Guarding against cyber-attacks

A three-step framework

Martin Österberg
2019-05-13

Department of Production Economy
The Faculty of Engineering, Lund University

Introduction

The business environment is constantly evolving, and the last 20 years is when the digital format, and overall digitalization has become a necessity for doing business. The amount companies increase by the day, and all companies extend information with other companies in one way or the other. The data that circulate online and is exchanged between entities daily is inconceivable large. It is therefore understandable that there are criminals that are willing to exploit this. As the rate of digitalization increase, so does the amount of cyber crimes. Cyber criminals try to steal precious information by accessing company servers or cloud services. Criminals inflict company networks with code that encrypt files in order to demand ransom, they even attack countries by disrupting important infrastructure, the list can be made long. Malicious code is easily distributed, and the content can be change and altered to fit specific intentions. Inevitable, it is of the utmost importance that organizations are able to deal with this type of risks and threats. Otherwise, companies will have a hard time to maintain the trust of customers and partners, especially since companies often manage sensitive information such as company secrets, credit card details and personal information.

In light of this, there are three main research questions that together formed the general guideline of the project and served as the foundation from which the framework was built.

- How to protect against cyber attacks, as well as how to estimate risks and mitigate effects related to cyber threats.

- How to act during an attack, to repair/re-operate and contain the threat.

- How to work after an attack, to reassess security protocols and security strategies.

By addressing these questions, a framework with a holistic approach was created to support companies improve their cyber resiliency, in terms of preparation, incident management and post incident management.

Methodology & Empirics / Benchmarking

The methodology used in this project is mainly of an exploratory approach combined with an element from the descriptive approach, which is the gathering of qualitative data from surveys. Moreover, an exploratory study helps in understanding the critical issues of problems and are used to analyze a problem situation, evaluate alternatives and create new ideas (S. Sreejesh, Sanjay Mohapatra, M. R. Anusree, 2014). This method seemed appropriate since the main objective of the project was to create a framework. When gathering information for the framework, a literature collection was carried out. Information related to the research questions were acquired mostly through articles, journals and books via LUB search, as well as government web pages. The information from these sources influenced the structure of interviews and surveys, from which the empirical data were gathered from. Interviews were most rewarding, compared to the scarce response rate of surveys. Interviews were held over the phone with appropriate representatives from Deloitte, Ålandsbanken, Yubico and an anonymous logistics firm. The information generated from here were analyzed in accordance with literature in order to extract the most interesting aspects and actions. Simultaneously, some aspects and approaches covered in the interviews were integrated directly into the framework.

Conclusions

The framework that was developed in this master thesis is general in its nature and consists of the following three parts: (1) Organizational Structure and Mitigation Efforts; (2) Incident Response and Action Plan; (3) Recovery and Postmortem. These parts are all interconnected and together create a solid foundation from which companies can develop and improve their cyber defense strategies. The three part will be described further in next sections.

(1) In order to be on the frontier in the combat against cyber attacks all companies need programs for identifying potential risks and ensuring ongoing business activity, all interviewed companies agree on this. The framework therefore suggests that risk management and business continuity management is implemented and practiced within all organizations. Together, these two programs constitute the foundation in the framework. However, this is not enough, and the framework suggest a series of complementing actions. For instance, the concern of errors from employees is raised. It is very important that organizations train their employees and keep them up to date regarding cyber threats. To further limit mistakes and provide additional security the framework explains the importance of back end technology and monitoring. For instance, intrusion detection and prevention system (IDPS), and programs that identifies behavior anomalies. With all things considered, the objective with the first part is achieve a security structure that have different layers of equal importance, which is demonstrated by the following picture.

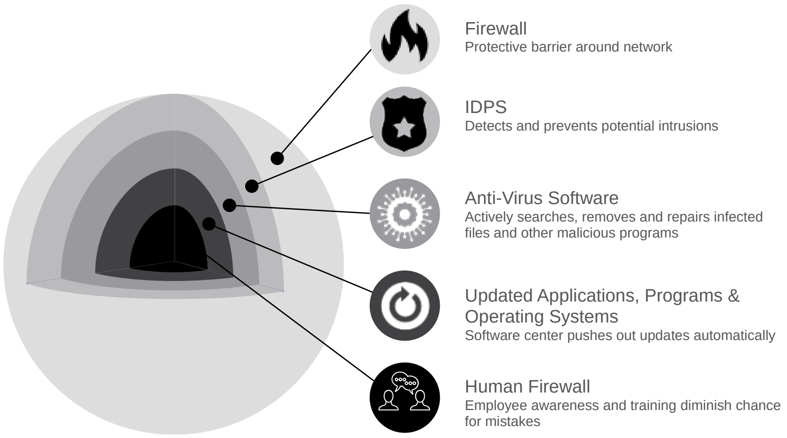
Firewall
Protective barrier around network
IDPS
Detects and prevents potential intrusions
Anti-Virus Software
Actively searches, removes and repairs infected files and other malicious programs
Updated Applications, Programs & Operating Systems
Software center pushes out updates automatically
Human Firewall
Employee awareness and training diminish chance for mistakes

Figure 1. Security structure with the different layers (Österberg, 2018)

(2) Companies need a response if a cyber threat were to be realized. The plan has to be fast and efficient. For every minute malicious programs or code harm company systems the cost can grow immensely. The previously mentioned business continuity management program is a holistic program that is very helpful in situations where disruptions of any kind is the result. It is therefore very important that this function properly, however the framework also explains a response to cyber attacks specifically. This is called an incident response plan (IRP), the objective of this plan is to ensure that cyber threats are detected, contained, and that systems are rapidly restored to normal function (Jadhav Harsh, 2018). If a threat is realized, the incident response plan is invoked, and a response team gather quickly and initiate the pre-determined and rehearsed recovery processes.

(3) When the treat has been eliminated and the functionality of processes and systems have been restored is important to understand what made the incident possible and what could have been done differently. This should be done through post mortem meetings where all relevant parties should be present. The goal during this meeting is to evaluate if the existing incident response plan is functional and an to create an overall understanding of the entire incident. Through discussion and evaluation, it will become clear were the problems lie and adequate measures can be taken in order to cope with them. When sufficient actions have been taken it is imperative to test the plan that is actually functions as intended, otherwise it has to be altered and tested again until desired effect is achieved. The following picture describe the correlation between the different parts and their content.

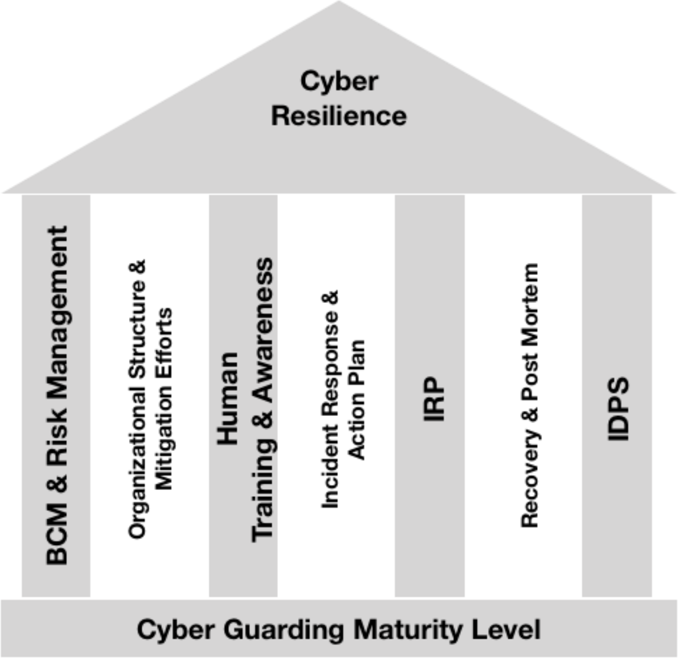
Cyber Resilience
BCM & Risk Management
Organizational Structure & Mitigation Efforts
Human Training & Awareness
Incident Response & Action Plan
IRP
Recovery & Post Mortem
IDPS
Cyber Guarding Maturity Level

Figure 2. Correlation and structure of the framework (Österberg, 2018)

Influences by Delimitations

Projects of these types are often in need of some type of problem delimiter. Delimiters are established in order to make a problem manageable. This can be done by assuming and disregarding certain aspects of the problem. Delimiters taken in this thesis is presented in the following list:

- Companies are targeted indifferent of size and business area.
- The framework should be applicable for organizations with a number of employees ranging from 25-1000.
- The framework is intended to be applicable for each business unit in large organizations, and for smaller organizations, which may only have one or two units.
- The framework will not focus on specific intrusions or attacks.
- Attacks are initiated externally and from unknown initiators without intentional help from the organizations' employees.
- Decisions and actions can be taken on site without confirmation from central management.

The above listed problem delimiters were formed in such a way that the created framework would be holistic and applicable for a wide range of organizations. For instance, the delimiter implying that decisions can be taken on site greatly reduce the complexity of organizations and thus allow analysis of larger companies.

Contribution to Science

This thesis contributes to science by offering a framework that is drawn from recent literature, surveys and interviews, thus reflecting reality very well. It also contributes to science by offering a holistic framework applicable on a variety of organizations, covering the central parts in cyber security including, prevention, action and evaluation. Companies should use the framework as a foundation and then, if necessary, further customize aspects to fit their specific business.

Future Research

Cyber security is a topic that constantly is evolving and based on this thesis there are some interesting areas for future research. Future research can focus on internal problems, for instance how employees aid cyber criminals, as well as act out on their own. Another area worth addressing further is how future methods/programs possibly can help trace cyber criminals, so that they not are able to slip away after a crime has been committed, like the often do today. Finally, AI is an emerging area in many industries. For future research it is interesting how this can be used in order to anticipate incoming attacks and spot ongoing attacks.

References

S. Sreejesh, Sanjay Mohapatra, M. R. Anusree. (2014). Business Research Methods, p. 29-32; 58.

Strategy and business. (2018). Planning for the Unexpected accessed from *https://www.strategy-business.com/article/Planning-for-the-Unexpected?gko=1dbff*

Jadhav Harsh. (2018). Be Prepared: Implementing a Cybersecurity Incident Response Plan, Special Issue: 6-8. 3p.