have, and they can apparently be easily changed. He maintains that the company policies should be highest with an overall perspective, meanwhile the instructions are more detailed although still obscure. Furthermore, he states that it is important that all information in the polices, manuals, and instructions are correct and actually obeyed, as there is no point in filling out these documents if the company does not apply the management system. Interviewee 5 said it is much easier to write too much and get a nice document than to follow reality (ApF/01:15:55).

5 Discussion

Information security has become essential for companies to prioritize. This is because almost all companies today work with large quantities of data. Data that needs to be handled and stored in a secure way, that is why it is important to use security controls to help the companies prevent malicious attacks and threats. The value of controls, and the reason why companies use controls, is that they can be essential for the company to function nowadays. All companies use a form of security control, whether it is a person who looks for threats or if it is an integrated advanced control in the system.

The study conducted shows a present day analysis of what security controls companies most commonly use to handle and address security risks. The study shows that the companies interviewed use different security controls to prevent risks occurring and to protect their data, especially when it comes to the personal data that they handle. The security controls that they use are within management, operational and technical controls. By dividing the different methods and tools included in the study into the three perspectives, a better understanding of how companies can use the controls in different aspects of the organization was gained. Regarding e-commerce, Covid-19 has had varying effects on the different companies, leading to them having either more work, less work, or no change due to it. There has, however, been a big increase in e-commerce during the last few years. Kuruwitaarachchi et al. (2019) state that this change of culture has led to a great need for e-commerce security. As a consequence, companies have had to find different methods of working with development, and have had to adapt how they work internally, both in relation to organization as well as security.

During the interviews the participants spoke of the different security controls they use, and they mentioned why they are useful and in some cases necessary. Depending on the resources the company has, they can use different strategies for implementing the security controls. Strategies are needed to manage the organization and to help the organization achieve the goals they have set up for the organization. Strategies were used by the companies to help prevent risks from occurring and to help work with vulnerabilities to improve the companies' systems. The interviewees talked about all the different risks and threats the company can have, and that having strategies to respond to them is essential for both prevention as well as being able to continue working with the companies' operation. The companies have to have preventative and detective measures, such as controls, to stop malicious actors from entering the system and accessing the companies' information. In the following text the controls studied will be divided up into more and less commonly used controls, based on the interview studies.

5.1 Commonly used controls

Authorization and authentication showed to be controls mentioned by all interviewees. They are fundamental for companies to verify that a user entering the company's system is not an unauthorized person, as Anna et al. (2020) also mentions in their study. Therefore security controls are needed to prevent unauthorized access by having authorization controls, which is where a user has to authenticate that they are the aforementioned user. This can be done by using Bank-Id, a common tool for e-commerce companies, and some companies have adapted a two factor authentication as well, which entails the user proving their identity with two pieces of evidence. These methods of using multiple factor authentication have been shown to

be effective methods in protecting confidentiality (Anna et al. 2020; Cabric, 2015). Authorization and authentication is also crucial within the organizations to make sure only the authorized employees can see the relevant information and data to their operation. Depending on a person's clearance level, or allowances, they have limited access within systems due to access controls. The companies check what information the user wants to access, authenticate the user, see if they have the authorization to see the information and then grant or deny the user access to the system. This control is as highly talked about as it is, since it can be considered a core aspect of information security. Saracino (2020) states that it plays a critical role among security mechanisms in ensuring proper behaviour against potential threats at each level of a software system. Authorization is a primary safeguard against intruders, and there are many tools and programs that cater to this function. It is also a safeguard that most people are generally aware of, as it is used in many people's daily lives, albeit for smaller data collections. It is also a good first step to keeping intruders out considering that failed authentication attempts send off an alert in security systems, putting notice on the user.

Furthermore, as presented in the literature review, least privilege and separation of duties can be helpful to define who is allowed to see and edit within certain systems or databases. This can reduce the company's security risks since only authorized users with access can tamper with certain information. These access limitations were also frequently mentioned in the interviews. As Stallings and Brown (2018) also explain, they are effective measures to ensure that employees are not tinkering in systems outside of their work scope. What was especially interesting is that by having access controls in place for employees, it also limits an intruder's access. Due to limitations set on employees there are security measures in place to keep unauthorized people from certain systems or processes. These in turn also act as hinders for an intruder, because if they penetrate the system, they still need to get past many hurdles to infiltrate the more secure systems and databases. Saracino (2020) claims that these aspects can be controlled by an Access Control Policy, by adding a structure to the specifications and procedures necessary for the categorization of access requirements.

Continually, a way to monitor that only people with the correct allowances are in certain systems, is by logging. Logging is something that all companies do, and it is an effective method to check if the companies work in accordance with the goals and expectations they've set up. Chuvakin et al. (2013) mention that there are no real set standards in logging, and therefore they might sometimes miss certain factors if they are not set up properly. As a result of this openness of logging, the companies can choose what they want to log and what to save from the logs. Logs can be useful to discover where there are risks, vulnerabilities and improvements needed in the company's system. The companies can look through the logs and see if they need to change a specific process or system, which can be helpful as a preventative measure against future incidents. One company mentioned that they look through logs to find patterns, and when something sticks out the company has an alarm that detects this and lets the company know that something is wrong so they can change this. Logging can also help companies keep track of their employees, to see that they work only with what they're supposed to, and allowed to. For instance, if an employee goes outside their access level, some companies have controls in place that detect this and send off an alarm. This, as in logging, was discussed in most of the interviews, but some did not want to go into detail. Assumably it is used by all of the companies in some way, but most of them confirmed that they do log certain things. Mostly they log data from the systems, and then it is usually the more secure systems that they want to keep track of. Chauvakin et al. (2013) states the ideal logging scenario being with just two simple categories containing urgent and not urgent situations, and working through that. Similarly, the companies use it to detect anomalies, as mentioned earlier, and it helps keep track of what is happening and who is doing it in case of

an incident, but they do not keep it as simple as two categories of do and do not, although this is an initial storing they do. It also acts as a preventative measure as people are less inclined to do something malicious if they are likely to get caught.

Another way of detecting anomalies in the systems is through testing. Testing is used by all companies interviewed, each using multiple testing methods, some to look for weaknesses in the systems and some to check usability. According to Watkins and Mills (2011), testing is an essential tool to improve the company's systems, and that it performs as it should, which is also how the companies show to use testing. Depending on what phase of development a system is in, then different types of tests can be conducted. It can even be used to help with risks due to human error, especially in the development phase as it can check for errors in code in real-time. It is a way for companies to understand where there are vulnerabilities, and to then find strategies to prevent them from becoming harmful. Specifically, penetration testing was mentioned several times by the companies as an especially efficient, albeit expensive, method of testing a systems security. It simulates a cyberattack, and then you can see where more security needs to be added to lessen the risk of a breach. Chen et al. (2018) state that penetration testing tools are needed to complement defensive mechanisms, and that they are also in need of efftivising due to many resource limitations that arise in different testing scenarios. This is shown by the care that the companies studied use penetration testing, as they use them only when they feel they are needed, but that they are a strain on resources. Overall, testing has shown to be a very common control. This is logical because, unlike the other controls mentioned above, testing provides a more proactive approach to security since it looks for the risks and vulnerabilities before they become incidents.

When the interviewees were asked the question regarding a scenario of a breach in their data centers, they all said they have some form of contingency plan. However, this contingency plan was always used in the case of one server being down, but never all. When a system is down it entails the operation has to be stopped in the area where it was affected, this can be costly for the organization and spending on the resources the companies has to handle the crash. Most of the companies rely on backup servers in different locations, but if the backup is not constantly up to date with the main server then a lot of work is lost. This is why it's important for the companies to have a contingency plan or a management plan for handling such a situation. However, Mathew and Mai (2018) present that there are weaknesses in solutions such as data centers, servers and decentralised solutions, which the companies use, and that a contingency plan is a multifaceted measure that requires back-ups in physical and virtual forms. The interviewees all seemed to appreciate the value of back-ups, and it seemed to be quite a given, during the interviews, that they have them. This is understandable as not backing up data is a fault most people fall victim to, so it may seem obvious that companies have them too for their data, just in different forms in some cases. Liu et al. (2018) explains that these forms of back-up are dependent on the type of data stored as well as the companies' data storage structure.

In the study conducted, risk management was brought forward as a necessity for organizations to work with information security. The interviewees presented different ways of handling and managing risks depending on what risks can occur to the data they had, risk with the methods they used to process the data as well as risks that can arise when someone is handling the data. Berger, Shashidhar and Varol (2020) state, agreeingly, in their study how risk management is crucial to effectively handle risks. Risk management helps the companies work with information security in a safe way, too, especially since the companies work with sensitive data which has to be handled correctly. It is important the companies prioritize confidentiality, integrity and accessibility, also called the CIA triad, since the companies work with large

amounts of data within e-commerce. Cabric (2015) presents the CIA triad as a tool to combat fraud and preserve integrity, which is a large part of information security in e-commerce. The CIA triad can help classify the risks the companies have, which is critical since the companies work with many types of risks that need to be prioritized. Li and Li's (2020) presentation that information security risk analysis combined with information security risk awareness being the optimal way to assess risk and conduct risk management, is reflected in the companies studied. A common way of prioritizing showed to be by creating a risk matrix, where the possibility of a risk occurring and the impact of this occurrence are put against each other to determine how high level the risk is termed. Giving different levels to the threats leads to better management of the risks. The companies have preventive controls to avoid risks from taking place and to mitigate the possible effects, and they have response and recovery controls for when a risk becomes an incident and needs handling. Risk management includes controls that reduce the chances of an incident taking place, and this is the ultimate goal in security, to avoid incidents, which Stallings and Brown (2018) corroborate.

A big risk companies face is leakage of data. Considering that the companies all work within e-commerce, the data they store could be very sensitive and include personal information about customers. For companies to be able to work with data and handle it, they need to be aware of the relevant regulations that exist. Seeing as the study only included companies with at least some offices in the EU, GDPR was looked into. GDPR is a regulation that has helped form how companies work with information security, with a focus on the gathering and handling of private people's personal information. To respect GDPR, the companies in the study have all had to put new policies in place, which has increased the value, as well as level, of security in these systems. Although the GDPR law is extremely present in the companies' policies, it is mainly due to law and not their own choice. The companies all said they appreciated GDPR due to the raised awareness of security needs across the company, making employees outside of the security departments more respectful of the importance of secure protection of information. The regulations have increased awareness in companies, shedding more light on security, but it is not common in the same way other controls protect systems, while GDPR protects individuals.

Furthermore, there are standards that add to GDPR in regulating the practices within information security. The ISO standards are most common for organizations to use, confirmed by this study as some of the companies claim to use ISO standards since they help achieve good information security. Eriksson (2016) specifies that the 27000-series is especially good for risk management within companies, while SIS (n.d.) values ISO 9001 which focuses on quality. Both of these standards are used by the companies which shows that ISO is a valuable tool to control standards within the company. Additionally, most companies use PCI DSS, which ensures that the employees are qualified and certified to work with card transactions and data. Yulianto, Lim and Soewito (2016) show that it is an important tool in ensuring quality and reliability in card processors. The companies use it to define the weaknesses within the organizations and perform safe sales transactions, which is essential within e-commerce. All of the companies do most likely use PCI DSS, since it is basically required to work with card transactions, but one of the interviewees did not specify the standard in their interview.

5.2 Less commonly used controls

Along with testing there is also auditing to check that everything is as it should be. The companies have audits conducted to see that they have the proper controls in place for common vulnerabilities. Petterson (2005) claims that these audits also ensure they are following all standards that are required of them. Although the CSI survey from 2011 shows that audits are one of the most common security controls, not all of the interviewees mentioned that they do them. Three of the interviewees said that they conduct audits, and presumably the other two do, too. However, since these two did not mention it in the interviews it is also possibly a sign that, although they may conduct them, it is not a control they consider to be as vital as other security controls. Be that as it may, the interviewees were not explicitly asked about auditing so auditing may actually be more important than perceived, as Petersson (2005) and Herath and Herath (2014) both state that audits are a very good tool to evaluate the effectiveness of a system.

Similarly, there is the four-eyes principle, which some companies employ as a double check policy to make sure activities are being done correctly. It denotes that a second person has to look at a product before it is implemented. Bodenschatz and Irlenbusch (2019) present that this can reduce human-related errors and keep employees from conducting malicious activity, since there is another person looking over your shoulder. This method was only mentioned by one of the interviewees, so it is assumed that it is not the most common security control, or at least not considered the most integral. The one interviewee said it was a common practice at their company, however, and that it decreases the chances of malpractice or errors. Osaci et al. (2018) mention that this principle is implemented to achieve top-level security, and is usually an additional control for higher security, so it follows that it wasn't mentioned by most companies considering it is seen as an extra detail rather than a crucial control for security. Like with testing, the interviewees were not asked explicitly about the four-eyes method, so it may be that they all use it, but due to the lack of mention it is deemed as less integral as a security control.

The companies differed when it came to the set up, or structure, of their IT environment. They either store data in the cloud, on local servers, or both. Two interviewees expressed a hybrid solution in their organizations. Since the companies are very big, this solution means that they have to be able to store and secure data internally, but also on the cloud. The cloud can be helpful for the companies to use since they need to store and process big chunks of data which can be demanding on the in-house servers, and therefore using the cloud can reduce the capacity needed within the company to store the data. One of the interviewees mentioned that their company uses SaaS solutions. They were the only one who said they use this along with their hybrid solution of on-premise and cloud storage. Liu et al. (2018) state that although SaaS has good features for providing secure systems, there are still weaknesses in the fact that with simple login methods it can be difficult to authorize the proper user of the system. The fact that the companies have such varying structures for data storage is intriguing because it shows that one solution does not suit all. Presumably, companies would have similar data storing structures because they have similar security concerns, but this argument falls apart in the detail that they are just similar organizations and not the same. The needs of each company are unique, and their internal organizational structure is also individual; and although there are arguments for and against each data storage solution, the companies have to evaluate what suits them best. Therefore, the companies logically have their own hybrid solutions or solely cloud or on-premise.

Moreover, zero-trust was only mentioned by one interviewee. This was, yet again, maybe due to the open questions placed, and not that the other companies do not implement it. Nevertheless, the interviewee who mentioned it only spoke briefly on the matter as a way to explain that networks need to be secure. Considering that Ahmed et al. (2020) states that it is a strong defensive technique, implementing the theory that you do not trust an entity until it is proven trustworthy, it would be a valuable tool to have in a company to secure the networks. Zero-trust is a concept that is quite prevalent in literature so it is slightly surprising that it did not come up in other interviews as a security control for their networks. However, considering companies have most of their employees working remotely due to Covid-19, this is a hefty process of entrusting outside networks to link to the company network.

Considering the risks prevalent in systems, CVE lists can help gather common risks across several companies and combine them in a common database, where it is easy for the companies to find what risks and malicious attacks have occurred. If a company is exposed to a malicious attack and they find out that others have been exposed to the same attack, they can help each other by informing how they handled this situation and sharing it. This can also help companies prevent attacks from happening by putting controls in place that work against the risks and attacks, as preventative measures. Blinowski and Piotrowski (2020) claim the CVE list is one of the most commonly used sources for companies to help each other against attacks, but it was only mentioned by two companies. It is therefore considered a less commonly used control. It is always there for the companies to use, but it is only used and looked at in certain situations, which hopefully do not arise very often.

6 Conclusion

The purpose of this research paper was to explore security controls in e-commerce security systems. In the face of the current boom in online shopping, what security controls do e-commerce companies most commonly use to handle information and address security risks? Although not all of the companies interviewed had experienced an increase of sales due to Covid-19, they have all had to adapt to different work conditions than normal. Despite this, most companies have experienced positive revenue effects from the ongoing e-commerce boom. This entails them having to adapt how they work with handling information in a secure way, as many more demands are being put on them by their consumers.

Some of the controls seemed to be much more prevalent compared to others. Access and authorization controls are implemented at all companies, and it seemed to be one of the main methods of avoiding problems from within the company, while also making it hard for intruders to navigate the systems. Additionally detective controls such as scanning, logging, and testing within the systems leads to, optimally, risk avoidance. If not risk avoidance, then the companies can take measures to mitigate the risk, or at least handle it as best they can under the circumstances. Through the use of policies and standards the companies can easily abide by external requirements set on them, and also implement best practice for general work. PCI DSS is used by most of the companies to ensure safe transactions are made, considering they're in the business of e-commerce. Furthermore, all of the companies mentioned having the CIA triad as a basis for their systems. It is the CIA triad that ensures security is being kept. Beyond this, all companies have to follow GDPR which dictates how the companies work with the personal data gathered, and governs how companies work with security regarding personal data.

On the other hand, some of the controls were not very prevalent across the companies. Some companies used audits to check that security controls operated in the intended way, which is a common method to implement according to literature, but didn't seem to be very big amongst the interviewees. Additionally, the four-eyes method was mentioned by a company as a useful control to reduce human-related errors, which is probably put in practice more often than realized. Furthermore, the companies differed when it came to the set up, or structure, of their IT environment. They either store data in the cloud, on local servers, or both. Their differing views on the data storage solution stemmed from opinions on what is most secure. The concern of network security also arises as a difference across the companies as only one company mentioned implementing a zero-trust method. Likewise, using a CVE list, or similar, as a control to stay up to date with the general security environment across the world, was only mentioned by two interviewees. These less common controls are deemed so based on how important they seemed to the interviewees when they were mentioned, and also how many of the companies brought them up. It is important to note that they may be more common than interpreted since the companies were not asked about them by name.

In e-commerce there are many controls that can be implemented, but the most common ones stem in the purpose of knowing what data there is to protect, and to keep unauthorized people from tampering with it. A combination of several controls ultimately results in a well rounded security system. Any one control on their own would have weaknesses, however some provide more security than others.

6.1 Future research

There are a multitude of security controls that can be implemented in information systems, and further research on this would be very interesting. For instance, a more thorough and detailed study could present valuable information for the field of informatics. An aspect that would be intriguing to explore is how security controls are used and why, rather than the commonality. With a deeper understanding of the reasoning and connection between the controls, a proposal of best use could be created. As well as this, some of the controls were presumed to not be common due to their lack of mention, but more detailed questions could lead to different results, which would be interesting to examine. After the study it was also found that there are many controls that companies implement. A future study could consider conducting a deep dive into a single company in order to avoid getting a superficial understanding of security control usage. Likewise, only studying one type of control across several companies can provide an extensive and comprehensive study of that control. Beyond this, future research can benefit from investigating more companies and employees working with security, to get a broader perspective.

7 References

Adshead, A. (2021). 'Data Lake Storage: Cloud Vs On-premise Data Lakes: What type of storage do you need to build a data lake on, and what are the pros and cons of on-premise vs the cloud?', *Computer Weekly*, pp. 29–33. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 8 May 2021]

Ahmed, I., Nahar, T., Urmi, S. S., and Abu Taher, K. (2020). 'Protection of Sensitive Data in Zero Trust Model', *Computing Advancements*. (ACM International Conference Proceeding Series), pp. 1–5. doi: 10.1145/3377049.3377114.

Alvehus, J. (2013). *Skriva uppsats med kvalitativ metod.* trans. N Engberg. Stockholm: Liber.

Anna, K., Olena, K., Mykhailo, K., Svitlana, K., Olena, S., and Rostyslav, Z. (2020). 'Methods of Security Authentication and Authorization into Informationals Systems', *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Advanced Trends in Information Theory (ATIT),2020 IEEE 2nd International Conference on*, pp. 270–274. doi: 10.1109/ATIT50783.2020.9349333.

Badotra, S. and Sundas, A. (2020). 'A systematic review on security of E-commerce systems', *International Journal of Applied Science and Engineering*, [online] 18(2). Available at: <https://gigvvy.com/journals/ijase/articles/ijase-202106-18-2-010.pdf> [Accessed 17 May 2021].

Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, *NIST Cybersecurity Framework*, doi: 10.6028/NIST.CSWP.04162018, Available at: <https://www.nist.gov/cyberframework> [Accessed May 17, 2021].

Berger, D., Shashidhar, N. and Varol, C. (2020). 'Using ITIL 4 in Security Management', *2020 8th International Symposium on Digital Forensics and Security (ISDFS), Digital Forensics and Security (ISDFS), 2020 8th International Symposium on*, pp. 1–6. doi: 10.1109/ISDFS49300.2020.9116257.

Blinowski, G. J. and Piotrowski, P. (2020). 'CVE based classification of vulnerable IoT systems'. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 8 May 2021]

Bodenschatz, A. and Irlenbusch, B. (2019). 'Do two bribe less than one? - An experimental study on the four-eyes-principle', *Applied Economics Letters*, 26(3), pp. 191–195. doi: 10.1080/13504851.2018.1456644.

Cabric, M. (2015). Confidentiality, Integrity, and Availability. *Corporate Security Management : Challenges, Risks, and Strategies. [e-book]*. Elsevier Science. pp.185-200. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 14 May 2021]

Chen, C.-K., Zhang, Z.-K., Lee, S.-H., and Shieh, S. (2018). 'Penetration Testing in the IoT Age', *Computer*, 51(4), pp. 82–85. doi: 10.1109/MC.2018.2141033.

Chuvakin, A., Moulder, P., Phillips, C., Phillips, C., Schmidt, K., Schmidt, K. J., and Schmidt, K. J. (2013). *Logging and Log Management. [e-book]*. Syngress. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 7 May 2021]

Creswell, J. (2013). *Qualitative inquiry and research design*. 3rd ed. Thousand Oaks: SAGE Publications.

CROS - European Commission. (2019). *Four eyes principle*. [online] Available at: <https://ec.europa.eu/eurostat/cros/content/four-eyes-principle_en> [Accessed 12 May 2021].

Crossler, R. E. (2010). 'Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data', *2010 43rd Hawaii International Conference on System*

Sciences, System Sciences (HICSS), 2010 43rd Hawaii International Conference on, pp. 1–10. doi: 10.1109/HICSS.2010.311.

Crume, J. (2000). *Inside Internet security*. Harlow: Addison-Wesley.

CSI. (2011). 'CSI Computer Crime and Security Survey', *Computer Security Institute*, pp. 1-42.

Dhillon, G. (2007). *Principles of information systems security: text and cases*. Danvers, Mass.: Wiley.

Eriksson, C.-H. (2016). 'Standardiserad informationssäkerhet inom systemutveckling : En pragmatisk metod för uppehållande av en hög standard med ramverket ISO 27000'. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 7 May 2021]

European Commission. (n.d.a) *Data protection in the EU.* [online] Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en> [Accessed 12 May 2021].

European Commission. (n.d.b). *What is a data breach and what do we have to do in case of a data breach?*. [online] Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en> [Accessed 12 May 2021].

Feher, D. J. and Sandor, B. (2019). 'Cloud SaaS Security Issues and Challenges', *2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI), Applied Computational Intelligence and Informatics (SACI), 2019 IEEE 13th International Symposium on*, pp. 000131–000134. doi: 10.1109/SACI46893.2019.9111529.

ForSea Ferries. (2021). *About ForSea*. [online] Available at: <https://www.forseaferries.com/about-forsea/> [Accessed 4 May 2021].

Fusilier, M. and Penrod, C. (2009). 'e-Crime Prevention: An Investigation of the Preparation of e-Commerce Professionals', *Journal of Internet Commerce*, 8(1/2), pp. 2–22. doi: 10.1080/15332860903341281.

Galhotra, B. and Dewan, A. (2020). 'Impact of COVID-19 on digital platforms and change in E-commerce shopping trends', *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020 Fourth International Conference on*, pp. 861–866. doi: 10.1109/I-SMAC49090.2020.9243379.

Ganesh, K., Mohapatra, S., Anbuudayasankar, S. P., and Sivakumar, P. (2014). 'User Acceptance Test', *Enterprise Resource Planning*, pp. 123–127. doi: 10.1007/978-3-319-05927-3_9

Gartner. (n.d.). '*Definition of CIRT (Cyber Incident Response Team) - Gartner Information Technology Glossary*', [online] Available at: <https://www.gartner.com/en/information-technology/glossary/cirt-cyber-incident-response-team> [Accessed 12 May 2021].

Gauravaram, P., Kelsey, J., Knudsen, J., and Thomsen, S. (2010). 'On hash functions using checksums', *International Journal of Information Security,* 9(2), pp. 137–151. doi: 10.1007/s10207-009-0100-7.

Gehling, B., and Stankard, D. (2005). 'eCommerce security', Information security curriculum development. (Information security curriculum development), pp. 32–37. doi: 10.1145/1107622.1107631.

Hajny, J., Dzurenda, P., Marques, R. C., and Malina, L. (2020). 'Cryptographic Protocols for Confidentiality, Authenticity and Privacy on Constrained Devices'. doi: 10.1109/ICUMT51630.2020.9222243.

Herath, H. S. B. and Herath, T. C. (2014). 'IT security auditing: a performance evaluation decision model', *Decision Support Systems*, 57, pp. 54–63. doi: 10.1016/j.dss.2013.07.010.

Hussain, M. (2013). A Study of Information Security in E- Commerce Applications. *International Journal of Computer Engineering Science (IJCES)*, [online] 3(3). Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.860.2205&rep=rep1&type=pdf> [Accessed 18 May 2021].

IBM Cloud Education. (2019). *What are Security Controls?*. [online] Ibm.com. Available at: <https://www.ibm.com/cloud/learn/security-controls> [Accessed 22 March 2021].

ICA. (2020). *Ica- gruppen i korthet*. [online] Available at: <https://www.icagruppen.se/om-ica-gruppen/start/ica-gruppen-i-korthet/> [Accessed 4 May 2021].

IMY (2021). *Introduktion till dataskyddsförordningen*. [online] Available at: <https://www.imy.se/privatperson/dataskydd/introduktion-till-gdpr/> [Accessed 4 May 2021].

ISO. (n.d.). *ISO and small & medium enterprises.* [online] Available at: <https://www.iso.org/iso-and-smes.html> [Accessed 3 May 2021].

Ji, Q. (2018). Study on Information Security Issues of E-Commerce. *IOP Conference Series: Materials Science and Engineering*. 452. 032050. 10.1088/1757-899X/452/3/032050.

Johansson, S., Kullström, M., Björk, J., Karlsson, A. and Nilsson, S. (2021). 'Digital production innovation projects – The applicability of managerial controls under high levels of complexity and uncertainty', *Journal of Manufacturing Technology Management*, 32(3), pp. 772–794. doi: 10.1108/JMTM-04-2019-0145.

Kurd, A. and Besli, N. (2020). 'Analysis of the Cryptography Methods for Design of Crypto-Processor'. doi: 10.1109/HORA49412.2020.9152929.

Kuruwitaarachchi, N., Abeygunaward, P. K. W., Rupasingha, L., & Udara, S. W. I. (2019). A Systematic Review of Security in Electronic Commerce-Threats and Frameworks. *Global Journal of Computer Science and Technology*.

Li, Y. and Li, J. (2020). 'Risk Management of E-Commerce Security in Cloud Computing Environment', *2020 12th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Measuring Technology and Mechatronics Automation (ICMTMA), 2020 12th International Conference on*, pp. 787–790. doi: 10.1109/ICMTMA50254.2020.00172.

Liu, J., Yuan, C., Lai, Y. and Qin, H. (2020). 'Protection of Sensitive Data in Industrial Internet Based on Three-Layer Local/Fog/Cloud Storage', *Security and Communication Networks*, 2020. doi: 10.1155/2020/2017930.

Liu, S., Yue, K., Yang, H., Liu, L., Duan, X. and Guo, T. (2018). 'The Research on SaaS Model Based on Cloud Computing', *2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), 2018 2nd IEEE*, pp. 1959–1962. doi: 10.1109/IMCEC.2018.8469462.

Mathew, A. and Mai, C. (2018). 'Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison', *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2018 3rd IEEE International Conference on*, pp. 2021–2024. doi: 10.1109/RTEICT42901.2018.9012485.

Meylan, A., Cherubini, M., Chapuis, B., Humbert, M., Bilogrevic, I. and Huguenin K. (2021). 'A Study on the Use of Checksums for Integrity Verification of Web Downloads', *ACM Transactions on Privacy & Security*, 24(1), p. 4–4:36. doi: 10.1145/3410154

NIST. (2020). *Standards & Measurements*. [online] Available at: <https://www.nist.gov/standards-and-measurements> [Accessed 3 May 2021].

Osaci, M., Cristea, A. D., Ghiuzan, D., and Berdie, D. A. (2018). 'Sap Authorization Based on the Four Eyes Principle', *Annals of the Faculty of Engineering Hunedoara - International Journal of Engineering*, 16(2), pp. 43–46. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 12 May 2021].

Petterson, M. (2005). 'The keys to effective IT auditing', *The Journal of Corporate Accounting & Finance*, pp. 41-46. doi: 10.1002/jcaf.20134

Postnord, Svensk Digital Handel, and HUI Research. (2020). *E-barometern 2020 Årsrapport*. [online] Available at: <https://www.postnord.se/vara-losningar/e-handel/e-handelsrapporter/e-barometern> [Accessed 4 May 2021].

Rubin, H. and Rubin, I. (2012). Structure of the Responsive Interview, *Qualitative interviewing: The Art of Hearing Data*. SAGE Publications, pp.115-130.

Sangeetha, M. K. and Suchitra, R. (2016). The Study of E-Commerce Security Issues and Solutions, *International Journal Of Engineering Research & Technology (Ijert) Ncrit – 2016* (Volume 4 – Issue 27)

Saracino. (2020). *Emerging Technologies for Authorization and Authentication. [e-book]*. Springer International Publishing. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 7 May 2021]

Shen, L. (2014). 'The Nist Cybersecurity Framework: Overview and Potential Impacts', *Journal of Internet Law*, 18(6), pp. 3–6. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed: 17 May 2021]

Simmon, E. (2018). 'Evaluation of Cloud Computing Services Based on NIST SP 800-145', *NIST Spec. Publ*, vol. 500, pp. 322. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf >[Accessed 4 May 2021]

Sindhuja, P.N. and Kunnathur, A.S. (2015). 'Information security in supply chains: a management control perspective', *Information & Computer Security*, 23(5), pp. 476–496. doi: 10.1108/ICS-07-2014-0050.

SIS. (n.d.). *Standardutveckling: ISO, International Organization for Standardization*. [online] Available at: <https://www.sis.se/standardutveckling/internationell-standardisering/iso/> [Accessed 3 May 2021].

Stallings, W., and Brown, L. (2018). *Computer Security: Principles and Practice*. 4th Ed, Global Ed. Pearson Education Limited, Harlow, United Kingdom.

SveaEkonomi. (2021). *Om Svea Ekonomi*. [online] Available at: <https://www.svea.com/se/sv/om-oss/svea-ekonomi/> [Accessed 4 May 2021].

Timmermans, S. and Tavory, I. (2012). 'Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis', *Sociological Theory*, 30(3), pp. 167–186. doi: 10.1177/0735275112457914.

Watkins, J. and Mills, S. (2011) *Testing IT. An off-the-shelf software testing process. [e-book]*. 2. ed. Cambridge University Press. Available through: LUSEM Library website http://www.lusem.lu.se/library [Accessed 14 May 2021].

Xie, T., de Halleux, J., Tillmann, N. and Schulte, W. (2010). 'Teaching and training developer-testing techniques and tool support', *Object oriented programming systems languages and applications companion*. (Conference on Object Oriented

Programming Systems Languages and Applications), pp. 175–182. doi: 10.1145/1869542.1869570.

Yulianto, S., Lim, C. and Soewito, B. (2016). 'Information security maturity model: A best practice driven approach to PCI DSS compliance', *Proceedings - 2016 IEEE Region 10 Symposium, TENSYMP 2016*, pp. 65–70. doi: 10.1109/TENCONSpring.2016.7519379.

Zhiyong, S., Ji, X., Tang, H., You, W. and Liu, Z. (2018). 'Research on Backup Method of Service Function Chain Based on Security Classification', *2018 IEEE 18th International Conference on Communication Technology (ICCT), Communication Technology (ICCT), 2018 IEEE 18th International Conference on*, pp. 1109–1114. doi: 10.1109/ICCT.2018.8599990.

Zwass, V. (2016). *Information system - Information systems audit*. [online] Encyclopedia Britannica. Available at: <https://www.britannica.com/topic/information-system/Information-systems-audit> [Accessed 6 May 2021].

Appendix A - Interview Outline

1. Questions of Consent
    - 1.1. May we record this interview, and then later transcribe it?
    - 1.2. Do you wish to be anonymous, or may we refer to your name, role, and/or company in our thesis paper?
    - 1.3. Do you understand and accept that:
        - 1.3.1. the information gathered in this interview will only be used in regards to this thesis study.
        - 1.3.2. you may choose to stop the interview at any time.
        - 1.3.3. If you wish, we will send our findings and final report when it is done.
2. Opening Questions
    - 2.1. Where do you work? What does the company do?
        - 2.1.1. How many employees?
    - 2.2. What is your role in the organization?
    - 2.3. What does your IT environment look like?
        - 2.3.1. Where is information stored? Local vs cloud
        - 2.3.2. All in house? Anything outsourced?
    - 2.4. What do you think is most important in information security?
    - 2.5. Have your sales been affected by Covid-19? Has this affected your work in information security?
3. Managerial Controls
    - 3.1. How do you categorize risks? What does your company value as high-level vs low-level threats? Can you give examples?
    - 3.2. What process do you have in response to risks?
        - 3.2.1. (accept, avoid, mitigate, share) depending on level
        - 3.2.2. Have a cirt? (computer security incident response team)
    - 3.3. In handling people's private information, do you feel there are more security concerns in comparison to other confidential data in the company?
    - 3.4. Do you have a strategy for handling and countering an attack on your service or application? If so, what is your strategy?
    - 3.5. What methods are in place to discover if there has been a breach or if someone has accessed information/data they are not authorized to see?
    - 3.6. Do you have to follow any defined security standards? If so, which standards? (ie ISO, IEC, PCI DSS)
    - 3.7. Does the company require you to work from a secure VPN?
    - 3.8. Are there policies regarding BYOD (bring your own device)?
    - 3.9. GDPR
        - 3.9.1. How has GDPR affected your work with information security?
            - 3.9.1.1. How have you adapted to the implementation?
        - 3.9.2. Do you have any authorization controls that limit who can access personal data? How is this set up and who administers it?
            - 3.9.2.1. Authentication of users?
        - 3.9.3. What routines, if any, are used to make sure the data that is gathered is necessary?
4. Operational Controls
    - 4.1. How is your security system managed? Do you have a set security system that is maintained or do you actively update and change it?
        - 4.1.1. Periodically check controls for relevance and intended functionality?

4.2. How do you limit human errors in the development of the systems?
  4.2.1. Least privilege
  4.2.2. Separation of duties
4.3. Does the company keep a log of each employee's activities?
4.4. Have you experienced that data or information that you work with has not been available?
  4.4.1. If so, what was not available and how long did it last?
  4.4.2. How did you handle or should you handle such a situation?
4.5. How do you allocate the resources in your department?
  4.5.1. Where do you invest?
  4.5.2. Tools vs employees
  4.5.3. Prevention vs recovery
  4.5.4. Compromises?

5. Technical Controls
5.1. What measures, if any, are in place to protect the confidentiality, authenticity, and/or integrity of information? (ie cryptography, etc)
5.2. Do you have controls to detect anomalies such as data loss or tampering? If so, what?
5.3. Do you have controls to detect discrepancies in the use of your system? (i.e. unusual access or unknown locations) If so, what?
5.4. What happens in the case of a systemwide crash, or mistaken delete of an important part of the system?
  5.4.1. Is there a worst-case scenario?
  5.4.2. Do you have continuous backups?
  5.4.3. Contingency plan?
5.5. If your service or application would have an intrusion by an unauthorized person, what preventative measures do you have in place? What detection and recovery controls are implemented in case the intrusion bypasses the preventative measures?

6. Closing Questions
6.1. Overall, are there any aspects of security that are unique to e-commerce businesses?
  6.1.1. Special considerations?
  6.1.2. Different threats?
6.2. Can we contact you if there is anything we would like to clarify?

Appendix B - Interview Transcript 1

00:00:02 Interviewer
Do you wish to be anonymous or is it okay if we refer to your name and role and the company in our thesis?
00:00:20 Interviewee
Yes, I've been looking at your questions and I'm not going to be able to give thorough answers on some of them because of security. I don't think that would change even if I could be anonymous. So, let's not be that.
00:00:48 Interviewer
Do you understand and accept that the information gathered in this interview will be used regarding our thesis study and you may choose to stop the interview at any time you want. And, if you wish, we can also send you the findings from our thesis report when it's done.
00:01:07 Interviewee
Yeah, that sounds interesting.
00:01:11 Interviewer
Where do you work? And what does the company do and how big is the company?
00:01:20 Interviewee
I work at Svea Ekonomi, which is a big FinTech company with many branches and I'm not going to describe everything that we do, but I'm part of the web-based payment business area, we call ourselves web pay internally. So, we are having e-commerce merchants as our customers, and we help them with the payment facilitation on their e-commerce sites. I'm the solution architect for this business area.
00:02:22 Interviewer
What does that entail?
00:02:24 Interviewee
That is about orchestrating how the development is being done and so in this business area. The web-based payment and we consist of seven teams which are working on different services that all together form this business area and each of the systems has their product owners that are driving development for their systems, but my work is to look at the whole and how development is going and what we will be changing in the future.
This business area has been active since 2008. We have had software since 2008 and some of it is new and some of it is old, and doing the changes needs coordination and that is my responsibility. We have architects on different levels, so there is an enterprise architect for the whole of Svea. I am the solution architect for these systems within the web pay business area, and then there are software architects in each of the teams.
00:04:03 Interviewer
What does the IT environment look like when you work? Is the information stored in the cloud or is it local?
00:04:18 Interviewee
I mean this is different for different companies in this sector, but we have nothing in the cloud. So, we have our own environment. I think it's one of the questions a bit further down, and so I can talk a little bit about that.
00:04:41 Interviewer
What do you think is most important when you're working with information security?
00:04:55 Interviewee
I think that it is finding the correct level of risk mitigation. If I was to try to mitigate all risks, it would be expensive, and if I wasn't trying to mitigate any risks, we would be really having problems and finding the correct level. That's really the most important thing for me.

00:05:26 Interviewer
How do you work with mitigating risk, what is your process?
00:05:37 Interviewee
Well, I wish that I had a process, but it basically consists of "omvärldsbevakning". Keeping up to date with current threats and development in this area, and then looking into our systems and seeing how the current threats could be applicable to us and then suggesting changes to our processes and systems.
00:06:17 Interviewer
E-commerce has been affected by COVID-19, has this affected your work with information security?
00:06:30 Interviewee
It has affected sales. We have a huge increase in sales because so much of the market, I mean people have changed to ordering on the net. So, we see that all our merchants have increased volumes, and that, of course, means that it hasn't really affected my work when it comes to information security, though, because that's just the volumes and you still must do the same work whether you have large or small volumes.
00:07:11 Interviewer
What do you do when you work with risks? Does the company have different levels for categorizing them and threats?
00:07:29 Interviewee
Yes, but unfortunately, I don't think that I'm the best one to describe that because we have people who are working more with risks. When it comes to hacking threats and similar then I don't have a categorization. So, it's more like a sliding scale. Perhaps I could give you another name. I don't know if he has the possibility to be interviewed, but it could probably be interesting for you to interview another person who is more on the low-level security parts. I'm not working a lot with the actual operations but more designing the systems and the future systems and then the people who are working with the operations are seeing risks differently than I do.
00:09:13 Interviewer
That would be great. Then we will go to the next question, do you have processes in response to risk?
00:09:45 Interviewee
Yeah, we have a system for creating tasks or issues, and there we have a special category for risk-related issues. So, if we have if any employee sees something that they think could be a risk, they have a system where they can just create a ticket and say that this could be a risk. It's the department that I was mentioning that will be taking those tickets and starting the process of analyzing them. So, I could possibly be the one reporting something to that system.
00:10:37 Interviewer
When you report, how does that process work?
00:10:46 Interviewee
Yes, they will probably handle it differently depending on the type of report and start analyzing it and they have a lot of external resources that they can use to gather and see the risk and the consequences of what has been reported. But that's not really my part of the work.
00:11:22 Interviewer
What did you mean by external resources?
00:11:31 Interviewee
I mean technology today is so complex and there are so many different things to know and so sometimes we bring in consultants, helping us with analyzing the threats. There are also services that you could subscribe to where you can check things. So, if you see something

strange in your systems, you can search for them in these databases and see if you get a match and if someone else has seen the same thing previously.
The threat actors today are global and many of them are professional. To work against them you need to be cooperating as well, so setting a company setting up services like this is helpful because then you can see the malicious code that we saw last week has been seen around the world in different countries in the last year perhaps and you can see what the effects have been in other places, etc.
The problem is that you need a subscription for most of these services, at least, because there are companies that have people who are good at describing this. So, they take in the reports, and they write articles about it, and so you need to have a company that can pay for it in order to access it.

00:13:55 Interviewer
When you are handling people's private information, do you feel there are more security concerns in comparison to other confidential data in the company?

00:14:09 Interviewee
No, I don't think so. If you look in the past, you will probably feel like most companies weren't very interested in keeping people's private information secure, but this has changed with GDPR. So yeah, today I would say that we value them quite equally.

00:14:42 Interviewer
Do you have a strategy for handling and countering attacks on your service or application, and if so, what is the strategy?

00:14:52 Interviewee
This is where I must be a bit, well, secretive and so yes, there are several strategies. I mean there are ways of monitoring the systems. We have people monitoring the systems 24 hours a day, and we have a lot of logging and ways of finding anomalies in the logs. That's basically as far as I can say.

00:15:41 Interviewer
What methods are in place to discover if there has been a breach or if someone has accessed information or data that they are not authorized to see?

00:15:53 Interviewee
As I said, we have a lot of logging and there might be other ways too that I can't disclose.

00:16:05 Interviewer
Do you have any defined security standards? If so, which standards?

00:16:13 Interviewee
Yeah, I should really know this by heart. But yes, PCI DSS, where you need to certify your developers, so the card payment systems you're not allowed to work on them if you're not PCI certified. And it's called PSD 2, Payment Services Directive. It's a big thing too, and I mean if you look at the company, there are lots more, a lot more standards, but these are the ones that are most important to me, I'd say.

00:16:58 Interviewer
Does the company require you to work from a secure VPN?

00:17:18 Interviewee
If you work from home, yes. I would say that we are like many companies during the pandemic, and we have been a bit reluctant to have people working from home and in our case, it has been from a security standpoint mostly, but since we had to switch to that we have seen that we can make it work.

00:17:42 Interviewer
Have there been any big struggles with working from home?

00:17:57 Interviewee
Not big struggles, a lot of small struggles. I would say I mean getting the technology to work.

And so, I mean you have VPN but when suddenly the entire company started using it. We had problems with the performance and then after buying more hardware that started working. I think we still have a problem that everybody needs to have a good workplace and when you're working from home, it's often not very ergonomic. We haven't really started addressing that much yet, but from a security standpoint, I think that we feel that we have everything we need. Basically, some people were already doing it before the pandemic, so the only thing we needed to do was roll out that solution to everyone, so we already had something that was analyzed and deemed secure. There are rules about not having any copies of the software in your local computer at home, for instance, so we're remoting into computers inside the company and then all the software that we're working on is there.

00:19:41 Interviewer
Do you have any policies regarding bring your own device (BYOB)?

00:19:50 Interviewee
Yes, there is an open Wi-Fi network, and that's the only one that you're allowed to connect your own devices to and then we have several networks for the company devices depending on what they are used for. But basically, you are allowed to bring your own device, but you're only allowed to connect it using the open network.

00:20:29 Interviewer
So, you're not allowed to do any work on your own device?

00:20:38 Interviewee
Well, you are allowed to do work stuff, but you're not allowed to have any information that could be deemed sensitive. So that means if you, for instance, have people reporting to you and you are doing things like workshops and stuff, you can have plans like planning the workshops, etc. So, there's a lot of work that is not sensitive and that you can do on your own device if you need to. And this also goes when we're talking about cloud services, we're not using cloud services for anything sensitive. But when you're doing stuff like workshops or meetings, it's good to have these cloud services for putting post-it's on the wall and shared whiteboards, etc. We do that, but we're only allowed to do that for information that is not sensitive. So, like, how do we plan the work? Will you be working on feature A, and you will be working on feature B? That's stuff that perhaps you could be planning like on your own device or in the cloud. But anything describing the code or the actual systems interconnections you wouldn't.

00:22:04 Interviewer
Does it feel obvious what is considered sensitive and not sensitive?

00:22:10 Interviewee
No, so that's something that we're struggling a bit with. You find yourself starting a discussion that is not sensitive and then suddenly you realize that, okay we can't continue this discussion, because we are now like in an open forum, and we need to log on to the VPN and go inside in order to be able to continue the discussion. It's quite cumbersome, but that's the way we must do it.

00:22:43 Interviewer
Do you have any policies that you can follow if you want to know where the line goes between sensitive and not sensitive information? Or do you go from, as you said, now we must change to the work device instead?

00:23:07 Interviewee
We haven't published any clear policies about that. We need to work on it.

00:23:16 Interviewer
Then we ask a bit more about the GDPR. How has GDPR affected your work with information security? Have you had to adapt after the implementation?

00:23:32 Interviewee

Yeah, so I think that as most companies we have known about the GDPR for a long time and once it started to be enforced a couple of years ago, suddenly we had to prioritize it. So that means that for people like me who perhaps always have been thinking about the privacy aspect. Suddenly it was a lot easier to get the business to support it and say that yes, we must do this. So there has been more work and it's been easier to get an understanding that it's a good thing to be careful when it comes to privacy.

00:24:20 Interviewer
So top management kind of came with after that?

00:24:26 Interviewee
Yeah, you often need a price tag on things in order to make them important, and GDPR is a big price tag, or it could be.

00:24:41 Interviewer
Do you have any authorization controls that limit who can access their personal data? How is this setup and who administers it?

00:24:52 Interviewee
Yes, we have. We have several depending on the age of the systems and it's set up centrally by the IT Department, who are also the ones administering it. A lot of stuff is being controlled using Active Directory, Microsoft Authorization solution. I think that that's probably the most common solution in any company today I would say, AD (Active Directory). But there are some other ways too, depending on the age of the system as I said.

00:25:45 Interviewer
What routines, if you have any, are used to make sure that the data that is gathered is necessary.

00:25:59 Interviewee
We have a yearly audit of our systems and that is larger than just privacy or GDPR, and it's a lot about following processes. But I would say that during that audit if we were doing something wrong, it would probably be found in the audit. We don't have any routines in day-to-day work. On the other hand, we already have most of our systems or we have a lot of systems and we're not building from scratch, and I think we would need to have a different routine if we were building this entire company from scratch. Like if we were a startup or something, so now it's more like we are doing incremental changes to the systems every day and we're not changing so much. We have a data protection officer that we can ask when it comes to and whether we are unsure. So sometimes we contact them and describe what we are building, and we get a judgment back like this is okay or, no you need to do it another way in order to be compliant.

00:28:29 Interviewer
How is your security system managed? Like is it maintained or updated? You mentioned you had some from 2008 and some newer ones. How do you decide what to keep?

00:28:51 Interviewee
Yeah, that's the difficult part of my job. Not throwing away anything that is working well for us and replacing stuff as we go along. And this is not just the security system, this is the entire business system that we work on like that. So, I would say we do actively update and change it. And parts of it is off-the-shelf software and part of it is stuff that we have written ourselves.

00:29:40 Interviewer
Do you have a preference between taking something that works and changing it a bit to suit you, or taking something off-the-shelf that you're like “this is exactly it”?

00:29:56 Interviewee
Yeah, you always strive to take readymade software as much as you can, and then you look at how much you would have to change in order to adapt to using it. Then sometimes you're

worse off by using this standard software because you need to do so many changes and then perhaps it's better to build something on your own.

00:30:23 Interviewer

How do you limit human errors in the development of the systems?

00:30:30 Interviewee

So, we have a thorough process for testing software, with several levels of testing, like, a developer testing, system testing, user acceptance testing. A staging environment and then a production environment. There are different tests that need to be done and green before we can go to the next level. This is not only for security, I mean this is to make sure that everything works, but this is also how security is being managed. So, we have a dedicated quality assurance department. They are basically experts on finding problems with our systems. Some of them are working actively in the teams and doing quality assurance as we develop and then some of these QA people are coming in at a later stage and performing specific tests on the software before we can release it.

00:32:05 Interviewer

You mentioned earlier that you log a lot. Does the company keep a log of all the activities that an employee does on their workstation?

00:32:21 Interviewee

I wouldn't know if the company does that because that's for something that would probably be done in the IT department. What I know is that we log a lot of things about what happens in our systems, like the payment systems. And so, we have back-office functions where personnel inside the building can change things and all those changes are being logged when they happened, and who did it.

00:32:54 Interviewer

Do you have measures in place to limit what the employees can do? Like least privilege or things like that, within the company as well.

00:33:13 Interviewee

Yeah, both policy-wise so that we have rules for what you can do and implemented in software so that you need to have a specific role assigned to you in order to be able to perform certain actions. I think you had some other question where it was more applicable, but I can mention it right now anyway. Certain actions will have to have what we call duality, or four eyes, which means that two people need to perform the action. And that is usually when it comes to things that have financial effects on the system if you are working with people's bank accounts or stuff like that. Our customers send order information to us, and we process it and when the payments are done, we need to make sure that the payments come to the merchant's bank accounts. And let's say that changing such a bank account could be a dangerous thing to do, so that is a typical duality action.

00:34:51 Interviewer

Is it a standard that it should always be checked with four eyes before it moves forward?

00:35:03 Interviewee

Yeah, for certain actions. So, it could be changing a bank account, but it could also be granting access to a new user into certain sensitive areas.

00:35:29 Interviewer

Have you experienced that data or information that you work with has not been available at any time?

00:35:51 Interviewee

Well, I mean sometimes we have system downtime and of course, the data is not available while the systems are down. But usually when you are in my role then you don't feel like you’re experiencing that the data is not available you keep working on bringing up the system again.

00:36:35 Interviewer
In your department, how do you allocate resources? Do you have certain parts where you'd like to invest more? Where's the focus?
00:36:55 Interviewee
Since we have different teams working on different parts of the system, the allocation comes to allocating people to these teams and we don't want to be moving people around. I mean, you want to have your team and you get good teamwork going there. So, we don't change this a lot. Basically, it's about putting people in teams and then hiring new people.
00:37:59 Interviewer
Do you feel like you've ever had to make any compromises?
00:38:10 Interviewee
Yes, we often must compromise when it comes to prioritizing things. Let's say that we have two important things, and both need to be done by the same team. We need to prioritize one before the other, but both will be done eventually, so it's more like a timewise separation. You do one and then you do next.
00:38:44 Interviewer
Do you have any specific policies or standards for what goes first?
00:39:10 Interviewee
We're working a lot on becoming better at this, and we're working with OKR (Objectives and Key Results). So, the business defines objectives like we want to be this big or we want to have this amount of revenue and you break that down into key results that you want to achieve. So, during the first part of 2021 we want to achieve something that is more limited in scope so that it's possible to achieve, and for each of those key results we tried to find actual tasks to perform that will go in that direction. We change these OKRs, every half year or every quarter depending on. And we try to make sure that all the tasks that we're working on should be focused towards one of the key results that it should be focusing towards one of the objectives.
00:40:26 Interviewer
Is there a person that keeps track of making sure that you work against the OKRs or is it that the whole team has a goal and then everyone tries to make sure that they work?
00:40:38 Interviewee
It's delegated, so we have this business area manager who is the boss of the whole operation, and he will decide on what the objectives would be. And of course, we can suggest new objectives to him and then we divide that into the teams and look into the key results that could be applicable to the different teams and there you have some kind of cooperation between the manager and the teams deciding on what to be done, and then each team define for their themselves what tasks they should perform to actually be working against these key results so that they can decide on by themselves. So different levels of setting up goals and defining what to do in order to come to those goals. The idea is to give the teams a lot of power and responsibility to find the correct tasks but helping them by giving them these key results that we want them to go towards.
00:41:59 Interviewer
What measures if any, are in place to protect the confidentiality, authenticity, and/or integrity of information?
00:42:21 Interviewee
I can't say too much about this, but I mean we have a lot. I mean normal authentication protection. So, let's say that the data is in databases, and the databases are protected, and the production databases shouldn't be accessible except to the database administrators. So normal users or developers won't have access to the production data so that they can change it. There are also validations when it comes to the merchants sending information to us with the API

calls and we have checksums on the calls, making sure that the messages haven't been tampered with. You're talking about the protection of data in transit or at rest and we need to have both. So, protecting the databases, that's the data addressed, and the checksums are protecting the data in transit.

00:43:49 Interviewer

You mentioned earlier that you do have things in place to check for anomalies, but do you have any specific controls that check them for things such as data loss or tampering?

00:44:15 Interviewee

This is also a place where I need to be a bit secretive, but in general, you can say that one good way of having that is to aggregate data in different ways. So, let's say that you have a lot of orders, and this is just an example, so this is not the real thing. But let's say that you have a list of orders, and you sum the order amounts over dates and then you sum the order amounts over a customer and both these sums should be the same. And the typical thing that would happen when someone is tampering with them is that one of these, or both these sums will change and suddenly they won't be equal anymore. So that is kind of a generic description of one way of detecting it. Redundancy you could say it, it’s another word for basically the same thing. So, you have the data stored in more than one way. And if someone would change it in one place but not in the other place, it would be detected automatically.

00:45:37 Interviewer

That's interesting because usually, we hear that you want to avoid redundancy. But then in this case it's quite a good check for security reasons?

00:45:49 Interviewee

Yeah. And I would say that, uh, I mean previously, if you go way back when data storage was expensive, you wanted really to avoid redundancy because I'm basically just talking about the data storage redundancy here, and today storage is so cheap so you can store the same data in multiple formats without having to pay a lot for. And, it's good for performance, because then you can save the data in one form where it's easy to get it out for one purpose and you can store it in another form where it's easier for another purpose. And that way you will gain performance. So, when someone wants to have a report and you go to a specific report database where you very quickly can get the numbers that belong to the report. But then in some other place, you need some other information and then you have the same data but stored in another way.

00:46:57 Interviewer

Do you have controls to detect discrepancies in the use of your system? We're thinking of unusual access or from unknown locations.

00:47:20 Interviewee

Yes, but I can't delve into that.

00:47:24 Interviewer

You already mentioned the scenario of a systemwide crash, what happens in that case?

00:47:40 Interviewee

I can talk a little bit about that and so basically the crash is what everybody is planning for, but where you seldom happen. Basically, we have two data centers, one North of Stockholm and one south of Stockholm, and they are complete copies of each other. So that means that if one would explode, the other one would contain everything. But it's a lot more difficult, the second part of the question, like a mistake and delete. But the classic way to deal with that is having good backups and if necessary, restore backup. Unfortunately, that would mean that you undo a lot of stuff that has been done if you have to go back in time too because you always have a time difference between when you detect something and when you have your last backup, so that is really something that you try to avoid doing.

00:48:44 Interviewer

You mentioned that for adding information or changing things, you have the four eyes method. Is that the same for taking away information?
00:49:02 Interviewee
I would say that removing information should usually be done automatically. You have schedules and you have rules for different types of data. So, this type of data should be purged after one year and then that will be done automatically. By having it set up like that we avoid having humans being able to perform that and do it wrong. So, it's set up once and then it's just the machines making sure that we remove the data when it's supposed to be removed. And the exception to that rule is of course the GDPR right to be forgotten. So, if someone calls us and says, “I want you to remove me from your systems”. Then we need to do that and that is being handled on a case-to-case basis.
00:50:10 Interviewer
You mentioned that you had two data centers and you mentioned what would happen if one of them crashed. Is there a scenario for if both of them were to crash for some reason?
00:50:26 Interviewee
No, then we would be gone. It's quite far between the two of them, so either it would be some kind of a synchronized attack and/or it would be like a nuclear bomb over Stockholm. So no, we haven’t planned for that.
00:50:53 Interviewer
Is this like the backup process from the second one, like quite immediate or do you work on both simultaneously?
00:51:04 Interviewee
It is immediate, we are performing everything in both systems at the same time, so they are always copying off each other. So, one is the one that is serving information and that could be different for different services like one service is active in one data center and another one is in the other one. But the copies of the data are the same in both places and if one would disappear then it would just switch over to only be using service just from one place. We don't need to copy any data to make that happen.
00:51:49 Interviewer
If your service or application would have an intrusion by an authorized person, what preventative measures do you have in place? Detection and recovery controls? Are there any that would be implemented in case the intrusion bypasses that preventative measures? Is this something you can share with us?
00:52:22 Interviewee
No, I don't dare answer that question.
00:52:37 Interviewer
Overall, are there any aspects of security that are unique to e-commerce businesses?
00:52:59 Interviewee
Perhaps not just E-Commerce, but I would say that what is typical for E-Commerce right now is that it's very fast-moving, and you need to be able to come up with new features very quickly. That means that if you need to build something new very quickly, then you need to be prepared so that you're not building something that is full of security holes. So, I would say that the aspect is that everything is so fast-moving, and you need to be prepared for that all the time. Also, the threats are moving very quickly. We see a lot of changes that previously used to be like, hacking kids, and now it's commercial. It's people who have fraud as a profession.
00:54:08 Interviewer
Are you working in a specific way to focus on these different threats since there can be, as you said, very many threats that can occur?
00:54:18 Interviewee

I would say that no, we work in the same way for both and it's just that it's a lot easier to deal with the hacking kid.
00:54:32 Interviewer
OK, is it okay if we can contact you after the interview if we want to clarify something or have any follow-up questions?
00:54:42 Interviewee
No problem.

Appendix C - Interview Transcript 2

00:00:09 Interviewee
OK, we have started recording. Welcome, today we are doing an interview for thesis work for Lunds Informatics, and this is recorded, and we are permitted recording from all three parties. It will not be used for anything else than the thesis work that is discussed today.
00:00:37 Interviewer
Thank you. As you said, we'll be using this for our thesis in looking into information security and E-Commerce, and we also want to inform you that you may stop the interview at any time if you want to, and we'll also send you the final report when it's done if you wish.
00:01:03 Interviewee
Yes, please.
00:01:03 Interviewer
We've confirmed that we'll also be keeping you and the company anonymous in the paper.
00:01:15 Interviewee
Sounds good.
00:01:18 Interviewer
We can start with you telling us what the company does and about how big it is and such.
00:01:29 Interviewee
We are a retail company; we are a global company. We are at IT where I work. We are about 4000 people working. We support the parent holding company and we also support I think about 80% of the stores.
So that is our main goal then we are providing some services for the one that owns the name and brand of the company.
Yeah, so you could say that for us it's mostly talking about the digital parts there. I work as a security engineer at IT. We support both home smart as well as a product, and then mostly it's our systems. We support a wide range of both information as an object and information down to a data point.
00:03:19 Interviewer
What does the IT environment look like there? Do you have information locally stored or is it cloud-based?
00:03:36 Interviewee
We are hybrid. We own our own server holes. That is not commonly done by retailers before or today, but the company owns several data server holes. We also have a hybrid solution where we own a lot of the instances in the cloud. They are mainly into vendors of the big vendors, so we don't act as small cloud supporters or cloud vendors.
00:04:09 Interviewer
Do you outsource some of the IT tasks, or is it mainly done in-house?
00:04:21 Interviewee
If you're talking about, like the workforce, or is it more of the application itself?
00:04:28 Interviewer
Well, both, maybe.
00:04:33 Interviewee
Depending on. So, we have a lot of in-house, both development, and in-house employees. You heard 4000 before, but we also have consultants and we also have SAAS solutions, where you have software as a service.
00:04:51 Interviewer
What do you think is most important in information security?
00:05:02 Interviewee

If we're talking information security is to know what information you have and where you store it, because you can't have so much of what is most important. But yes, knowing what you're protecting, is a huge step up when we talk about security.

00:05:27 Interviewer

Have the sales been affected by COVID-19 in your company and has this affected your work in information security?

00:05:46 Interviewee

I cannot comment on sales, I can comment on what I do. We, instead of what you may have thought that we do, would or would not work. It's like we have much more to do right now than we have had before.

00:06:03 Interviewer

How is it different? How do you adapt right now since it's in the middle of the pandemic?

00:06:26 Interviewee

If I can take it on more of the general spectrum, than my situation. If you see many of the security memes coming up, it is usually (I can send you a couple of them) but it's like: "Who drives your information security strategy? Is it the CEO or CIO? Or is it COVID-19?"

The thing is, we are changing a lot: all the sudden people are working from home. That means that our endpoints are not in our network anymore. It puts a lot of stress on if you have a VPN solution. It puts lots and lots of stress there and I don't know if you are familiar with the zero-trust strategy?

Traditionally, you work with securing your network, and that's where everyone works. They worked inside your willing network. We had our own network. We've put up firewalls, detectors, and connectors. Everything that was secured in our network, but suddenly, if you take out your endpoints outside it and that is not secured, then you have a problem. So, zero trust builds on that you don't trust anyone: you don't trust the homepage; you don't trust certificates; everything is verified again. That makes the endpoints in the strategy of having zero trust make it secure, and if you could see now in covid times where we have people working very differently. So, if you say that me and my husband work in the same house with the same network. If he's infected, then I'm also a suspect to be infected. So, we cannot just rely on our company sphere. We need to also see that each endpoint stands alone securely. So that has changed it a bit.

So that is one spectrum pure security-wise. A lot of it is network, I would say. Then you go one step further, it's also the consumers or customers who are acting very differently today. You order in by phone, you buy things for your home, everything. So much more is pushing to be online than before, and we have consumers where they say that they are not early adopters, that they wouldn't buy anything online before. Studies say that some ages wouldn't be where they would be reluctant to buy online. We are seeing them. They are very noticeable in the statistics, when you see online sales. Not talking about my current company, but you see in the industry it's as such. Those numbers are crazy and that is of covid. We have a lot of people that are either isolated or the country is closed so they don't have any choice.

Yeah, so those two parameters are the biggest that have contributed to us having more to do.

00:09:58 Interviewer

How do you categorize risks there? Like what does the company value as high-level versus low-level threats? Do you have that?

00:10:23 Interviewee

Yes, we have a model for it. Also, I can say that we don't have a digital risk versus risk as a company. Our risk work is on a higher level than digital. So, all digital risks come from the whole risk perspective. It's an impact probability model, so you look at the risk of if it's probable it will happen and what impact it will then have.

00:11:24 Interviewer

So, it's more like a general model that you have through the whole company that you use?
00:11:31 Interviewee
Yeah, and it's applied depending on how you are working or what your business model looks like. Because we are pure IT, but we also have the same risk coming down to one store, for example, they also look at the risk they are having.
00:11:54 Interviewer
Do you have a process in response to risks? A way to approach if you see that one of these risks is threatening to the company? What's the response to that?
00:12:14 Interviewee
Digital risk? If we see a risk and we have responsible disclosure programs in IT or where we both have consumers and customers can reach out, but also inside where we can do it. We have several processes, or one of them is also for all risks. So yes, we have it. We have, depending on how severe the risks are, we're having different processes and we're handling how to bounce between them as well.
00:13:07 Interviewer
Does the company happen to have like what's called a computer security incident response team?
00:13:51 Interviewee
When it's detected, because you don't detect the risk really, you identify risk. But when you detect something that is connected to our risk, it's usually an incident.
So, it depends a bit on how you mean. We have a dedicated workforce that works with risk because when you are talking about risk, it's something that can happen. When you're talking about an incident or something happening, it's in detection or response mode. Yeah, we have both.
00:14:32 Interviewer
In handling people's private information? Do you feel like there are security concerns in comparison to other confidential data in the company?
00:15:35 Interviewee
Yes and no. Usually you don't think that's flatly that it's either or. You have the same protection in procedures. It's more dependent on how you classify your data and information and such.
Now we have GDPR, you have the problem that there are very strong fines connected and brand reputation to customer and coworker data. We are also set out to be very conscious that it's about integrity and your own data, but we classify that as high as our financial data, as well.
When we talk about data, we talk about how you classify it depending on, usually, the CIA triangle: confidentiality, integrity, and availability. So, we need to know that we keep that together. Depending on your classification to those three then you look at what protective measures you have or need to have. So, I wouldn't say that we separate them.
Usually, I would say that our most sensitive data is on the same level. They have the same security requirements. They are treated very differently because financial data goes through other audits than, for example, when GDPR is more of a when you have an incident, so it's a bit different, more in the “what you do next”.
00:17:25 Interviewer
Do you have a strategy in handling and countering an attack on your service or application?
00:17:43 Interviewee
Yeah, the thing is I don't work with an application anymore, so I work with more strategic security, and I go into application teams and help them secure their environments. I can say that we recommend it. I can say that we have a lot of applications, so it depends on what we have.

00:18:17 Interviewer
What methods are in place to discover if there's been a breach or if someone has accessed information that they are not authorized to see?
00:18:29 Interviewee
Here is the same thing I need to be quite general here, but I can say that we have detective and reactive measures and by buying tools and in house tools.
00:18:44 Interviewer
Do you follow any defined security standards at the company?
00:18:53 Interviewee
Yes, yeah.
00:18:56 Interviewer
Can you specify which types of standards?
00:19:01 Interviewee
Depending on where, and it's also that we are fulfilling some audits, those I cannot mention, I can say them generally as we go through mandatory and voluntary audits to keep us in a good state. We are also aiming for NIST. I think that is one of our standards to work with in the whole process from requirements until compliance.
00:19:34 Interviewer
OK, I thought that was an American standard?
00:19:39 Interviewee
Yes, it is, but the thing is there you could say because they have a lot of open-source work. They are one of the standards that are very general, so otherwise you have a lot of cloud standards, or you have when it's on prem standard. Or you have very information security and then you have technical security. You should remember when you talk about security it's such a huge spectrum when you read like 3 different of these standards, they are super different because they take another scope.
NIST is very general, but deep dives in a good way. I don't say that that is the only right answer. I'm just saying that for us when we are looking at it, it has the right level, because our teams, product teams, that are working and building them are either on prem or in cloud. They have SAAS, they have on prem, they have something they built by themselves, or was bought 20 years ago.
We don't have one application; we don't have 10. Multiply it. So, you cannot say that we only follow a cloud strategy, because then we will lose so much of our landscape when we do a security assessment. Therefore, we choose NIST to be general, and that the ones that have worked with it are some of the greatest names in security.
00:21:34 Interviewer
Thanks for clarifying that. Now that a lot of people are working from home, does the company require you to work from a secure VPN?
00:21:46 Interviewee
No comments.
00:21:48 Interviewer
OK, are there policies regarding bringing your own device (BYOB)?
00:21:55 Interviewee
Yeah.
00:21:57 Interviewer
Are there any that you can elaborate on?
00:22:01 Interviewee
No, I can say that there is a policy but not what it contains.
00:22:09 Interviewer
How has GDPR affected your work with information security, if it has?

00:22:23 Interviewee
Yes, I would say. Both information security and digital security, it has affected a lot.
If you want the more general answer, it's in getting everyone to know what information security is and what is the risk we are having. We worked with these questions long before GDPR, but at the same time it's harder if it's not connected to a fine, or something severe will happen if you don't do this.
In some way it's nice because we got a lot of attention to security and previously, especially. Because I can say that we are not even information security or digital security is working mainly on GDPR. We have another team that goes into GDPR questions.
I would say that, if you want specifics then not general, it is that we have better traceability where information objects are handled and where we have master data instead. So, you get better structuring data. There are also more processes put in place to support the GDPR.
00:23:49 Interviewer
Besides getting a lot of people on board for the project, have there been a lot of struggles, or has it been a difficult adaptation to this implementation?
00:24:05 Interviewee
Yes, and I would say that the hardest part may have been that GDPR came into the pipeline, that GDPR will be coming, but even when it was released it wasn't clear what was expected. It's like GDPR has evolved through time as well as companies that need to abide by it. I think that is the most difficult part, because evidently you would like to have a requirements list that says do this, that and that, and you're done, you or have fixed GDPR. There is no such list, and those lists are too unspecific to fulfill their purpose.
00:24:50 Interviewer
Do you have any authorization controls that limit who can access personal data? How is it set up then, and who would administer that?
00:25:07 Interviewee
When we talked at the start about risk, I said that we are setting different severity with your classifications on a risk and on an information object. If we see that for example, it's a risk. If we leak customer data. Then we classify information high, that it needs to be confidential, has integrity, and is always available. Then we have what you could say controls in place, or that you could utilize, or you should have equal controls by yourself in the team that develops the tool.
So yes, there are, and I would say here we steer more by recommendation and we steer by requirements, so if you should have information on objects that are very highly classified. You need to have these security controls in place, and that limits of course who has access and how you authorize that page or to the application itself.
Any controls are steering how you do it, because for me both access control and authorization are two different things, and they can be put in place as a control to take away a risk.
00:28:20 Interviewer
What routines, if any, are used to make sure that the data gathered is necessary?
00:28:32 Interviewee
Cannot say.
00:28:57 Interviewer
How is your security system managed? Do you have a security system that is maintained, or do you actively update and change it?
00:29:09 Interviewee
You must remember we are aiming to be about 90 security engineers. We are not a small company, so not only one security system, but we also have multiple. I cannot say how many, but yes, we have a responsibility. We have ownership within one organization or one part of the company with it.

Maintain, update and do most of the parts. Then if it's a SAAS then the vendor deals with it, but we ultimately have the most responsibility I would say for updating and maintaining.
00:29:56 Interviewer
Is there a preference between if you update and maintain or make your own, or if you have this SAAS?
00:30:06 Interviewee
Usually when you have a security system you have, now I'm talking about detectives when it detects when something goes wrong, an abnormality, it usually is that they have checks. An application security testing and it tests the scope.
So, when you're coding you can see your code and then you run it through and set it to that application testing system, that notes where you are having security flaws right in the code. We are using several of these tools. There are open-source ones, SAAS ones, on prem, they exist in many flavors.
We use a lot because we have a lot of different languages. It depends on the language and what you are developing. What SAASed tool you use later. They abide by rules and checkers, they're called, and if you use an open source, or if you are using a SAAS or on prem solution it doesn't matter. You choose which checkers are mixed.
Some people just go with the original configuration, that is it, but we are having teams that are going in and looking at these rules and checks and iterating them, and when we see something happening in the market or in a CVE list. So, if we see that something is happening, we can draw it in and detect it already in line when they are developing.
This is very different from small companies, where I worked before. When they had one security system and maybe it was turned on, but they never looked at it, so it's very different depending on what kind of company you are looking at. We are such a big security team, it becomes a bit different because we are not having that one person fix all the securities, we are many that can help and do different things.
00:35:17 Interviewer
How do you limit human errors in the development of systems?
00:35:35 Interviewee
Usually, you say that humans are the biggest security risk. Here it comes down to validation a lot. It comes down to processes, I'm a big fan of ITIL where you define your process in a very fine-tuned way and that you can also add security features down to it. I think that those two are very important and that we are talking a lot about them. How we do secure developments and that it's not just us that are security. Every developer at the company is a part of security, because if they don't know what security is, we cannot maintain it. We cannot do anything about it. So those three elements I would say are the biggest.
00:36:48 Interviewer
Does the company keep a log of each company employee’s activities?
00:36:56 Interviewee
Cannot answer.
00:36:59 Interviewer
Have you experienced that data and information that you worked with was not available?
00:38:03 Interviewee
I cannot answer.
If it's access control, you could want to get into the security part of least privilege if that is what you like, and yes, we are aiming for least privileged and that means that you should only know what you need to know. Yeah, you should not have access to more information that you should have.

For example, I shouldn't have access to customer data because I don't need it, but that is natural and not something I see as weird. So, when we get into these things, it's more of getting to know what I should know or not.
00:38:51 Interviewer
How do you allocate resources in your department?
00:39:29 Interviewee
I don't have that insight in theory or in budgeting as such.
00:39:34 Interviewer
Do you feel like there's a focus though on the best way to get solutions?
00:40:00 Interviewee
If you see from a security standpoint security is very almost personal. Each person that comes in has another experience and ideas than we already have here. So, for us we have a big focus on competence, because we can see that many security tools can either be built, enabled by open-source code or similar. However, at the same time I know that we are running very, very big security tools as well, so I cannot weigh in on who is the most important budgeting wise, but if you see from my perspective, I can see that we are aiming a lot at investing in people. Taking in a lot of competence, looking into how we can make most of the people that are here. Not looking at if we can build or customize our tools more. We're looking: what idea does the individual have and let's run with that. I think it's gained us a lot, because I could say, and this is not from my current company but from a previous place, when you are looking at the application you get a lot of customization that doesn't make sense. After a while you get a heavy application that doesn't make sense, but when you look from a people perspective, you usually talk about personas and customer journey, where you see how it's used and how you utilize things. You get a lightweight process, very customized to the person that will use it. That we have gained by looking it more into resources right now, I think.
00:42:10 Interviewer
What measures, if any, are in place to protect the confidentiality, authenticity, and/or integrity of information?
00:42:26 Interviewee
Yes, we usually do a classification through assessments, and we go from there.
00:42:37 Interviewer
What kind of assessments do you usually do?
00:42:42 Interviewee
We call it business impact analysis. So, we look at what can happen in the business if something is breached or if something happens. Where do we see impact and how can we then take down the risk? And that gives us how confidential it is or how we classify it.
00:43:12 Interviewer
Do you have any controls to detect anomalies such as data loss or tampering, and if so, what?
00:43:24 Interviewee
Yes, we have it, but no comment on what.
00:43:29 Interviewer
Do you have any controls to detect discrepancies in the use of your systems?
00:43:38 Interviewee
Yes, and no comment.
00:43:40 Interviewer
What happens in the case of a system wide crash or a mistake and delete of an important part of the system?
00:43:53 Interviewee
The thing is when we set out controls, when we say that your application has a very high security classification, you need to have a disaster recovery plan. You have it mirrored out so

you can just shift. If it's a cloud instance, you can have it in another region. So, if European instances go down, you can just pick it up from North America instead. So, it's very different how you do it. From the general way of how I see it, you need to have a disaster recovery plan in place. We keep it so super general so everyone can apply it depending on their business criticality.

00:49:32 Interviewer

If your service or application would have an intrusion by an unauthorized person, what preventative measures do you have in place, and what detection and recovery controls are implemented in case the intrusion bypasses the preventative measures?

00:49:48 Interviewee

Very general is that we have tools for it, and we have also processes that come in place where we have one responsibility that takes care of the whole way of getting through to what happened, why did it happen and how can we prevent it?

00:50:10 Interviewer

Overall, do you think there are any aspects of security that are unique to e-commerce businesses?

00:50:23 Interviewee

Which company is not an E-Commerce company anymore? From information security and digital information security, no. No, that's probably the same, it’s just how you fine-tune it, how much you investigate it.

00:50:42 Interviewer

Can we contact you if there's anything we want to clarify?

00:50:55 Interviewee

Yes.

Appendix D - Interview Transcript 3

00:00:11 Interviewer
As you know, we are writing a thesis in information security and specifically to do with E-Commerce, so that is why we are conducting this interview with you.
Before we start, do you wish to be anonymous, or may we refer to your name, role, or company in our paper?
00:00:39 Interviewee
Can we get back to that after I know what we've discussed?
00:00:47 Interviewer
Of course, and then also we just inform you that the information will only be used in our thesis study and that you may stop the interview at any time, and if you wish we will also send our findings and final report when it is done.
00:01:02 Interviewee
Yes, I would very much like to see it when it's done. As I said over email, there's quite a lot of questions I don't want to get into, maybe, but let's go through them and I'll tell you why I won't get into them when we get them.
00:01:18 Interviewer
That is no problem, we can start with where you work, and what your role is?
00:01:32 Interviewee
Yep, sure I work for ForSea Ferries. We operate the ferries between Denmark and Sweden. I am the head of IT so I'm responsible for all of it, including IT security and very involved with OT and OT security, so operational technologies, that's what's needed for navigation and engines and everything like that on our ferries.
We have 5 ferries, 3 currently in traffic. When it's Corona it's a bit less and 2 of those are battery-driven and the rest is still old-fashioned diesel. Our business is, in a non-Corona year, roughly a third freight, a third pedestrian and car passengers, and a third is what we sell on board, where we have restaurants and cafes and stores and so forth. That's kind of an overview.
00:02:46 Interviewer
What does the environment look like in the IT department? Is it a lot of local locally stored stuff or cloud-based? How do you work?
00:03:06 Interviewee
Basically, everything is in the cloud, which can mean basically anything. We have a partner that helps us with all our IT infrastructure, and they have a data center in Malmö, where we have most of our servers. We have a few physical ones, mainly on the vessels themselves. In case the internet connection to the ferries goes down, we still need to have kind of a working infrastructure on each ferry, as well. Those are mainly the physical machines we have; they are on location or on the ferries themselves.
I've learned a lot about how to get reliable Internet connection to the ferries and so forth since I started here, it's the whole world in itself.
00:04:01 Interviewer
Yeah, also especially since it's across countries?
00:04:06 Interviewee
Across countries doesn't really matter, and we have an advantage that it's so close. It's 4 kilometers across here and so we have managed to get a very reliable internet connection to the ferries, basically 24/7, so it's a luxury to get that far.
00:04:27 Interviewer
What do you think is the most important in information security?

00:04:35 Interviewee
That is very hard to answer because that's such a broad question. There's not one thing that's the most important, or you mean the most important to protect or the most important thing to handle, or what do you mean?
00:05:02 Interviewer
That's up to interpretation, but an aspect that when you work with this is the main thing you must think about or something that you're looking at.
00:05:15 Interviewee
OK, for us at ForSea, very specifically to us, the main thing is that the ferries keep on running safely. Nothing should stop the ferries operating safely, that's number one. That's how we define what's the most critical systems, they are the ones for navigation and thrusters and fire prevention. Everything like that on the ferry, that's number one. Everything else is less important than that, and so for us, that is our most protected asset. There are quite a lot of systems involved in battery-driven ferries controlling the batteries and everything like that. That's very sensitive. If somebody gets into it and overreaches the battery or something like that, and so for us, that is the most protected asset and the most important.
00:06:07 Interviewer
You mentioned earlier that the sales have been affected by COVID-19, has it affected your work as well?
00:06:20 Interviewee
Yes, you mean IT security-wise then specifically? It has affected our work, but not very much. If anything, it’s giving us time to focus more on IT security when there are other things we can’t do. So, if anything, it's been positive from an IT security standpoint, maybe not from a revenue standpoint, but from a security point of view, it's good.
00:06:50 Interviewer
How do you categorize risk? What does your company value as high-level and low-level threats? Can you give any examples?
00:07:05 Interviewee
We are talking about security here, right? Since our most protected assets are everything that has to do with safely running the ferries, any risk to that is serious, and of course, it's serious if we have ransomware in our IT infrastructure in general, but we can have that and still run ferries safely. We won't make any money because we can't charge for anything, but the ferries will still run safely. So, everything that has to do with the risk has to be put into that perspective.
We cannot take the risk that there is an accident with the ferries, or somebody overheats the system there or whatever it might be that that cannot take place and we have quite a lot of the maritime regulations on both, both in Sweden and Denmark and internationally that we must take into consideration there as well.
00:08:23 Interviewer
What are some risks with the IT security part? Like what can be a threat to like the system?
00:09:05 Interviewee
If we discount somebody specifically targeting ForSea for whatever reason, for, I don't know scamming inside of millions of crowns or terrorist threats or whatever it might be. If we discount those, which are unlikely and very hard to protect against, the big risks are information leakage, of course, and especially then customer and employee data, GDPR protected data basically, and the other one I would say is ransomware. That has hit quite a few shipping companies already and I think the most likely scenario is that somebody is not really targeting us, but we're getting caught in some automated scan and there's a vulnerability so they can get in and that's the most likely way in.

The nightmare scenario in the shipping industry is what happened to Maersk in 2016/17 with NotPetya from Ukraine or from Russia. I mean it costs, I think $10 billion worldwide or something, that attack.

00:10:57 Interviewer

You mentioned there is some ransomware. How is that a risk?

00:11:07 Interviewee

Oh well, basically, if some ransomware gets in and encrypts all our data. I mean, that's a nightmare scenario and then they want, I don't know $600,000 in Bitcoin or something and I don't want that to happen, please.

00:11:29 Interviewer

When you do have these risks or if you see that something is happening. How do you decide what is going to be a higher level, you mentioned earlier that of course you have everything in comparison to the safety of the travels and all. Is there a certain policy? Is it all mainly compared to that that you consider like if it's high or low level?

00:11:58 Interviewee

We look at the likelihood and the potential impact of those risks, and since the potential impact of something that affects the safe operation of the ferries could be human lives. That is the highest impact you can have. Then, of course, we take those two risks more seriously. But we look at the likelihood and the potential impact of it. Some things are very likely, but there's basically no impact and other things are unlikely, but the impact is we could lose passenger or employee lives, which must be taken very seriously.

That's for the whole company. We do this risk matrix. For the company-wide cybersecurity is basically one line, but then I break it down into much more detailed threats that we need to deal with.

00:13:17 Interviewer

What is the response to risk?

00:13:42 Interviewee

Every risk has a mitigation strategy. How do we lower it? It could be a technical solution; it could be a policy change. It could be training for the personnel. Or probably a combination of all of those. It could also be requirements that we put on our vendors. You must follow these policies. You must live up to these security requirements or and so forth.

When an incident happens, it really depends on what the incident is. If something would happen, that's GDPR related, we have by law certain procedures we must follow, for example. If we identify that there is an intruder in our network, we don't have laws regarding that unless they have gotten to GDPR protected data, but we still have a plan on how to handle that incident together with our infrastructure partner.

00:15:13 Interviewer

In handling people's private information do you feel there are more security concerns in comparison to other confidential data in the company?

00:15:29 Interviewee

Yes, there's GDPR, which is a collection of laws that is both very vague and very specific at the same time, so that must be taken seriously. Beyond the legal ramifications there it's just bad PR and bad customer experience if we leak your information. You're not expecting that to happen, and if it happened, whatever the law says, it's a bad look.

There's also quite a lot of toxic data that we do not want, for example, facial recognition. You can go down to NetOnNet or whatever and buy a camera that can perform facial recognition. There's open-source software you can download from GitHub and do facial recognition, but we don't even want data about that. We don't want that ability, it shouldn't even be theoretically possible for us to do that, because I consider that toxic data. Things will go wrong if we have that ability and that data stored somewhere. Sooner or later, it will get out.

Same with credit card numbers, it's toxic data we don't want. We let somebody else handle this, banks or Klarna or whoever handles that, we don't want it.
I think it's a lot about deciding: what data do you have to have, and what data do you absolutely not want to have? Then you're lowering your risk immediately because we can't leak it, we don't have it. I think the whole idea with toxic data it's quite the fundamental change in how you think about data. It can be useful sometimes, but it can also be used against you.
00:18:03 Interviewer
What information do you have on your customers, for example?
00:18:09 Interviewee
If you buy a ticket in cash in the harbor, we have nothing, we don't know anything. We do have a bit more if you buy online because we must be able to send you the tickets and you do pay for them then by card. So maybe we can get some information there from our payment provider, but we have very little.
Most ferry companies do have to collect a lot of information about their customers. So, if you go to Gotland you have to give up your social security number and you must give up your name and your address of everybody in your car and so forth because they must know that by law. Since we have such a short journey, just 20 minutes, we don't. We have very little data about our customers.
00:19:47 Interviewer
Do you have a strategy for handling and countering an attack on your service or application and, if so, what is that strategy?
00:19:54 Interviewee
Yes, we have, and no comment on what it is.
00:20:16 Interviewer
What methods are in place to discover if there has been a breach? If someone has accessed information or data they are not authorized to see?
00:21:18 Interviewee
Speaking general hypothetical terms. We have some and we are in the process right now to put in ways to identify if a malicious actor is in our network. Once we have identified that we also have a technical means to then figure out: “what are they doing and what have they been doing.” Because if somebody got in, it's a difference if they would just be poking around in our marketing material compared to if they're poking around in our customer information or our financial systems.
So, we have our ways to identify an intruder and we have ways of knowing what they're doing and then limit their access, once we know those things.
00:22:28 Interviewer
Do you have to follow any defined IT security standards, if so which standards?
00:22:39 Interviewee
Uh, we mainly have requirements from Swedish, Danish and international authorities when it comes to maritime law. So Sjöfartsverket, for example, International Maritime organization and so forth, have requirements. Most of the safety regulations are related to physical safety, the operations of the ferries. Cyber threats, cybersecurity, and so forth are becoming more and more a part of that naturally. The requirements on cybersecurity from those kinds of authorities are still very vague. You should be safe, and you should do things about it.
We don't have any other strict external policies that we must take into consideration. If anything, internally we have much stronger policies than the external requires of us.
00:23:57 Interviewer
Does the company require you to work from a secure VPN?
00:24:03 Interviewee

We don't use VPN, we use Citrix, which is another solution than VPN. With VPN you are basically connecting two networks together and we don't want anybody else connecting their networks to ours. So, Citrix, that's what we're using for remote access to our systems. We don't want to connect two networks. No other network should be connected to ours, and with Citrix you basically log in remotely to a computer, not using a VPN. Basically, working in a virtual machine that's hosted on our network.

00:24:58 Interviewer

Are there policies regarding bring your own device (BYOB)?

00:25:05 Interviewee

Yes, there are, but not very strict ones. Bring your own device is very hard to control unless you really have the manpower to do so, and everybody will hate it. What we do have is that you can't bring whatever device you want and just connect it to our network. We have guest Wi-Fi for example, available to guests, customers, and employees to connect their own mobile phones to, you don't connect that to the company network. However, we don't have a very strict one that if you plug in an external device to the network it won't work, it will work.

00:26:09 Interviewer

How has GDPR affected your work with information security?

00:26:18 Interviewee

It puts a very bright spotlight on a certain type of data, which is good. It also makes things complicated because GDPR is, as I said, both very specific and very vague at the same time. It's impossible to say, yes, I am 100% in compliance, because it all kind of depends on everything else. It's more recommendations than strict rules. That has made it more complicated because it's not very clear on quite a lot of issues.

00:27:06 Interviewer

Do you have any authorization controls that limit who can access personal data and how it is set up, and who administers it?

00:27:15 Interviewee

Yes, we do. How it's done depends on what system that data is in and the focus of working with this kind of data is, to begin with, limiting what you have. If we don't need it by law, we shouldn't have it.

Then it's a lot about setting up the processes and systems so the people that don't need that data for the job shouldn't have access to it. How we do that depends very much on each system as well because it's not all in one big database.

00:28:22 Interviewer

What routines, if any, are used to make sure that the data that is gathered is necessary?

00:28:36 Interviewee

The routines again depend on what data and what system it’s in. We do have processes. The most important is, of course you need to keep track of not saving data longer than necessary and to not give everybody access to everything. You should have access to what you need and nothing more.

I still think that the most important thing is to control when you start gathering something new, why do you do that? Do we need it? Should we have it at all? Like credit card numbers we can outsource to somebody else that can deal with it safer than we can, like a bank or some payment provider, for example. I think the most important step is step number one when you're starting to gather data, then question everything and set up routines on how you maintain it, and so forth.

00:30:15 Interviewer

You do that depending on the different systems?

00:30:19 Interviewee

Yes, because it's not only depending on the system, but some things are also manual or semi-manual collection of data. I mean we have dangerous goods. You can take a ferry over with dangerous goods. Some of the dangerous goods are discarded batteries, but it could also be some acid or explosives or whatever, and all that needs to be reported to us. That's a lot of manual steps, but it still can contain data that we need to protect, so it's not only in the systems, it's more about the capabilities and the processes. Systems are a part of that, but we shouldn't discard the manual collection of data as well. I mean, GDPR doesn't make a difference if you keep it in a database or if you keep it on post-it notes, it's data anyway.

00:31:26 Interviewer

How are your security systems managed? Do you update and maintain them, or do you replace them?

00:32:22 Interviewee

Absolutely, yes. It's like if you're developing a website: you're never done, ever. You're never done with IT security, ever. If you stop keeping your servers patched, there will be a new vulnerability tomorrow and you will be open to it. I mean it was just said a month ago or something like that, that there was a new vulnerability identified on mail exchange servers and that had to be patched worldwide on everybody that had it. If you didn't, you were vulnerable to new vulnerabilities, and it was known that the Chinese hacker group was using it to get access to companies worldwide. So, you must keep up to date all the time.
That's probably the most important thing in IT security. Just if you do nothing else, apply the patches. I mean, if you do that, you've done a lot, and that's not always easy if you have old systems that might not be able to use the patches and so forth. Which every company does, have old systems then.

00:33:42 Interviewer

Right, so then with that, do you try to work with your old systems, or do you maybe change them out?

00:33:51 Interviewee

In a perfect world, I would just scrap them and have something else. But we don't live in a perfect world, so the legacy systems that we cannot easily get rid of, or maybe it doesn't make financial sense to get rid of should be isolated from the rest. Basically, it should have no connection to the outside world, it should have no connection to other systems within our infrastructure. It should be hard to get to and if somebody does it, they shouldn't be able to get anywhere else. Isolate them basically. But there's no company that's been in business longer than five years and has more than one server that doesn't have a legacy system. Everybody does, and if they don't, I'm sorry, they're lying.

00:34:45 Interviewer

How do you limit human errors in the development of your systems?

00:34:53 Interviewee

We don't have very much development in our own system. It's mostly done by external parties, and which makes it hard to control for human error. I mean you can test, but most of the things that are serious vulnerabilities you don't see on the surface unless you dig around. So, we don't do enough there I can honestly say.

00:35:19 Interviewer

Does the company keep a log of each employee's activities or anything like that?

00:35:30 Interviewee

Not a comprehensive log on what to do in every system. Now in some key systems, we know exactly what you're doing. So, it depends on the system and how critical it is, and what critical data it might contain.

00:35:47 Interviewer

In those systems that are monitored, do you have access controls in place? Like least privilege?
00:36:06 Interviewee
Yes, absolutely.
00:36:12 Interviewer
Have you experienced that data or information that you work with was not available at some time? It may be some error in the system, or a crash, or something like that.
00:36:31 Interviewee
Yeah, yes.
00:36:33 Interviewer
How do you handle that?
00:36:35 Interviewee
Well, since I'm head of IT and if it is not available, it's my fault. Basically, that's my job, so. I call people, I make people fix it. It's better if we at IT discover it first instead of the users because that means we can be one step ahead and hopefully fix it before somebody else has a problem. But yeah, it does happen.
00:37:10 Interviewer
What is the cause of that being, most commonly?
00:37:16 Interviewee
This is not very common at all, I would say. I would say the most common reason for people not being able to reach their data is human error, user error. They will not admit it, but that's the most common problem, and that's much more common than internet connection being shaky, or the server being down. I mean, those things could happen too, but human error is usually the most common thing.
00:37:50 Interviewer
Do you mean human error from the customer side?
00:37:54 Interviewee
Yeah, from the user, if it's a customer or if it's an employee, just for the user. Of course, it's not always a good idea to tell people that it was human error. Sometimes it’s better to say it was a technical issue and make it impossible to make that same error again, but that's another story.
00:38:15 Interviewer
How do you allocate resources in your department? Where do you invest?
00:38:51 Interviewee
We're a service organization, so there's no need for us to have an IT department unless we make the other department jobs easier. I mean, unless we make it easier to sell tickets and make money or sell wine or coffee onboard or to run the ferries or whatever it is, we have no reason to exist. So, our priorities must be the priorities of the rest of the organization. How can we make their life easier, quicker, cheaper, sell more, spend less, whatever it might be. From an IT security standpoint, we do regular tests of our IT security.
We take in external experts to do pen tests and use that as what we need to focus on. Because it's easy to sit by your desk and say, oh yeah, this should be done and it should be done, but you will miss things that are obvious to somebody else that knows more than you. So, we usually take in external experts to test the security, and that has shown to be a very good way for us to prioritize what needs to be done. A very good way to confirm that yes, with the actions we've taken, we have mitigated the problem. Also, a very good way to highlight to all decision-makers that this here is a problem or it's not the problem. So, it's also a good way to communicate the need for IT security.
00:41:07 Interviewer
Do you have one that you think is more important to focus on: prevention or recovery?

00:41:14 Interviewee
Yes... Prevention I would prioritize there.
00:41:27 Interviewer
Do you ever feel like you have to make compromises?
00:41:31 Interviewee
Yes, every single hour of every single day, yes.
00:41:36 Interviewer
In what way?
00:41:40 Interviewee
We don't have unlimited time. We don't have unlimited budgets and we don't have an unlimited number of experts. So, it always compromises. If I spend 100,000, maybe I get 90% of the way that I want, but to get those last 10% I need to spend 100,000,000 and so that's a compromise. I mean, it always compromises non-stop.
00:42:07 Interviewer
What measures, if any, are in place to protect the confidentiality, authenticity, and or integrity of information?
00:43:20 Interviewee
We have a lot of both processes, policies, and technical safeguards in place for that. But you can never be 100% anyway, whatever you do. We do have quite a lot of technical solutions to limit access and to make sure that nobody gets in where they shouldn't. Again, human error is the biggest problem, so it needs to be verified. Pen tests for example are a good way to verify that everything has been done. Have you missed something in a policy when you configure a database or whatever it might be? Also, to test our own systems to verify that they work, verify that the backups work and that kind of thing.
00:44:31 Interviewer
I'm a bit curious about the technical controls if it's possible to give a broad sense of what kind of technical tools you use?
00:44:43 Interviewee
It's mainly about not giving anybody access to functionality and data that I don't absolutely need. If you have a computer and you don't need admin access to that laptop, you shouldn't have it. So, nobody does, except the people working with setting up laptops.
I mean our CEO doesn't have admin access to his laptop, because why should he? That philosophy goes all the way down to individual fields in a database. If you don't need access to it, you shouldn't, and if you don't need to have admin privileges in the database you absolutely shouldn't have that either.
It's related to the question you asked before of who has access to what, that also applies to functionality in servers and databases and so forth.
00:45:48 Interviewer
Do you have the controls to detect anomalies such as data loss or tampering?
00:45:57 Interviewee
Some yes.
00:46:01 Interviewer
Any you can share?
00:46:03 Interviewee
Not really, no.
00:46:06 Interviewer
Do you have controls to detect discrepancies in the user system?
00:46:18 Interviewee
No, because we don't have very many of those. I mean, of course we do everything we can so we make sure that it's only the person that should have access to, for example, tickets that can

have access to them and we make as sure as we can with that, but beyond that, no, we don't do very much with them.

00:46:57 Interviewer

If your service or application would have an intrusion by an unauthorized person, what preventative measures do you have in place?

00:47:15 Interviewee

Number one is to identify that something is going on, which is tricky. Well, we have measures in place to do that and number 2 is to figure out: what are they doing and what have they been doing? Depending on the path, we could limit their access, throw them out and so forth. Then, of course, analyze everything to see that they didn't leave anything behind.

So, for example, the exchange hack that I mentioned before. Microsoft didn't just release Patch; they also released a long list of things to check for. To make sure that nobody had used this vulnerability on your system. So, we needed to patch our system and then we need you to follow those steps to make sure that nobody had been in there, which they had, which was nice to hear.

00:48:21 Interviewer

Are there any aspects of the security that are unique to e-commerce businesses?

00:48:39 Interviewee

We are not mainly an E Commerce business, we are an operator that sells tickets online and I don't know if I'm the right person to answer that. I mean e-commerce, I mean web security in general. Of course, security around payments that should be the main parts I would guess.

00:49:56 Interviewer

Those were all the questions. May we contact you if we have any further questions or clarifications?

00:50:07 Interviewee

Yes, no problem, no problem.

And I don't think I need to be anonymous in this, we didn't get into that many sensitive things.

Appendix E - Interview Transcript 4

00:00:02 Interviewer
Vill du vara anonym när vi skriver uppsatsen? Med tanke på ditt namn, roll och företagets namn?
00:00:10 Interviewee
Nej, det spelar ingen roll. Det enklaste är om du kan skicka den efter mötet och vi kan kolla igenom den.
00:00:31 Interviewer
Absolut, vi kan både skicka transkriberingen och skicka uppsatsen när den är klar, så får du se den. Vart jobbar du, vad jobbar du med och vad gör du på företaget och vad gör ditt företag?
00:00:44 Interviewee
Jag jobbar på Ica Sverige och ICA Sverige är ett retailbolag som förser våra handlare med varor och tjänster, det är 1300 handlare. Vår affärsidé för ICA är att vi har 1300 handlare som arbetar i samverkan, de är egna juridiska personer som väljer att köpa från ICA och använda ICA:s tjänster. Vi är en grossist i förhållande till dem och kollar butikslägen och koncept. Handlarna äger sina butiker och väljer vad de köper för varor. Vi har även andra segment inom ICA också. Vi har Rimi, ICA fastigheter, ICA bank, Apotek Hjärtat (Min Doktor), ICA försäkring och så vidare som vi samverkar med. ICA Sverige och Rimi är den största delen i koncern och vi är väl typ 80% av verksamhet. Vi har huvudkontoret i Solna, Stockholm, och jag är Dataskyddsombud för ICA Sverige och har tidigare varit även Informationssäkerhetschef och dataskyddsombud. Vi delade på de här rollerna i november, då började jag som endast Dataskyddsombud, innan var detta en gemensam roll. Några år sedan när vi byggde ledningssystemet för informationssäkerhet som var kopplat till dataskyddet i informationsarbetet vi arbetade med. Då var det naturligt att Informationsssäkerhetschefen även var Dataskyddsombudet, men nu har vi kommit ytterligare ett steg i vårt dataskydds arbete. Detta var anledningen till att vi delade på dessa roller och för att nå målet med ännu bättre Governance och styrning.
00:02:53 Interviewer
Hur ser er IT miljö ut?
00:03:04 Interviewee
På ICA Sverige har vi olika verksamhetsområden, vi har en avdelning som heter Verksamhetsutveckling och IT. Jag sitter på Verksamhetsutveckling och IT och där i IT chefen stab. Vårt ansvar är brett, Verksamhetsutveckling och IT avdelningen, det täcker hela ICA Sverige. Vi arbetar med att göra IT leveranser och IT-drifter till dem olika verksamhetsområden, vi har även kontakt med ICA-gruppen och har ett eget IT-drift som vi har koll på.
00:04:03 Interviewer
Lagrar ni er information på Cloud eller lokalt?
00:04:11 Interviewee
Vi har en hybrid i en så stor organisation som ICA, vi har både saker “lokalt lokalt” och även gemensamt inom ICA men även ute i olika typer av moln. Vi har även att vi har lagt ut driften till en extern part.
00:04:45 Interviewer
Vad tycker du är det viktigaste med informationssäkerhet?
00:04:52 Interviewee
Ja det är den stora frågan, men egentligen kan man säga att det är 3 aspekter som vi pratar om. Konfidentialitet, riktighet och tillgänglighet och sen har ju vi utifrån de lagstiftningar som vi tangerar. Vi har ju exempelvis också PCI DSS. Vi hanterar mycket värden i de

ekonomiska system vi har. Det är mycket ekonomisk information som vi har och dessa har ett skyddsvärde. Och sen är dataskyddet då, som är jätteviktigt för oss. Vi har ju nästan hela vuxna befolkningen som är kunder till Ica Sverige. Detta ger mycket uppgifter från kunderna, därför är det är jätteviktigt är att vi kan hantera det på ett bra sätt. Det är viktigt med skyddet av informationen och hålla förtroendet öppet till hur vi hanterar den informationen vi tar in och hanterar. Det är inte bara kundernas information utan även medarbetarnas, vi har leverantörer som vi arbetar kontinuerligt med och det är viktigt att vi hanterar deras information på ett bra sätt.

00:06:18 Interviewer

Hur har era sales påverkats av Covid-19? Och har det påverkat hur ni jobbar med informationssäkerhet?

00:06:38 Interviewee

Det har den inte eftersom vi flyttade till det huvudkontor vi har nu, för 2 år sedan, det innebär att vi införskaffade ett nytt arbetssätt. Innan vi flyttade var det en startsträcka på ett par år med planering och vi hade höjt våran ribba med det digitala arbetet. Vi har ju aktivitetsbaserat kontor så det var då att användaren har ju ingen arbetsplats så är det allting finns i maskinen. När Covid-19 kom var det väldigt lätt för oss att ställa om med att sitta hemma och jobba istället för att vi hade all infrastruktur för det. Vi hade "allt i nätet" för det och det gjorde att det var enkelt för att liksom att ta det steget. då så Informationssäkerhetsmässigt har vi inte haft någon händelse eller effekt som har påverkat oss rent negativt utan sen är det ju alltid utmaningar som uppkommer. Då vi har suttit hemma i ett år kan det uppkomma utmaningar som exempelvis om man kanske har dokument. Jag är en sån som sitter med dokument och skriver ut dem för att jobba med det och hur hanterar man det? Jag är en säkerhetsnörd som tänker på det, men kanske inte alla medarbetare tänker på det. Eftersom på jobbet har vi sekretess hinder och annat för att hantera detta. Men vi har inte haft någon incident eller någon stöld eller annat som tagit effekt.

00:08:18 Interviewer

Har ni någon policy som medarbetare kan följa?

00:08:29 Interviewee

Vi har regler som vi alltid har haft. Vi som modern arbetsgivare har vi haft ett externt digitalt arbetssätt. Man jobbar när man reser och även på andra platser då vi har kontor på olika ställen. Vi jobbar väldigt flexibel och det har fungerat väldigt bra hos medarbetarna. Dem vet om vad dem får göra och inte får göra, vi har även byggt in funktioner i exempelvis Microsoft 365 för informationsklassning. Om man sätter upp en informationsklass som är mera känslig, då kan den informationen inte tas ut av vem som helst på vilken device som helst. Utan då blir informationen automatiskt krypterad och hanterad på det sättet när man även kommuniceras.

00:09:21 Interviewer

How do you categorize risks? What does your company value as high level vs low level threats? Can you give examples?

00:09:52 Interviewee

Vi har en riskhanteringskonsekvens skala som går inom olika segment. Allt från ekonomi till lagefterlevnad samt påverkan på enskild och så vidare. Det är ett antal kategorier som man gör bedömningen på i den skalan. Från noll till 5, då så är det klart att vi är där så är det högsta så är det lite mer att i siffror på den skadan kan vara då den skalar man kan begära. Vi har även regler när det gäller större projekt med en större omsättning, ska man även göra en affärsmässig riskanalys. En görs emot produkten, systemet man bygger ska alltid göras med löpande riskanalyser. Vi har även en skala där vi definierar vår riskaptit i konsekvensskalan. Vad det gäller privacy risker så har vi också särskilda regler för det om man ser att risken är stor för hela verksamheten. Då är det också så att då ska den eskaleras till vår VD då som

fattar beslut om hur den ska hanteras då. Vi har en Governance struktur kopplat till Riskhantering som stora bolag som ICA har. Vi gör riskanalyser på längden och tvären genom verksamhetsåret och vi har en riskkommitté som finns denna typ av bolag och sedan finns även koncernstyrelsen ytterst, en gång per år. Och detta finns för att kunna ha diskussionen om ICA tar för stora risker inom ett område eller utvecklingsfas.

00:11:43 Interviewer

What process do you have in response to risks?

00:12:05 Interviewee

Vi gör riskanalyser genom hela verksamhetsutveckling löpande, riskanalyser görs både i projekt eller i utveckling av projekt. Vi har riskanalyser genom hela arbetsmiljön, vi har även riskanalyser som görs för att förordningar säger att vi måste göra dem. Detta kan vara att vi måste Data Privacy impact Assessment och då gör vi det för att se vilken risk finns i förhållande till den registrerar och inte enbart risken mot bolaget. Vi har många olika steg i den processen och det är vi inom IT som arbetar med att arbeta med dessa aktiviteter.

00:13:17 Interviewer

Finns det en person som är ansvarig för att hålla koll på specifika risker?

00:13:36 Interviewee

Ja, i större organisationer har vi beskrivet vem som får fatta beslut och vissa ekonomiska värden. Det är ifrån den lägsta nivån till VD:n, vilka ekonomiska beslut får dem olika nivåerna fatta. Och detta kan kopplas även till risk, den verksamhetsområdet som risken mest pekar på blir riskägare. Det görs en dialog om vem som ska vara ansvarig för risken och vem som blir riskägare. Om den pekar mot IT och då är det ju oftast IT chefen som tar ansvar för den funktionen som verksamheten använder. Det måste alltid måste föras en dialog om vem som är riskägare.

00:14:31 Interviewer

Hur gör ni bedömningen om vem som ska ta på sig ansvaret?

00:15:00 Interviewee

Det är på det stora hela inte ett problem vill jag påstå då vi för en dialog i start av projekten samt när vi arbetar i förhållande till organisationerna bör vi ha en diskussion om det behövs det diskuteras varför det behöver vara den specifika personen som tar ansvaret. Om ansvaret finns hos andra verksamheter också blandar man i det.

00:15:18 Interviewer

In handling people's private information, do you feel there are more security concerns in comparison to other confidential data in the company?

00:15:50 Interviewee

Normalt sett när vi bygger en applikation eller hanterar ett system inom EU/ESS brukar det inte vara några andra krav än dem som vi har i vår kravlista. Vilka krav ställer vi på ett informationssystem och då är kraven redan inberäknade där. Exempelvis som personuppgifter, då startas ett åtgärdspaket som är kopplad till detta. Det vi måste titta särskilt på ur ett dataskyddsperspektiv är att man har vidare behörigheter om det är ett system som inte har personuppgifter. Men när man behandlar personer med känsliga personuppgifter eller särskilda personuppgifter, kan man ha begränsat med behörighet för denna information på ett helt annat sätt. En effekt av att det finns personuppgifter, ökar säkerheten lite mer än vid annan information. Om det är landsöverföringar, måste vi göra det mer som en tjänst. Vi måste titta på ytterligare krav som behövs ställas för att skydda informationen under kommunikation och under bearbetningar till landet man finns i och ta hänsyn till deras lagar.

00:17:17 Interviewer

Do you have a strategy for handling and countering an attack on your service or application? If so, what is your strategy?

00:17:34 Interviewee

Ja, PCI DSS regelverket ställer krav på att man skall ha en förmåga kopplat de systemen. Vid träningarna för hur vi ska klara en incident, detta kan påverkar hur vi arbetar med hela IT miljö exempelvis. I en stor organisation som ICA, händer incidenter hela tiden och då tränar vi skarpt på grund av detta. Vi utvärderar händelsen och vad vi lärt oss utav detta, samt jämför med andra händelser som skett. Vi har inget stort, särskilt program för att titta på olika typer av attacker. Hur dessa attacker skulle vara och vad skulle vi göra om dem skedde. I projekt kan vi göra skrivbord simuleringar, du kan föra diskussioner, göra riskanalyser om de möjliga attacker och risker som kan uppkomma. Samt om vi har förmåga att motverka detta.
Jag tror att i en vanlig verksamhet som vi driver, har vi inte dem behoven eller är riskutsatt på det sättet. Vem våran angripare är, är en fråga man alltid borde ställa sig.

00:18:50 Interviewer
What methods are in place to discover if there has been a breach or if someone has accessed information/data they are not authorized to see?

00:19:21 Interviewee
De infrastrukturkomponenter som finns i M365, i säkerhetsmekanismer som brandväggar, IPS register och annat. Det har ju loggfunktion, loggfunktionerna innebär att det triggar igång larm om man bryter mot dem säkerhetsreglerna som är uppsatta. Och, vi har exempelvis skydd mot skadlig kod och så vidare. Alla de här larmar när det händer någonting. I varje komponent som finns i infrastrukturen, finns den här typen av igångkicknings effekter. Vi har vi ett centraliserat system som alla de här kommer in i och sedan analyseras och sedan utifrån det, hur de ska hanteras. Det finns mekanismer för det då. I Microsoft 365 är den miljön, tidigare Office 365. Där finns det mekanismer som exempelvis där du kan införa olika typer av prevention funktioner som triggar igång larmfunktioner om man försöker gå utanför sina behörigheter. Exempelvis om vi ser att Johan alltid sitter hemma och jobbar och har plötsligt trafik från nån annanstans, kan det också kicka igång ett larm.

00:20:54 Interviewer
Do you have to follow any defined security standards? If so, which standards? (ie ISO, IEC, PCI DSS)

00:21:26 Interviewee
Grunden för vårt informationssäkerhetsarbete och för vårt dataskyddsarbete är ISO standarder. Vi jobbar med 27001 och 27002, och vad gäller dataskydd är det 27701 som är integrerad i ettan och tvåan vad gäller dataskydd. Vi jobbar med PCI DSS som standard också och sen finns det andra standarder som vi har. Exempelvis hur man bygger upp incidenthantering. Men det är ISO standarder vi jobbar med framförallt. Säkerhetsregler används för att se hur de följs i utveckling och annat. Vi har CSI i 20 kontroller ytterligare en som funktion vi använder för att hålla koll på hur ska jobba säkerhetsmässigt.

00:22:07 Interviewer
Does the company require you to work from a secure VPN?

00:22:26 Interviewee
Ja, det gör vi och detta underlättade vårt distansarbete då vi hade dessa funktioner på plats. Vi jobbar hela tiden via VPN och vi har även andra lösningar som drevs igång på grund av pandemin, för att få upp effekten.

00:23:11 Interviewer
Are there policies regarding BYOD (bring your own device)?

00:23:30 Interviewee
Man kan säga inte som en egen policy utan vi har vår policy för hur vi jobbar med informationssäkerhet och vad vi tillåter. Regeln är om vi kan managera enheterna är det okej att använda enheterna. Kan vi inte manager den så är det inte okej. Exempelvis om jag skulle använda min privata iPad för att arbeta med jobbet. Kan jag ansluta den? Ja, då kan jag manager den. Och det innebär ju att då kan ju ge raderad information som är på den exempel.

00:24:10 Interviewer
Ifall ni hade haft en dator hemma som ni vill använda er av nu när ni sitter hemma, behöver ni nollställa den först innan ni använder den?
00:24:25 Interviewee
Behöver man inte göra, men det kan man managera den datorn då ifrån våra system. Det har aldrig varit frågan att man ska köra på sin egen maskin hemmavid. Vi är väldigt noggranna med att tillhandahålla datorer både för medarbetare och för konsulter, men sen har vi också andra det lösningar, alltså andra tekniska lösningar där man kör virtuellt. Då kan du köra på din egen maskin, men via VPN, likt då du kör virtuellt istället. Då behöver du ingen maskin utan det har ju egentligen inte förrän från vilken maskin var som helst i världen.
00:25:11 Interviewer
How has GDPR affected your work with information security?
00:25:30 Interviewee
Det är klart att med de riskerna som finns och det viktiga med GDPR och den ambitionsnivån vi har på ICA så påverkar GDPR informationssäkerhetsarbetet väldigt mycket. Vi måste ha koll på ett helt annat sätt än tidigare. Att ha koll på er vårt skydd ändamålsenligt, om den gör det den ska och så vidare. Och sen var det mycket stor påverkan på de här processerna, exempelvis med incidenthantering. Och så är det för de här tiderna som är också i enlighet i förordningen. Idag är väldigt mycket kopplat till tredje land överföringar och vilka risker som finns kopplat till det. Det påverkar informationssäkerhet mycket och vi har sett också att på lite längre sikt måste vi ha andra gemensamt i koncernen för antal andra säkerhetsåtgärd, exempel för att kunna hantera kryptering på ett annat sätt än vi har gjort tidigare. En annan funktion kan vara också att hur vi anonymiserar information, vi kanske behöver en tjänst för det här. Det är sådana saker som driver på informationssäkerheten och just nu är det dataskyddet som driver informationssäkerhetsarbetet framför sig. Hur den aspekten egentligen får de resurser och de förändringar vi behöver göra, det är drivet av dataskyddet och GDPR. Men även resursmässigt har det påverkat i någon slags arbete igen en del i att man har tillräckliga resurser, så det har ju också ökat genom dataskyddet också.
00:28:04 Interviewer
Do you have any authorization controls that limit who can access personal data? How is this set-up and who administers it?
00:28:20 Interviewee
Ja absolut det görs för varje projekt, för att se hur ska behörighetsstruktur sättas upp för den applikationen eller den accessen till den data som finns. Det finns olika tekniker för det, vi har system som hanterar det både generellt men sen kan det även vara att bygga in funktioner utifrån de krav som är ställda på funktionerna i applikationen. Man köper in då istället. Det är hela team som håller koll över de funktionerna.
00:29:01 Interviewer
What routines (if any) are used to make sure the data that is gathered is necessary?
00:29:17 Interviewee
Med att få upp GDPR för att bygga in funktioner, för att kunna radera informationen och se till att man gallrar den informationen som inte behövs utifrån de tider man har satt upp för applikationen. Detta ska finnas för varje applikation. Och vi kör rensningar, vi har ett stort system som vi håller på och rensar i nu. När vi rensar ut gammal data, har vi exempelvis Outlook där vi har tidsgränser. Då är det automatiska körningar som görs och rensar bort den informationen då efter den bortre tidsgränsen. Då behöver vi inte tänka på det utan det som behöver sparas måste särskilt sparas, annars rensas det bort. Vi bygger in system funktionerna som automatiskt kickar igång.
00:30:19 Interviewer

How is your security system managed? Do you have a set security system that is maintained or do you actively update and change it?

00:30:38 Interviewee

Ja, när man talar om ett säkert system måste man definiera vad man menar med det. I ett säkert system är det många komponenter som behövs för att skydda informationen, alltifrån nätverkskomponenter till systembehörighet till loggning och så vidare. I vår infrastruktur, men sen även då på applikationen så är det ju i den förvaltningen i applikationen så skulle de sköta sina delar då för att administrera då exempelvis om det behörighets hanteringen i en applikation. Annars så har vi då särskilda säkerhetsregler för vad den infrastruktur som sköter om olika delarna. Det finns och en hel organisation som gör det då och det kan man göra om man är så stora som vi. Det är Security operations center och de sköter då alla de säkerhetskomponenter vi har i vår infrastruktur för att säkra informationen under lagring, kommunikation och så vidare.

00:31:57 Interviewer

How do you limit human errors in the development of the systems?

00:32:08 Interviewee

Vi jobbar Agilt. Vi har agila team som utvecklar allt. Det som är viktigt är att när man har den strukturen som vi har med våra butiker då, de är våra kunder egentligen. De här tretton hundra butikerna som finns ute så vi väldigt stor påverkan direkt om något inte funkar. Därför är jätteviktigt att vi testar ut våra funktioner ordentligt och då är det så att den som utvecklar testar inte. Utan det är en annan roll eller person som testar det den andra har gjort, exempelvis kod. Och det här görs för att ta bort de mänskliga felen. Sen finns det både automatgenererade tester som körs, alltså att man testar koden automatiskt. Det finns många såna funktioner. Och ofta kan man säga så här att om man har något brukar inte vara fel i koden, utan det är ju att man kanske har inte driftsatt sin applikation funktion som jag inte är tillräckligt ut testa då vi använder oss som är har man inte gjort alla de delarna som borde göras.

00:33:23 Interviewer

Does the company keep a log of each employee's activities?

00:33:41 Interviewee

Ja, inte alla anställda utan vi bestämmer det. Det finns två perspektiv när man talar om loggning, det ena perspektivet är för att kunna hitta fel och hantera en störning eller avbrott i system. Det andra är om någon har brutit mot säkerhetsreglerna. Det finns även regler för vad som ska loggas i förhållande till användaren och systemets känslighet, exempelvis vilken typ av informationsklassning det är. Detta ställer högre krav på loggning. Det sker loggning både i applikationen, samt på servrar och även på andra funktioner också, så man kan se vad man gör då. Det är en behandling vi gör när man tar loggar och detta kan vara även en behandling i sig, ifall man tittar på dataskydds perspektivet måste man beskriva hur länge loggning informationen behövs hanteras. Detta är en säkerhetsfråga. Det måste man vara tydlig med, liksom vilka bevarande tid vi har för den typen av information. Och normalt brukar det ligga på en ett år upp till 15 månader, för säkerhet loggning information. Om man inte har upptäckt säkerhetsrisker på den tiden, har verksamheten problem.

00:35:07 Interviewer

Have you experienced that data and information that you work with was not available?

00:35:25 Interviewee

Ja, men då är det ofta en teknisk störning inom en komponent eller en brist i ett system på grund av att det inte var färdigt. Det inträffar hela tiden och inträffar alla, dem som säger att dem inte varit med om detta håller inte på med IT. Det händer störningar hela tiden och då behöver vi vara duktiga på att hantera störningarna. Tiden av störningen är väldigt kort från

att man upptäcker det till att man har åtgärdat det och därefter fortsätter verksamheten att rulla igen.

00:36:14 Interviewer

How do you allocate the resources in your department?

00:36:23 Interviewee

Vi jobbar Agilt genom hela organisationen. Vi gör årsplaner och i denna årsplanen beskrivs vad som ska göras i det kommande året. Detta bryter man ner i tertial i 4 månaders perioder. Och då sätter man upp mål för verksamheten, exempelvis om ett system ska utvecklas kommer dem till min avdelning och ber oss göra detta eftersom resurser som vi besitter krävs för att göra utvecklingen. Riskanalyser, behandlings analyser, informationsklassning, framtagning av säkerhetskrav och så vidare, utformas. Detta görs även med informationssäkerhets funktionerna. Vi planerar i 2 veckors sprintar för aktiviteterna som behövs göras, det är mycket kommunikation på tvären för att kunna veta om olika resurser behöver allokeras nånstans. Vi som jobbar med dataskydd och informationssäkerhet, jobbar löpande med att ständigt förbättra hela ledningssystemet.

00:37:38 Interviewer

Använder ni er av resurser från andra team och avdelningar?

00:37:44 Interviewee

Ja, vi samverkar mycket med dem som jobbar inom sourcing, och har mycket kommunikation på tvären genom organisationen.

00:37:57 Interviewer

Vad tycker ni är en prioritet? Att ni har kompetenta personer inom ert team eller att ni har tillgång till de tekniska resurserna finns?

00:38:23 Interviewee

Vi vill komma in så tidigt som möjligt, i förstudien när vi talar om projekt. Vi tittar på vad är det vi vill göra med projektet och vilken information är det vi hanterar. Vi gör informations klassningar, riskanalyser och bedömning av vilken påverkan man vill göra. Samtidigt används även PCI DSS, Dataskydd och så vidare. Denna bedömning görs i förstudien och om man väljer att gå vidare, bedöms vilken kompetens kommer behövas. Exempelvis säkerhetsmässigt i ett arbete och dataskydds mässigt i ett annat arbetet. Det kan vara att ny teknologi används, därför behövs en informationssäkerhetsarkitekt behövas i lösningen då alla inte har kunskap om de specifika tekniska områdena som ska beröras. Eller om teamet är osäkra på hur säkerhetspaketet ska omsätta den nya tekniken och då är det väldigt viktigt att dessa bedömningar görs väldigt tidigt i projektet för att planera för dessa faktorer.

00:39:20 Interviewer

What measures, if any, are in place to protect the confidentiality, authenticity and/or integrity of information? (ie cryptography, etc)

00:39:45 Interviewee

Det vi använder i grundpaketet är 27002. Regelverket 27002 reglerar vilka komponenter och detaljer vi ska använda. Reglering över hur långa lösenord ska vara behövs, därför göra en bedömning om hur långt lösenordet ska vara eller om användning av tvåfaktorsautentisering behövs. 27001 är själva ledningssystemet och 27002 är säkerhetsåtgärderna, dessa innehåller Guidelines för vilka säkerhetsåtgärder man ska införa. Dessa har gjorts en bedömning av i förhållande till de säkerhetsåtgärderna på ICA.

00:41:18 Interviewer

Do you have controls to detect anomalies such as data loss or tampering? If so, what?

00:41:29 Interviewee

Ja, det kan man säga. Det beror på vilken plattform vi pratar om så finns det olika funktioner för det. När det kommer till säkerhetsåtgärder, pratar inte organisationer om dessa. Man brukar inte prata om vilka produkter man har valt och var de sitter någonstans utan det blir ett

mer generellt svar om säkerhet. Detta på grund av att då kan en angripare veta vilka produkter vi använder för att motverka detta och var dessa finns.
00:42:27 Interviewer
Vad är det för typer av kontroller ni använder för att hitta detta?
00:42:36 Interviewee
Genom användning av 27000–2. Jag vill inte vara mer specifik än så.
00:43:07 Interviewer
Do you have controls to detect discrepancies in the use of your system? (i.e. unusual access or unknown locations) If so, what?
00:43:21 Interviewee
Ja, det kan vi säga att vi har på samma sätt som tidigare med 27000–2.
00:43:26 Interviewer
What happens in the case of a systemwide crash, or mistaken delete of an important part of the system?
00:43:38 Interviewee
I det fallet finns det en process med två stycken delar. Om det blir en störning eller ett avbrott i ett informationssystem, gör man en bedömning av allvarligheten och vilken prioritering ska hanteringen ha av denna. Det finns 4 stycken klasser inom ramverket ITIL, mellan klassningen P1 till P4. Det styr vilken organisation som går igång för hanteringen av störningen eller avbrottet. Vid lägsta klassen, jobbar jag med det själv i IT förvaltningen och i den högsta klassen går en organisation in. Dem hjälper till och stöttar för att få igång systemet så snabbt som möjligt, eller återställer till och med genom en åtgärd. Om man gör bedömningen att det har någonting med säkerhet att göra, behöver ytterligare en process sätts igång där man drar igång en säkerhetsorganisation för att hantera händelsen samt i vissa fall även respektive bolag. Säkerhetsorganisationen går in och leder hanteringen i det fallet och detta görs via en särskilt process. Det finns även organisatoriska delar med det hela, det är vanligt med avbrott som inte har med säkerheten i verksamheten att göra.
00:45:05 Interviewer
Har ni någon Contingency plan för det?
00:45:28 Interviewee
Inom IT finns det återställningsplaner, ofta som man har för att återställa informationssystem, detta är en del av verksamhetens kontinuitet plan eftersom verksamheten måste ha en plan vid återställning. Ifall dem inte har stöd ifrån en IT funktion måste denna återställas så snabbt som möjligt.
00:45:57 Interviewer
If your service or application would have an intrusion by an unauthorized person, what preventative measures do you have in place? What detection and recovery controls are implemented in case the intrusion bypasses the preventative measures?
00:46:11 Interviewee
Ja, då går Informationssäkerhets incidenthantering igång. Och beroende på vad som inträffat kan olika säkerhetsåtgärder vidtas. Detta loggas och kollas igenom för att kunna ses vilken typ av attack som skett, var det skett, vad gärningsmannen har gjort till systemet. Samt ser vad konsekvensen är och för detta finns det flera olika åtgärder som kan tas i IT infrastrukturen för att säkra den. I varje fas i incidenthanterings finns det olika typer av åtgärder som kan tas och det krävs att stänga effekten av attacken så att den inte kan fortsätta och återställa systemet.
00:47:13 Interviewer
Vad händer om den tas sig in? Vad gör ni?
00:47:33 Interviewee

I IT-strukturen gör vi segmentering inom IT-miljön, vi vill inte att om en person kan ta sig igenom den första dörren sedan är inne hela IT miljön. Man måste ta sig igenom ett antal lager innan man når informations resurserna och därför gäller det vi snabbt serverar den delen i nätverket eller i systemet, där personen eller angriparen kan finnas. För att sedan stänga ute dem och återställa systemet.

00:48:07 Interviewer

Overall, are there any aspects of security that are unique to e-commerce businesses?

00:48:22 Interviewee

Det är oftast väldigt känsligt med händelser som har med tillgänglighet att göra. Tjänsten måste vara igång hela tiden eftersom kunderna handlar hela tiden, verksamheten måste vara igång 24/7. Tillgänglighetskraven är viktiga och tjänsten måste fungera till varje pris, därför måste uppgifterna som utförs vara säkrade och skydda detta. Det kan vara exempelvis att spara kontokortsnummer och annat, för att köpet ska gå snabbare nästa köp. Därför måste informationen vara skyddad, konfidentialitet och tillgänglighet är därför väldigt viktigt och det är viktigt att funktionerna som bevarar detta finns. Det är självklart viktigt med detta inom alla delarna inom organisationen, samt riktighet är viktigt då endast behöriga personer ska kunna ändra i informationen. Det är viktigt att någon ska kunna ändra att du köper 10 saker istället för endast en sak som du beställt. Allt detta är viktigt inom verksamheten men ett fokus finns på att tillgängligheten fungerar.

00:49:43 Interviewer

Tack så mycket. Går det bra om vi kontaktar dig om vi har några frågor?

00:49:46 Interviewee

Ja, det går bra.

Appendix F - Interview Transcript 5

00:00:02 Interviewer
Vill du vara anonym sedan när vi refererar till dig och din roll i företaget i vår kandidatuppsats?
00:00:12 Interviewee
Nej det behövs ju inte, men det är viktigt att ni nämner Svea Ekonomi då. Det är där vi jobbar så att säga. De har satt som krav på att ställa upp på sådana här saker att det ska framgå att det är att vi jobbar på Svea Ekonomi.
00:00:40 Interviewer
Perfekt, och ifall det är så att det är någonting som du vill att vi kanske inte ska spela in kan du säga till så stoppar vi inspelningen eller tar bort det sen.
00:00:55 Interviewee
Nej, men det är lugnt.
00:00:59 Interviewer
Då kan vi börja med: vart jobbar du och vad gör ditt företag?
00:01:09 Interviewee
Jag jobbar på Svea Ekonomi AB. Som är en koncern då, den startades i Sverige. Fortfarande samma ägare och grundare i bolaget, men idag så är vi rätt stora och jobbar inom i huvudsak faktura försäljning, och vi köper mycket fakturor också. Sen är det inkasso i en stor bit av Sveas område, och på senare år så har vi också hållit på med finansiering av webbtjänster och det är alltså i betalväxel då för webbtjänster. Det menas att webbhandlaren, när man kommer till betalningen så är det vi som utför betalningen och webb handlaren får då minus någon avgift beloppet då direkt. Medans vi tar då och skickar ut fakturan till kunden eller om de gör en kortbetalning så är det vi som tar hand om kortuppgifterna och såna saker. Är det något man inte betalar sen då är det våran inkasso som tar över och driver ärendet och så att säga. Så webbhandlaren släpper så fort han har sålt, då släpper han affären. Så webbhandlaren den tar inga risker och det växer väldigt mycket, det området. Sen finns vi i hela Norden, vi har kontor i Norge, Finland, Danmark. Vi har också kontor i det vi kallar för DACH. Det är alltså Schweiz, Tyskland, Österrike. Nederländerna finns vi också i. Och sen har vi ett helägt bolag i gamla öststaterna skulle jag säga, att det är väldigt mycket Baltikum, Ryssland forna Sovjetstater med inkasso verksamheten. Det är nästan 1000 anställda där, så det är rätt stor del. Det är väl vad Svea håller på med stora drag.
00:03:57 Interviewee
Så når vi också har vi ett dotterbolag som är bank. Vi köpte ju Amfa Bank och då har det blivit Svea Bank, och det gör att skillnaden är egentligen inte så stor emellan ett kreditmarknadsbolag och en bank utan stora skillnaden är att man clearar pengar direkt med Riksbanken. Det går lite fortare betalnings vägarna då, när man banker emellan kan cleara sina skulder mellan varandra, via Riksbanken. Och det går lite fortare än när man är som kreditmarknadsbolag för då måste man gå via en bank för att kunna göra den här clearingen och det tar tid. Det ställer lite andra krav på bank och sådana saker. Det är Svea, jag ska inte säga spretigt, men det har blivit rätt många olika områden som vi jobbar med.
00:04:58 Interviewer
Vad är din roll i själva organisationen?
00:05:08 Interviewee
Jag är IT säkerhetschef, om man säger så här, vi har 4 tårtbitar när det gäller det vi kallar för informationssäkerhet, då är det delen informationssäkerhet som hanterar ledningssystem. Sen har vi IT säkerhets biten som är min och sen har vi det som vi kallar för cybersäkerhet och det är bland annat utredning av incidenter ärenden, men också där man tittar på cyberhot och såna

saker. Och sedan fysisk säkerhet som är larm, brandlarm men också kontroller eller om det är personskydd och sådana saker. Så det är i fyra tårtbitar det här säkerhetsarbetet. Jag har det som rör våra system och våra tjänster. Som jag försöker göra så gott vi kan att säkra. Vi har mycket fysisk eller har fortfarande datahallar som vi har våran egen utrustning i. Men som sagt mer och mer kommer till att e-handel och även att tjänster ska vara publika sajter även för de andra affärsområden.

00:07:20 Interviewer

Hur ser er IT miljö ut i organisationen?

00:07:34 Interviewee

Vi är lite traditionella där. Som bank och kreditmarknadsbolag i Sverige lever man under Finansinspektionens kontroll och i förlängningen så är det EBU, alltså europeiska bankunionen, som ställer krav på oss. För att få vara kreditmarknadsbolag måste vi uppfylla vissa kriterier och det är deras finansiella kriterier, man måste ha ett visst antal kapitaltäckning som det kallas. Vi måste ha visst antal pengar på banken för att få låna ut pengar till privatpersoner och såna här saker, men de ställer också krav på IT säkerhet utifrån de här regelverken. Och genom att i EBU som bestämmer det mesta så kan man säga att finansinspektionen de bygger sina regler på, och där det uppges nivå då så att det ska bli så förhållandevis lika som möjligt för alla banker i EU. Och då får man inte göra vad som helst. Och det är ett problem som man kan nämna. Det är att det här med molntjänsterna som har blivit väldigt populärt. Det är någonting som bankerna är generella drag i Sverige har svårt att leva upp till att lägga personuppgifter till exempel i molntjänster, för vi vet inte vad de hamnar någonstans. Och det här är ett dilemma för oss. Genom att de stora aktörerna är oftast amerikanska bolag och att lägga saker hos Microsoft, det kan bli så att det inte de här bankuppgifterna hamnar då i ett annat land än inom EU och det är ett problem, så därför har vi våra egna datahallar med våra egna servrar och egna lagersystem. Och där sparar vi alla kunduppgifter. Och det kan vara oftast väldigt känsliga uppgifter vid speciellt på inkasso till exempel. Där är mycket personuppgifter som samlas in och det här ställer krav på oss att vi ska upprätthålla ett gott skydd som de säger vad det innebär, men det hela gäller att se till att man skyddar kundens data så mycket som möjligt som det är. Det gäller verkligen att tänka till, hur vi sparar data.

00:10:46 Interviewer

Vad tycker du är viktigast när ni jobbar med informationssäkerhet.

00:10:52 Interviewee

Det vi har märkt är att omvärlden har blivit en.. eller vi har blivit en måltavla. Kanske vi har varit det hela tiden, men nu är det ännu tydligare skulle jag säga. Att de man tror att man, ja att hacka en bank eller lura en bank och göra saker att man skall då tjäna pengar på det. Och det har visat sig att de har lyckats med det. Och det gör att intresset av att försöka, jag säger hacka men det finns så många förfaringssätt i det här, det är allt från att lura våra kunder till att försöka fysiskt komma åt våra saker. Men det har ökat enormt de sista åren och det är nog för att bankerna har varit dåliga på säkerhet och de har blivit av med pengar. På grund av att det har gått att lura dem helt enkelt. Och vi ser som sagt speciellt mot privatpersoner att det förekommer både att man ringer upp folk och säger att de är från oss. Ett modus som dykt upp nu är att man ringer och säger att man är från inkasso och då blir folk lite "åh hjälp. Vad har jag gjort nu? Ja, men det är den här fakturan nu som du inte har betalat och så. Men jag har inte nått att betala. Men jo betala den nu." Och det där är någonting som vi gör allt för att informera om att nej, vi ringer aldrig upp en kund oavsett vad det är. Vi begär aldrig ut någon bankid, uppgifter om folk och sådana saker. Det är ett modus som har ökat väldigt. Och då går man gärna mot lite äldre personer som är IT ovana och osäkra, och så låter man väldigt övertygande och man har väldigt mycket argument för att varför skulle du lämna ifrån dig dina bankuppgifter eller bankid eller liknande?

Så där har vi jättestort informationsansvar, att informera om sådana här modus. Och som sagt, vi jobbar väldigt nära samarbete med polisen och sådana saker också när det gäller för att försöka stoppa det helt enkelt. Och även med leverantörer. Vi har till exempel ett nära samarbete med Telia på grund av att de kan spåra vilka operatörer som försöker fejka båda telefonnummer och då kan Telia stänga av dem mindre seriösa operatörerna när de ser vem det kommer. För man kan luras med det. Det här med att det syns i vem som ringer i telefonen. Det är väldigt lätt att lura nämligen om man är operatör.
Man går också hem till kunden. Man ringer först oftast, men sen då vet man var de bor och då går man dit och knackar på dörren och säga att ja, men vi hjälper dig. Vi kommer till dig såna här saker, men alltså bara de egentligen vill, det är att får de att knappa in den där bank eller bank IDt, så då tömmer man, oftast sitter de parallellt och tömmer kontot hos kunderna.
00:15:31 Interviewee
En annan sak är att använda, som vi börjat använda, det är 2 faktorer. Då måste man göra någonting mer än att bara logga in. Det här QR koden som dyker upp och då måste du med en annan enhet att kunna scanna den där QR koden. Och det är ett sätt att se till att det är du som sitter bakom din device, till exempel. Ja, det försöker vi också då att alltid ha dubbla inloggningar man ska kalla det. Användarnamn och lösenord har nästan helt försvunnit utan du har bankid oftast, men sen krävs det kanske ett sms med en kod eller att använda något autentiserings program för att godkänna att du får komma in. Fler och fler inser att det är den vägen måste gå, för att stoppa det här.
00:16:45 Interviewee
Men, sen kan jag ju säga vi, vi gör någonting som kallas för sårbarhet scanningar också. Vi utifrån gör kontrollerade skanningar av våra nätverk och system för att leta efter sårbarheter, alltså kända sårbarheter eller saker och ting som är fel konfigurerade. Och vi gör även det från insidan så att vi har skannings motorn sittande på insidan av nätverket och skannar även våra servrar på insidan. Och det här gör att vi får en bild på hur sårbar är våra system för en attack. Att det är någonting vi ser ökar lavinartat, det är försök till hackning. Förr var det väl kanske att man trodde den typiska hackaren, det var en överintelligent ungdom, den bilden håller helt på att försvinna. Nu är det stater ner till riktiga organisationer, alltså företag som sitter och gör det här konstant. Och det finns några riktigt allvarliga rapporterade incidenter som har hänt. Och då har man kommit fram till att det är faktiskt en stat som ligger bakom och jag kan säga det, för det är ingen hemlighet. Det är liksom Kina och Ryssland, de är de 2 stora aktörerna på det här, men även andra.
00:18:41 Interviewee
Så det är en viktig del. Sen har vi någonting som kallas för frat intelligens och det är ett annat sätt att försöka stoppa buset i dörren och det är alltså att vi köper tjänster där Sveas namn.. De letar konstant över hela nätet, även i darkweb efter Sveas namn som uppkommer i vissa saker. Och då kan vi helt plötsligt hitta på darknet till exempel att det finns inloggningar till våra system för att köpa för 19 dollar. Och då har vi en möjlighet att kunna se ja vad är det här? Jo, är det något allvarligt eller vem är det som har blivit utsatt? Förekommer vårt namn i suspekta chattgrupper till exempel. Det är såna information vi får. Intelligent hot analys kanske man kan kalla det. Men man får faktiskt väldigt mycket uppgifter på de här systemen. Och man kan hitta då och börjar det bli en stor diskussion om hur man tar sig in i ett visst system eller att Svea är utsatt för någonting. Det började att pratas om det här först innan det sker en attack. Och vi kan till exempel hitta personen som jobbar hos oss som har gjort saker. Vi har haft utvecklare som har lagt upp kod till exempel. På nätet för att de vill kanske ha hjälp, de har fastnat i ett problem och lägger upp kod som inte alls är något bra att vem som helst kan se. Så med den här varningen får vi upp att den här utvecklaren, han lägger upp saker i en chattgrupp för att försöka få hjälp, medans i den där koden har lagt upp det står i våra servernamn allt möjligt som man inte vill sprida utanför huset.

00:21:26 Interviewer
Vad gör ni om ni ser att en utvecklare har lagt upp kod?
00:21:29 Interviewee
Då får han en tillsägelse att ta bort det han lagt upp helt enkelt. Och det kan säga det händer inte ofta, men det händer ibland. Men det är mer vanligt att vi hitta inloggningar till våra system för försäljning. Men vad vi har upptäckt hittills, är det inga nya grejer utan det är gamla grejer som är borta för länge sedan. Men det är klart om det är någon som kan betala 19 dollar har de ändå tjänat pengar på någonting som är värdelöst. Men det vet de inte när de köper det. Så det är ett viktigt arbete för oss att göra så här.
00:22:25 Interviewee
Vi har också till exempel scannat nätet efter våra bin nummer, den första delen av kontokortsnummer. Det bestämmer vilken bank det är som har gett ut de här. Och vi är också kortutgivare så att då letar vi efter nätet efter de jag tror är 6 första siffrorna i ditt kontokortsnummer. De är inte hemliga på något sätt det beskriver bara vilken bank det är som ger ut de här korten och ett sätt att scanna nätet på kontokortsnummer. Det är att finns det en läcka någonstans med våra kontors nummer så är det väldigt intressant att få reda på det i tid. Och det hittar vi ibland. Och då är oftast kunder till oss som är drabbade, de alltså blivit av med sitt. De har knappat in sitt kontokortsnummer någonstans som har kommit på villovägar och när vi hittar sånt, då spärrar vi sådana kontokortsnummer, så att de inte går att använda huvud taget. Och vi skulle då upptäcka en större läcka av kontokortsnummer, också på det här sättet, och i tid att kunna stoppa det. Det här är inte vanligt tror jag att man gör det på svenska företag. Men som sagt, vill man ligga lite i framkant så måste man lägga lite pengar på den här typen av skydd. För det här traditionella skyddet med en brandvägg och det finns kvar men det är så mycket annat som vi också behöver göra för att skydda oss.
00:24:44 Interviewee
Det är lite tvingande då, dels för att vi sparar kortdata då, kortföretagen ställer krav på aktörer som sparar kortdata då, och vi sparar mycket kort data. Så vi har till och med en årlig granskning av ett av kortföretagen som utsett en granskare, de kommer in och tittar på hela kort hanteringen. Allt från hur vi anställer personal, till att utvecklarna måste vara utbildade, men också på säkerhet. Hur ser det ut i brandväggar? Hur ser det ut i databaserna? Hur krypteras kort numret? Hur ofta byter ni nyckel i de här datorer som krypterar, bara kryptera kortnummer, det är speciell hårdvara som gör det som är extra säker då att kunna göra det extra svårt. Så att då blir vi granskade utifrån det perspektivet varje år.
00:26:21 Interviewee
Sen gör vi egna penetrationstester. Alltså vi köper från företag. Folk som sitter och försöker ta sig in i våra system helt enkelt. Och de sitter och försöker använda kända sårbarheter och försöka ta sig vidare in. Kostar rätt mycket pengar, men vi känner att det är vi är tvungna att göra. Dels ur regulatoriska skäl men också för egen vinning. Vi har så otroligt mycket olika system så att det är svårt att skanna allt. Men vi försöker verkligen ta de här riktigt allvarliga publika systemen att vi sårbarhets testar dom. Inte bara med automatik eller system som kollar, utan med fysiska personer som sitter och försöker ta sig in. Det är nog någonting som kommer att bli större krav på i framtiden. Man ser redan nu i regelverken att det kommer krav från regelsättare här. Och det är mycket från EU skulle jag säga att det kommer bli krav på sådana här penetrationstester. Så de företagen där ska man köpa aktier då kanske.
00:28:04 Interviewer
Ja, det är smart med demonstration tester. Är det då just specifikt på systemen och är det ni använder? Eller utför ni också användartestning?
00:28:13 Interviewee
Ja eller nej inte så mycket, utan det är bara systemen. Man har diskuterat att göra sådana här lite större, alltså där man försöker att ta sig in i lokaler och sådana saker. Men vi har det inte

egentligen. Jag tyckte att inte det är riktigt värt för oss, för vi är inte riktigt den typen av verksamhet. Och våra datahallar, de är så skyddade genom att vi köper den tjänsten och då är det företag som har både säkerheten och det är riktigt svårt att komma in där. Vi känner att det inte är viktigt att någon skulle komma in i våra lokaler. Ja, det är nog inte så jättesvårt egentligen. Vill man så kommer man in. Men vad ska man göra när man är inne där då? Ja, man kanske kan sno någon dator eller någonting, men det är inte så mycket mer man kan göra.

00:29:43 Interviewee

Då är det värre med hotbilder då för att det är någonting som vi ser ökar också, men har förvånansvärt varit väldigt lite hos oss och det är inkasso. Det är mycket hot på telefon. Att du skriker och gormar och du ska göra allt möjligt med den personen som du pratar med. Men det att gå till att göra en fysisk handling, det har vi sett väldigt lite av, men det är ett hot som vi tar på allvar. Därför tränar vi receptionspersonal, vad ska de göra om det kommer någon som är hotfull. Det är viktigt att tänka på sådana saker, men som sagt, det händer inte. Det händer väldigt lite incidenter på det, men jag kan säga att de personerna som sitter på callcenter och tar inkasso som talade om. De har fejkade namn där, till exempel. De berättar inte vad de heter på riktigt utan de har sina artistnamn. Man ska inte kunna hitta de här sen. Det är jag skulle säga att det är något i månaden har ifall som är ett hot som incidenter rapporteras och ibland polisanmäls det också för att det blir för grovt. Speciellt med våran verksamhet. Vi jobbar mycket till de här stora parkeringsbolagen också. Vi sköter deras parkerings hantering och det är klart har man fått en p-bot kan man bli skitsur. Men att en sådan kund ska bli så sur så att han verkligen gör något fysiskt det är rätt långt till det, men vi måste tänka på. Det är mer våran riskbedömning.

00:32:24 Interviewer

Med ert arbete med informationssäkerhet, har Covid-19 påverkat er försäljning eller arbete?

00:32:39 Interviewee

Ja, e-handeln har gått upp väldigt mycket sen det började. Det ger ringar på vattnet när det gäller faktura försäljningen också då att vissa företag skickar mer fakturor medans andra skickar mindre fakturor. Och där är typiskt besöksnäring. Även bolag och sådana saker där har minskat väldigt medans, men det växer upp av att, ja prylar om man säger så allt från bygghandel till allt möjligt så har det ökat väldigt mycket.

Så vi har inte som bolag märkt av. Vi har snarare högre försäljning än vad vi hade innan. På alla fronter, skulle jag säga. Så att det är, det har inte slagit alls emot oss. Jag skulle säga att det är mycket mer att göra nu under den här tiden.

Och det är klart sen ställer det lite krav på oss också. Ja, som att vi sitter hemma, de flesta av oss och jobbar. Numera är det två år men ser vi att försökt att hålla kontoret med så lite folk som möjligt då. Vissa avdelningar har inte möjlighet att jobba på distans som callcenter till exempel. Det gick inte att flytta systemet utanför huset. Men de har ju fått mer plats och sin tur och när de flesta sitter hemma så kunde vi sprida ut dem lite mer på kontoret. Och vi viss personal inne någon dag i veckan, men som sagt för mig var det väldigt länge sedan jag var inne. På gott och ont skulle jag säga. Det är rätt skönt att slippa resväg och så där. Men också säkerhetsmässigt så har det ju inneburit att det är med datorer som vi måste ha koll på än vad vi hade innan. Förut var det arbetsstationerna på jobbet inom låsta väggar. Som man hade stenkoll på, nu är det massor med hemdatorer som sisådär säkerhet kan man säga.

00:35:39 Interviewer

Har ni policies på det, BYOD?

00:35:44 Interviewee

Det har vi gjort precis. Vi har både via policies och best practice. Vi försöker hjälpa våra medarbetare med att se till att när ni har virus på eran dator att de har fått virusskydd av oss då så att säga för att säkra upp sin operator också. Men det är svårt. Det är inte våran

utrustning, vi får inte riktigt göra allt vi vill med en medarbetares privata dator. Fast de använder ändå i tjänsten, det blir lite en gråzon. Alternativet var att alla skulle få en företagsdator, men det var inte realistiskt att få in så många på så kort tid. Vi fick in en bråkdel. Jag tror vi köpte 50 laptops precis när det startade. Men det skulle nog behövas några 100 till, men det var inte praktiskt. Det gick inte. Det fanns inte att köpa, helt enkelt.

00:37:11 Interviewer

Ja, men då måste man jobba från ett VPN eller liknande lösning när man jobbar hemifrån?

00:37:20 Interviewee

Ja varje användare loggar in då, via VPN till sin stationära dator på arbetsplatsen då. Det är först där på den datorn som de kan komma åt de systemen som de behöver jobba med. Det går inte att göra via hemdatorn, det enda man gör det är att man startar upp VPN anslutningen och ansluter till sin arbetsstation på arbetsplatsen. Och det gör att vi inte har flyttat ut någonting utanför vårat nät. Sen visst du kan ta ett dokument och lägga på din egen dator. Men där har vi försökt med policy.

Sen är vissa saker jobbiga då vi har en del såna här procedurer där man ska skriva under vissa dokument och såna saker, och det är lite jobbigt. De flesta har inte skrivare, hur ska man sen scanna in, ännu färre som har scanner hemma. Så praktiska problem har uppstått, men det var som sagt mycket enklare, vi har släppt lite på det. Och det är inga som säger någonting egentligen. De vet varför.

00:39:19 Interviewer

Har ni bestämda standarder som ni följer i företaget?

00:39:34 Interviewee

Ja. PCI DSS måste vi följa genom att vi hanterar över flera miljoner transaktioner så att vi levererar rätt på PCI DSS. Och det är för att det har så stora volymer så vi har högsta nivån på granskningen av det.

Sen är er vi inte ISO 27001. Men jag kan säga att regelverken från finansinspektionen bygger mycket på ISO 27001, så ja vi måste följa dem. Sen inkasso, de ligger under Datainspektionen för de har kontrollmyndighet och de ställer sina krav. Men som sagt, vi har Finansinspektionens krav på oss och jag skulle säga att de är snäppet tuffare än vad ISO är. Vi får kontroller från finansinspektionen på oss.

Sen har vi också en intern granskning av verksamheten som görs varje år och det är beställts av våran styrelse. Då är det en extern aktör som går in och tittar. De tittar mycket på finansiella verktygen också då, men också på IT. Och tittar på att vi följer vårt ledningssystem. Att vi gör det vi har sagt att vi ska göra. De går in och tittar i virusskyddet till exempel. Hur många här som har virus programmet installerat på sin dator då så går de till den datorn och tittar. De nöjer sig inte med att man säger att ja, vi har virusskydd på alla datorer, det räcker inte, de ska se med sina egna ögon. Man kan tro att de ska skärpa oss, men de ska faktiskt hjälpa oss att bli bättre.

00:42:29 Interviewer

Är det så att ni på något sätt kategoriserar risker på ett specifikt sätt?

00:42:36 Interviewee

Ja, det måste vi göra. Det är även information som vi måste kategorisera, hur skyddsvärd informationen är, och det finns olika nivåer. Och jag kan inte säga.. banksekretessen är nog den högsta. Den är väldigt tufft och vara vilken information kategori den ska hamna under. Den är tuff.

Ibland är det jobbigt för man kan inte ens försvara sig. Om, det är en kund som skriver någonting om oss på internet. Säg att vi har sett att den här kunden håller på med bedrägligt beteende, och vi stänger av den kunden. Ja då sitter de och skriver i sociala medier att Svea Ekonomi är en skit bank, de gör ditt och datten. Och då kan man inte ens försvara sig. För att

banksekretessen sätter stopp, vi kan inte ens förklara varför den här kunden har blivit avstängd. Det får man vara jättenoga med.

00:43:59 Interviewer

Okej, ja.

00:44:04 Interviewee

Samma sak gäller i systemen också. Vi loggar väldigt mycket data vi har nästan 50GB data varje dygn från våra system som vi analyserar. Vi har en så kallad 24/7 som de sitter och tittar på larm från våra system då, det kallas SOC, står säkert för något fint. De sitter och tittar 24/7 på all loggdata som kommer från andra system och letar efter mönster som sticker ut. Och då blir det ett larm om det är någonting som, det kan vara driftmässigt men också säkerhetsmässigt, att det ser att någonting håller på att hända. Då får vi ett larm att nu är det någon som försöker att göra någonting åt ett system. Då kan de agera, de har mandat att stänga ner saker och ting på bums de kan dra ut sladden om det är riktigt allvarligt att dra ut sladden direkt.

Men det vanligaste är att de sorterar och vi eskalerar till berört affärsområde eller kanske till någon systemtekniker eller DevOps, alltså utvecklarnas supporttjänst kan man kalla dem. Där tittar de på, vad är det som händer? Varför blir det fel på den här hemsidan? 10 gånger i sekunden, så blir det ett fel här. Vad är det som händer? Är det en attack eller är det en bugg eller vad är det?

00:46:10 Interviewer

Hanterar ni risker olika beroende på vilken nivå den har eller kategori?

00:46:21 Interviewee

Nej, jag skulle nog inte säga. Men det är klart det som upptäcks av SOC:en, de gör ju en första bedömning av hur allvarligt är det här. Kan vi leva med det en stund, några timmar eller ett dygn eller sådär. Så de gör den första kategorisering av felets art. Och sen är det vissa tidpunkter. Jag menar Black Friday till exempel. Då har vi personal på plats, 24/7 också. Det får inte fallera, ingen av systemen får gå ner. Det är sån viktig period för våra handlare då, att det verkligen funkar och då sitter man och tittar lite grann på belastningar. Även nu utvecklare för situationen helt enkelt för att om det är någonting som händer så ska de kunna agera snabbt. Och julhandeln är också sånt där. Det är en viktig period för våra webbhandlare. Då får det inte fallera.

00:47:49 Interviewer

Vad händer om datan inte är tillgänglig under denna period? Exempelvis om systemet ligger nere?

00:47:59 Interviewee

Ja och det är våran mardröm, därför jobbar vi väldigt mycket med lastbalansering. Att alla system ligger dubbelt helt enkelt eller ännu flera gånger som våra webbservrar. Jag vet inte hur många webbserver igen och mer belastningen ökar, desto mera servrar dras igång. Och det är någonting som användaren aldrig upptäcker, för de går bara till en sida, men för oss är det så är det antal servrar som går igång då. Och det är de här lastbalanserare som fördelar kraften och det är därför man blir lite förvånad när man ser den här regionens app för vaccinationer som gick ner här? Vad snackar du om underhåll i 50 000 användare vill gå in och boka vaccinationstider. Och så klarar de inte det och hundrafemtiotusen, det är ingenting. Men en konsert som säljer till exempel när du släpper biljetterna till någon nya konserter, eller nya häftiga gympadojor, lovar jag att det är mer folk som vill köpa dem, än folk som vill boka vaccinationstider. Det går att bygga system som verkligen klarar stor belastning. Det är bara att man måste tänka till lite grann innan.

Men det är mardrömmen. Det är så mycket pengar, det får verkligen inte hända så därför dubblerar vi systemen också så går en brandvägg sönder, då tar den andra över och det märker aldrig användaren att det händer. Och det är ett sätt att vi ska kunna hålla underhåll på våra

prylar också. Det är att vi kan stänga av en maskin, säg en brandvägg, uppdatera den och sen slå på den igen. Och sen stänger vi ner den andra som var igång och så uppdaterar vi den och så slår vi på båda två liksom. Så gör vi kontinuerligt hela tiden med alla våra system. Så att vi ska kunna uppdatera saker och ting i lugn och ro istället för att behöva stänga ner ha sådana servicefönster där ingenting funkar mitt i natten.
Det är någonting när man tittar på webbhandeln, är det att när man tror att ingen ska handlas och ni skulle bli förvånade hur mycket försäljning det är på nätterna till exempel. Folk kan inte sova, sitter och handlar istället. Så services mitt i natten är nästan sämre än mitt på dagen. Fantastiskt hur beteendet har ändrat sig. Förut stängde affärerna klockan 6. Man tänker att de borde gå och sova någon gång. Eller så har de vaknat kanske att börja hända? Jag vet inte, men det är väldigt hög försäljning. På nätterna kan jag säga. Det är förvånansvärt mycket.
00:52:22 Interviewer
Du pratade om att ni loggar 24/7, finns det specifika kontroller som kollar dess loggar? Och är det någon som administrerar detta?
00:52:50 Interviewee
Man letar efter mönster i de här loggfilerna. Det loggas otroligt mycket data då, men man letar efter ett mönster som sticker ut och det är det som är nyckeln i det här. Att få 100 rader loggning som säger OK dem är ointressanta, men det kommer ändå mitt i där som säger inte okej. Det är den vi vill fånga upp och därför är det en så kallad AI motor egentligen som sitter och letar efter det här när mönstret inte stämmer, och då kan en tekniker titta på det. Det har hänt rätt mycket på den fronten just att leta efter ett visst mönster och till exempel om det är en enklare saker att den server stammar eller någonting sånt där. Det är också ett larm då till SOCen då, och då kan de eskalera det eller så kan de starta om den maskinen och ser vad som händer, går den upp igen och ser frisk ut? Och ibland måste en tekniker titta.
Men det här att leta efter ett mönster från många olika system. För det är inte bara servrar, utan det är brandväggar och det är virusprogram och det är även all sårbarhet. Scanning skyfflar vi in i de här systemen för att leta efter saker och ting. Det har blivit en väldigt viktig del för oss att hitta saker som går snett. Och ju mer vi loggar på korrekt sätt, desto bättre upptäcker vi hot i tid, för det är det det är frågan om hela tiden liksom. Skulle vi få till exempel en ransomware attack emot oss, då skulle vi upptäcka den väldigt fort och kunna stänga ner delsystemet eller den datorn. Det upptäckts väldigt fort. Tiden är helt avgörande, om man skulle lyckas få in någonting. Och peppar peppar, så har vi aldrig sett något sånt men det stoppas i dörren av så många kontroller som vi gör. Om någon skickar ett mail med en länk till oss, då är detta våra system, den packar upp det här mejlet provar alla länkar om de ser suspekta ut innan det släpps vidare. Här fastnar allt sånt här skit skulle jag säga, det kommer inte vidare. Det kommer lite användaren. Baksidan på det där, det är jättebra, men det är alltså kostsamma system. Vi får lägga ner rätt mycket pengar på såna där saker man kan tycka kanske i onödan. Men det är som verkligheten här, det är så det ser ut.
00:56:44 Interviewer
Loggar ni även vad era anställda gör?
00:56:50 Interviewee
Nej, men där får man vara lite försiktig. Alltså det loggas. Det är klart, går de in i ett system och gör någonting då är det vissa saker som loggas, men det är mera, inte vad de har gjort, kanske utan mera, i ett beteende från systemets sida. Att den har gjort rätt för att för att upptäcka felaktigheter i programvara och såna här saker, loggar systemet vem det är. Loggningarna har ett stort verktyg för dem som jobbar med fraud också, alltså med brottsligheten, för de vill följa ett mönster. Hur har den här kunden betett sig? Och då letar efter ett visst spår i våra loggar att den här personen han har suttit på den. Våra brandväggar sparar all information om den trafiken som har varit så kan man säga direkt att den kunden som loggar in här, satt på den här datorn i det här området och sånt är i en brottsutredning.

Polisen är väldigt intresserad av att få del av det att de vill ha det här elektroniska spåret på kunden. De använder såna VPN tunnlar då som de köper och det är klart, vi ser att trafiken kommer från en sån här VPN tjänst, då vet vi att det är ett beteende. Men sen har vi lyckats se att några gånger har de glömt att slå på den här VPN tjänsten och då kommer trafiken från deras dator och då kan man ringa in. Alltså, det är några hus nära så kan de ringa in den polisen och då kan polisen ta det här datan från flera aktörer och så kan de agera. Och det är inte ovanligt att vi hjälper polisen jättemycket med att ta fram de här elektroniska spåren av kunden. Men vi får bara det som händer emot oss, att kunden har gjort det mot oss. Sen kan polisen ta information från flera. För oftast de här brottslingarna de går mot, jag ska inte säga alla banker med nästan, och det gör ju det att polisen får ett väldigt bra underlag då från flera banker som kan se att den här kunden kommer ifrån den här datorn, och försökte göra samma sak mot de andra bankerna som man har försökt mot oss. Och då bygger de sina åtal på det där sedan. Medans vi lämnar bara våran del. Givetvis, för det är det vi har information om. Så det använder vi väldigt mycket och polisen.

01:00:16 Interviewer

Hur undviker ni humar error i systemen?

01:00:39 Interviewee

Hela strukturen bygger ju på... Vi har mest Microsoft miljö då så det är Microsoft AD som vi använder, som bestämmer vem och vad får en användare komma åt. Där är det mycket group policy, som det kallas. När en ny medarbetare börjar, då får man berätta: Vad ska den här medarbetaren göra? Vilka system ska den få åtkomst till? Då blir det så att det blir en nivå som sätts på medarbetaren. Det här kan du se, du kanske bara kan läsa informationen från ett visst system.

Och banken, till exempel. Du får inte se alla kunder i systemet. Du kanske bara får se dina kunder i systemet för att dela upp det, så det är så beroende på vad du tittar på. Och det är klart en inkassohandläggare får inte se in inloggningen på den här kunden till exempel. Det är såna där vattentäta skott emellan. På gott och ont, ibland skulle man kanske vilja ha kundens hela engagemang för att kunna hjälpa kunden på ett bättre sätt. Men det går inte. Utan du som medarbetare har tillgång bara till en viss del. Och sen har vi också system som hanterar lösenord till de här mest känsliga delarna som aldrig mista törs lösenord och såna saker. Det ligger i ett speciellt system, så det är ingen tekniker som har ett lösenord till en server, till exempel. Utan han måste gå via det här systemet att begära åtkomst via den. Då ser man en fullständig loggning vem det som har gått in på den server som administratör för att göra någonting. Det ser därmed våran SOC, så att vi får ibland larm att det är en konstig användare som går in i ett väldigt känsligt system. Då får vi ett larm därifrån och då får vi säga ja nej, men det var en tekniker som gick in där för att göra någonting. Och då är det system som normalt sett ska ingen gå in där helt enkelt. Men det är fullständig loggning på vem som gör saker och ting. Det är jätteviktigt. Man vill inte ha en tekniker som kan göra något dumt själv. De letar vi aktivt efter. Visst kan vi lita på våra medarbetare, det måste vi göra, men det största hotet vi har det är faktiskt en medarbetare som på något sätt skulle bli sur och göra något dumt liksom. Därför är det väldigt viktigt att man loggar all aktivitet när det gäller den här inloggningen.

01:04:43 Interviewer

Har ni flera metoder för att kryptera eller flera ställen där ni ser att det är viktigt, utöver känsliga nätverk?

01:04:50 Interviewee

Alltså den tyngsta krypteringen vi har det är för kort data, för där är HSM då, alltså det är hårdvara som krypterar. Och där bits i de här krypto nycklarna med jämna regelbundet. Sen är det andra nivåer och kryptering som inte är lika tufft, men våra certifikat som vi köper då som sitter i våra webb. Allt som har med webben att göra är idag certifikat. Det finns ingen trafik

som inte går via https från oss. De certifikaten har ungefär 2 års giltighetstid innan de byts ut. Och här försöker vi då att inte tillåta för dåliga protokoll. Om man säger att man inte tillåter en viss nivå, då stänger man ut det ett antal webbläsare och mobiltelefoner till exempel. Men någonstans måste man dra en gräns och det är lite byter bransch. Vi tittar på vad andra aktörer gör också. Apple gick ut med till exempel att de kommer inte tillåta TLS 1.0 nu till exempel på sina enheter. Ja, men då blir det jättebra. Då stänger vi också av TLS 1.0 för om Apple som stor aktör av mobiltelefoner inte tillåter det i sina telefoner, ja, men då behöver inte vi tillåta det. Sen tittar man på webbsidor, till exempel internet Explorer 6 till exempel. Har man det kvar då kan man knappt surfa idag, det finns knappt någon sida som klarar den bra också. Nej, men varför ska vi tillåta den för då? Nej, men då stänger vi ner den. Så har man inte Internet Explorer 6, då får man ju upp en sån här sida där du måste uppgradera blind browser till en nyare för att det ska fungera. Det där är avvägningen. Om jag fick bestämma om vi skulle vara supersäkra, då hade jag tagit det högsta säkraste direkt, men då är det kanske är så att det är rätt många användare som inte skulle kunna komma in. Och det är där då verksamheten vill ha att alla ska komma in. Och det är någonstans vi måste hitta en rimlig nivå på säkerhet och delning. Ibland är det lite diskussioner om vi verkligen ska tillåta den här browsern.

01:08:55 Interviewer

Okej.

01:08:58 Interviewee

Det är skillnad på om det är en känd sårbarhet, det triggar mer, men också om det har publicerats ett verktyg för att använda på den här sårbarheten. Då har man öppnat dörren. Jag menar att det finns en sårbarhet, det betyder inte samma sak som att nu kommer alla att börja använda sårbarheten. För att det är så ofta så tekniskt svårt för att det är så få personer som verkligen kan utnyttja de där även bland hackare. Men om det helt plötsligt finns verktyg, alltså någon lägger upp på internet, verktyg för att använda den här sårbarheten, då helt plötsligt kan man med bara lite kunskap använda det här verktyget för att utnyttja den här sårbarheten i den här browsern, eller om det är mot ett system. Då flaggas den mycket högre, den får mycket högre värde och bör fixas snabbare då, sårbarheter som kanske är jätteallvarligt men där det inte finns verktyg för att använda den. Det är också en bedömning vi gör. Vi tittar inte bara. För sårbarheter har ju en tiogradig skala. Idag hur allvarliga de tycker att gå med. Och får man 10, då är den jätteallvarlig. Men det kan vara väldigt svår att använda. Och det gör att man får ett lägre värde då när man tittar på sannolikheten att det används och den skalar ner från noll till 100 tror jag, där 100 är väldigt högt då. Och saker som ligger över 70 skulle jag säga, att då börjar vi titta på det väldigt noggrant för då har de fått så hög sannolikhet att de kan användas. Då börjar de bli intressanta att stoppa, och lägga ner tid och utveckling och allt vad det innebär för att få bort den där sårbarheten. Men har vi en sårbarhet som kanske har 9 men kanske bara 27 i sannolikhet att användas. Ja, men då behöver vi kanske inte fixa den på en gång. Sannolikheten att den ska användas är så liten. Den finns där, men den är så liten och det är sådan bedömning vi gör hela tiden.

01:11:36 Interviewer

Så det är hur allvarligt det är blandat med sannolikhet?

01:11:44 Interviewee

Ja, det är lite klassisk riskhantering. Det här får vi hjälp med av de här systemen som vi använder. Det är flera aktörer på marknaden som debatterar de här sårbarheterna. Det är en organisation som sätter vad de tycker vilken nivå sårbarheten ska ha. Det är till exempel den här Microsoft är sårbarheten som dök upp för någon månad sen som var väldigt omskriven, eller Microsoft Exchange mot e-postservrar. Den sårbarheten hade väldigt hög sannolikhet att man skulle utnyttjas. Till och med att Microsoft Sverige ringde till oss och sa att: ni vet väl om att den här finns att ni behöver uppgradera. Det är nog första gången det har hänt faktiskt.

Den var väldigt hög sannolikhet att den användes. Och det syntes också, det var väldigt många, Microsoft tog fram till och med specialverktyg för att man ska kolla sina e-postservrar så att den här sårbarheten inte fanns, och det är inte ofta Microsoft gör såna grejer. Så det var väldigt allvarligt. Där var det väl ett aktivt. Och det kallar de för (?), alltså att det inte finns en lösning på sårbarheten. Och de är alltid allvarliga och då har man ingenting, då kan man inte ens stoppa. Då får man leva med det. Och jag kan säga, där är det de som är riktigt duktiga och då är det länder. Det är bara de som har de ekonomiska musklerna att använda sådana sårbarheter, för de har mycket pengar att de har mycket personal som kan klura ut hur de ska använda den där sårbarheten. Det är inte någon hemma på kammaren som gör, oavsett att man är väldigt duktig. Man behöver väldigt mycket, både kunskap och datakraft för att lyckas. Så de klassas väldigt högt de där typen av svårigheter. Men sen är ändå sannolikheten att den används är väldigt låg. Jag kan tänka mig få folk som jobbar med försvarshemligheter och såna här saker, de agerar något väldigt annorlunda här vad vi gör som mindre nischbank, eller vad vi ska kalla oss. Det är skillnad. Vad är skyddsvärdet?

01:15:31 Interviewer

Har GDPR påverkat ert arbete inom er verksamhet? Hur har det påverkat ert arbete med informationssäkerhet?

01:15:55 Interviewee

Informationssäkerhet gäller ju hela bolaget och det är vårt ledningssystem som styr det arbetet och våra myndigheters krav på att vi följer ledningssystemet, dels att vi har ett ledningssystem och följer det. Det är jättelätt att skriva massa fina papper, men att verkligen göra det som står i de här papperen, det är det svåra. Det är det vanligaste misstaget de flesta gör. Det vi har upptäckt den hårda vägen är att det är bättre att skriva ledningssystemet som vi använder det, än att jag tvärtom, att göra en pappersprodukt. Vi kan skriva att vi är jätteduktiga, men det hjälper inte när vi inte gör det som står där. Så det är bättre att skriva ledningssystemet som det används och sen gradvis öka om det är någonting som man tycker att: nej, men det här vill vi nog bli lite säkrare på, eller det här vill vi förändra. Ja, men då ändrar vi ledningssystemet och det är inget svårt. Vi har olika nivåer i vårt ledningssystem, vi har de översta policies till exempel. De tas av våran styrelse och det är klart de är så luddiga så att de behöver bara titta på de här en gång om året och godkänna de ett år till. Men de är jätte svepande. Ja, vi ska ha en god informationssäkerhet, det räcker. Men sen har man ju dokument under då, både instruktioner och manualer. Och manualer är exakt de här systemen ska ha det och det. Och de är lätta att förändra, för de ligger på t.ex. mitt bord eller på den verksamheten som använder dem, så att de kan ändra de här i princip hur mycket som helst. Tanken är att policyn ska vara överst väldigt övergripande medans de här instruktionerna lite mer detaljerade men fortfarande rätt luftigt. Medans med manualerna, då är det exakt hur vi ska göra. Och då är det istället för att skriva en massa saker som man inte gör så är det bättre att skriva det man gör och sen får man fylla på liksom. Det är många som ljuger i de där ledningssystemen. Man tror att det är någon som ska titta i det här sen och så ska de läsa och vi ska göra så här liksom, men det gör vi. Det är jättelätt att skriva för mycket och få ett fint dokument än att få följa verkligheten liksom.

01:19:11 Interviewer

En mer generell fråga, finns det några säkerhetsaspekter som är unika för e-handelsföretag?

01:19:24 Interviewee

Nej, det skulle nog inte säga. Vi hanterar nog oavsett om det är handel eller om det är ett fakturasystem så det hanterar vi nog väldigt lika. Till exempel, alltid hög säkerhet på kundens, de som har lån och sparkonton och så, till exempel, men att de systemen måste också vara säkra så att kunderna inte ska kunna bli hackade och kunna bli av med pengar. Nu kan de inte riktigt bli det för att systemet kan inte skicka pengar hur som helst. Men skulle du hacka en spar kunds konto då kommer de kunna skicka ut pengarna till ett annat

kontonummer, och det är illa nog. Men det är aldrig så att de kan byta kontonummer på webbsidan, till exempel, för det är då du kan flytta pengarna någonstans som buset då kan utnyttja. Nej, jag tycker nog att e-handel sektorn har sina problem med tillgänglighet, men vi ser nog ingen skillnad på de. Det är lika allvarligt att ha en hackning mot webbhandeln som på sparkonton eller fakturasystem.

01:21:56 Interviewer

Tack så mycket. Är det okej om vi kontaktar dig om vi har några följdfrågor?

01:22:04 Interviewee

Ja, men gör det. Skicka era frågor där så ska jag försöka svara så gott jag kan och får, det är lite problemet med affärshemligheter. Om exakt hur vi gör. Men jag kan ändå måla upp hur branschen jobbar, eftersom vi är rätt lika. Vi ligger under samma regelverk och vi har rätt tuffa regelverk. Det är skillnaden mot annan webbhandel skulle jag säga. Finansiella verksamheten har haft finansinspektionen många år som har granskat oss och de har ställt krav som är lite unika på webbhandeln. Nu när EBU också kom in och med europeiska banken unionen, då ställer de tuffare och tuffare krav varje år. Och de tuffaste kraven man kan ha, det är från kortföretagen. Mastercard och Visa och det är det här PCI DSS då. Det regelverket är det tuffaste. Och det är många som sneglar på dem. Tycker att fasen vad de gör det bra liksom vi snor bitar av det där liksom och det ser man även på europeisk basis. Att det kommer mer och mer ifrån PCI DSS hur man ska hantera agera på hot och sådana saker. Det och där tror jag att vi som bransch, finansbranschen, skiljer ut oss lite grann emot övriga handel. Där du inte behöver tänka lika mycket på det, men är en byggfirma till exempel som säger att han skulle ha en egen webbshop och hantera betalningarna själv. De skulle inte alls ha den säkerheten som vi på finansbolag är tvingade att ha på grund av regelverken. De kan göra best practice, men vad är det? Och det är därför den normala webbhandlaren, han vill inte hålla på med det där när du kommer och ska klicka på betala. Då är en annan aktör som tar över.

01:24:43 Interviewee

Och det här har Klarna varit jätteduktiga på att komma in, men det är även i det segmentet vi här. Det är fler aktörer än vi, men då har du lämnat det, som webbhandlare, lämnar du över ansvaret på säkerhet och sådana saker till oss. Då behöver inte du oroa dig, då ska du göra det du är duktig på. Det är inte att se till att betalnings vägarna är säkra eller att du har en säker betalningssida. Det är värt att sälja den biten till oss då som håller på med det här dagligdags. De fyller på sina webbshoppar med deras produkter, och försöker sälja det så gott det går. Sen lämnar hela betalning biten till oss och även om kunden inte betalar. Vi kan erbjuda till exempel delbetalning och såna här saker. Det är ett sätt att ge mervärde till den här behandlaren, men en kund som vill dela upp i 4 betalningar, för då kan de då köpa de här sakerna så det är ju win win för båda två. Sen kan jag säga delbetalningar är det vi tjänar absolut mest pengar på, det är mycket avgifter och höga räntor. Det sämsta vi kan göra det är när ni betalar och väljer faktura att betala inom 14 dagar och betalar hela beloppet inom 14 dagar. Det är en det är en dålig kund. Förlustaffär. Medans den dag ni missar att betala den där efter 14 dagar. Det är då ni blir en riktigt bra kund. Det är lite cyniskt men det är så det funkar. För då börjar avgifterna bli höga och många. Så gör inte det, betala i tid.

01:27:21 Interviewer

Tack så mycket för din tid. Det var väldigt givande.

01:28:01 Interviewee

Absolut!