MASTERTHESIS

ORGANIZING VIABLE INFORMATION SECURITY GOVERNANCE AND MANAGEMENT

DEGREE	MASTER OF SCIENCE
ORIENTATION	EXECUTIVE MASTER IN IT GOVERNANCE & ASSURANCE
ACADEMIC YEAR	2018 - 2020
STUDENT	KEVIN BOLLENGIER
PROMOTOR	YURI BOBBERT, PHD (AMS)

Antwerp Management School

MASTHESIS

ORGANIZING VIABLE INFORMATION SECURITY GOVERNANCE AND MANAGEMENT

DEGREE	MASTER OF SCIENCE
ORIENTATION	EXECUTIVE MASTER IN IT GOVERNANCE & ASSURANCE
ACADEMIC YEAR	2018 - 2020
STUDENT	KEVIN BOLLENGIER
PROMOTOR	YURI BOBBERT, PHD (AMS)

Antwerp Management School

Abstract

Business information security has evolved over the years, where it first started as a technique to protect critical information assets from the growing use of information technology and its accompanying risks, it now has grown to a topic widely discussed on board level. Cybercrime also has evolved to being much more than an attempt to steal logical, information assets. Hardware assets, networks, servers, employees and even organizations themselves have become targets. Organizations must ensure that they remain viable against the rising and evolving threats of utilizing information technology and its accompanying risks.

In order to provide guidance, this research attempts to provide concepts from the Viable System Model, established by Stafford Beer, in order to diagnose the viability and resistance against cyber threats. Using concepts from management cybernetics and this viable system model, this research, furthermore, proposes a new holistic way of looking at business information security and to step away from silo thinking and looking at the organization and its organization of security management and governance as a whole.

Business information security, VSM, Viable System Model,
information security governance, information security management.

Samenvatting

De beveiliging van bedrijfsinformatie is in de loop van de jaren geëvolueerd, waar het aanvankelijk begon als een techniek om kritieke informatiemiddelen te beschermen tegen het toenemende gebruik van informatietechnologie en de bijbehorende risico's, maar nu is uitgegroeid tot een onderwerp dat algemeen wordt besproken op bestuursniveau. Cybercriminaliteit is ook uitgegroeid tot veel meer dan een poging om logische informatiemiddelen te stelen. Hardware-activa, netwerken, servers, werknemers en zelfs organisaties zelf zijn doelwitten geworden. Organisaties moeten ervoor zorgen dat ze levensvatbaar blijven tegen de toenemende en evoluerende bedreigingen van het gebruik van informatietechnologie en de bijhorende risico's.

Om hierin begeleiding te bieden, probeert dit onderzoek concepten te leveren uit het Viable System Model, opgesteld door Stafford Beer, om de levensvatbaarheid en weerstand tegen cyberbedreigingen te diagnosticeren. Gebruikmakend van concepten uit management cybernetica, en het Viable System Model, stelt dit onderzoek bovendien een nieuwe holistische manier voor om naar informatiebeveiliging van bedrijven te kijken, namelijk om weg te stappen van silodenken en naar de organisatie en haar organisatie van beveiligingsbeheer en governance als een gezamelijk geheel te kijken.

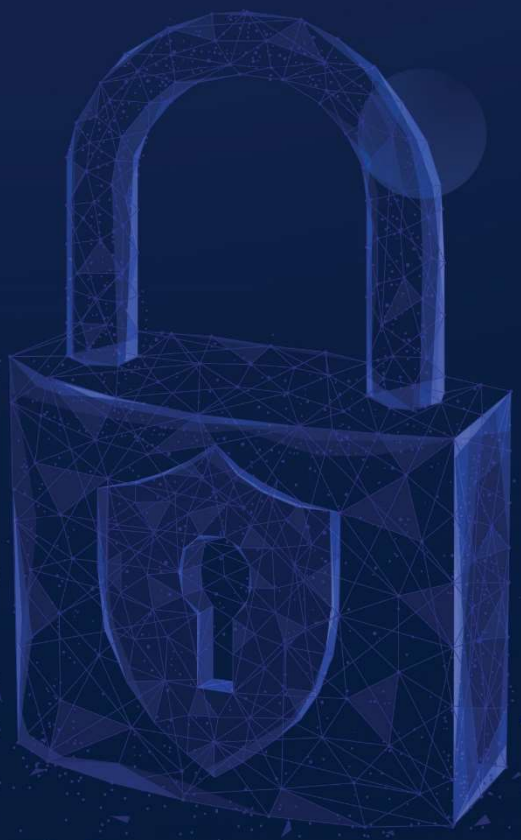
Business informatie beveiliging, VSM, Viable System Model,
beleidsvoering voor de veiligheid van informatiesystemen,
bestuur van de veiligheid van informatiesystememen.

TABLE OF CONTENTS

Table of contents

MOTIVATION & INSPIRATION

1



1 Motivation & inspiration

Thanks to lucky circumstances, hard work and a very interesting internship I had the honor to start as IT Security & Compliance and Data Protection Officer at Kinepolis Group, being responsible for the security of the IT environment as well as for the protection of personal data. However, I quickly concluded that showing the benefits of investing in IT security and the positive evolution of the security maturity within the organization was challenging. Another challenge is to get management support regarding this very technical topic, where adequate knowledge is required to correctly take calculated risks, especially when you have a very technical background in IT security.

One of the challenges I faced when I first started on this position was my lack of knowledge on security management and governance, as my Bachelor's was more IT technical oriented.

Because of my position at Kinepolis I felt the urge to enrich my skill set with non-technical skills in order to be able to better communicate on a management level. Therefore, I would like to thank my team leader, friend but most of all mentor and coach Bjorn Van Reet to help me decide on the orientation that would suit my career the best. Bjorn has been a true inspiration since the first day I've known him. Bjorn, thanks for inspiring me, coaching me but most of all challenging me every day to become a better version of myself!

Secondly, I want to thank the professors from Antwerp Management School, with special notion to my promotor Dr. Yuri Bobbert, Dr. Tim Huygh, and the Dean Dr. Steven De Haes. I want to thank Steven, for the opportunity for accepting me as youngest Executive Master candidate ever, without meeting the professional career experience requirement, Tim for your highly valuable input from both your PhD and our informal lunch and thought discussions on applying the Viable System Model. And finally my promotor Yuri, for the feedback and discussions we had during this research project and the actionable literature that was provided.

I want to thank the students from my Cohort for both the thesis and professional career advice during our informal talks at Korsakov with a "Bolleke" in the hand.

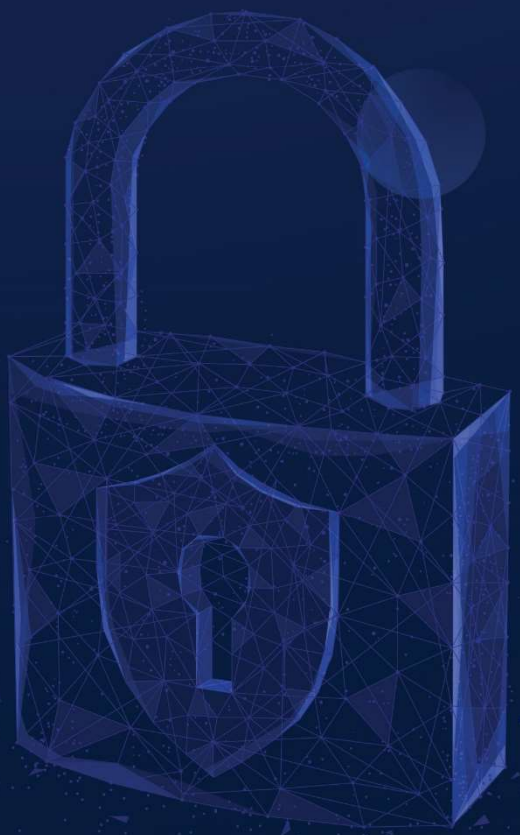
A thank you to my ex-teacher and friend Jill VandenDriessche for the support and taking the time to go to the movies, up to the point of driving to France to meet one of our favorite actors, when I could use the break and distraction from my studies.

For the creative design of my Master dissertation matching the theme of cybernetics, I thank Kris Geluykens from Slidedesigners.

And finally I want to thank my parents, for the trust when I decided to invest into gaining this Executive's master's degree and for the patience when the pressure on the road was high.

INTRODUCTION

2



2 Introduction

In the introduction, I will introduce the problems that arise with implementing an information security program in an organization, both from a practical and academic point of view. These inputs will be followed by a formal problem statement from which I will formulate a main research question acting as main motive for writing this master thesis.

2.1 What is the problem?

In any modern commercial organization, the use of information has become important to thrive the business. This (business) information is stored in computerized information technology (IT) systems in most if not all companies. The challenge in this digital age is for companies to reasonably assure that this information is protected against possible risks against breaches of confidentiality, integrity and availability (CIA). Furthermore, resulting from legal and other regulatory developments of which Sarbanes-Oxley and the General Data Protection Regulation are examples, the roles and responsibilities of senior management and Boards of Directors have escalated. Now people in these positions have become personally accountable for the health (security) of these IT systems (B. Von Solms, 2006).

As organizations are entering a mode of digital transformation where they adopt digital business strategies with high level technological deployments, they can no longer ignore or avoid taking IT related decisions.

With "digital" being put on the agendas of these business strategies more frequently, organizations are required to be aware of the risks that come with embedding IT into the business. Decision makers within organizations need to take account of the increasingly sophisticated threat environment following this digital agenda.

As such, the organization must govern information security, by implementing the required information security components from a holistic perspective to minimize the risks arising from the use of IT and digital assets (Soomro, Shah, & Ahmed, 2016; Veiga & Eloff, 2007; B. Von Solms, 2006). Information security governance (ISG) is a direct corporate governance responsibility and lies on the shoulders of the Board of a company (SHV Solms & Solms, 2008).

However, within the practitioner's field, some problems related to the implementation of ISG arise. In particular, the fast-evolving digital environment, the increasing threat complexity, the lack of IT knowledge and the intangible results from investing in information security.

A fast-evolving digital environment

We live in a fast-evolving digital age where businesses are continuously exposed to threats resulting from vulnerabilities in information technology (IT) systems. These vulnerabilities lead to risks which given this everchanging environment, threaten the confidentiality, integrity and availability (CIA) of (business) information (SHV Solms & Solms, 2008).

On the other hand, with the continuous cycle of digitalization, organizations are embedding IT into their core business processes in the hope of gaining a competitive advantage. This effectively leads to the ongoing escalation of more complex security threats (Carcary, Renaud, McLaughlin, & O'Brien, 2016; R. Von Solms, 1998).

The need for effective information security governance (ISG) increases as organizations are becoming heavily dependent on their IT systems to process their information. Therefore, ISG must be an integral part of the Corporate Governance of an organization (SHV Solms & Solms, 2008; B. Von Solms, 2006).

One specific example of how the digital environment has changed drastically, is the growing importance of data and data analytics. Organizations started capturing significant amounts of (personal) information so that they would be able to act on certain patterns or behaviors.

As part of this growing concern, a new regulation with the purpose of data protection and privacy was approved on the 14th of April in 2016 (Bollengier, 2018). The General Data Protection Regulation ("the GDPR") attempts to make organizations aware of the importance on information (security) governance. This is done by ensuring that organizations know which information they possess and that it is secured appropriately. And that when in the case it goes wrong, appropriate incident response is respected and the breach is reported. The GDPR also establishes a new governance structure within ISG, namely that of the Data Protection Officer ("the DPO") which has one of the tasks to raise employee awareness and provide staff training related to the use of personal information and the protection thereof (European Parliament and the Council, 2016b).

As additional answer to the fast-evolving digital environment and with it, its exposure to cyber security risks, the European Union established a Directive ("the NIS Directive") to ensure a standardized approach for cyber security, aimed in particular at critical infrastructure and digital service providers. As an example, the Members States of the Union are required to establish a national strategy on the security of network and information systems, including but not limited to an information security governance framework (European Parliament and the Council, 2016a; Sabillon, Cavaller, & Cano, 2016).

Increasing threat complexity

The European Network and Information Security Agency (ENISA) provides a yearly report on the evolution of the cyber threat landscape. The key takeaways for 2019 are that cyber criminals continue to professionalize their attacks. They achieve this by increasing the automation and efficiency of attack vectors. This is demonstrated in the increasing complexity and sophistication of their attacks e.g. phishing attacks.

Next to automation and increasing the efficiency, cyber criminals are developing new types of cyber-attacks for example Advanced Persistent Threats (APT) or Crypto jacking an attack which is slowly replacing the use of ransomware. Another new trend gaining popularity are "Cybercrime-as-a-service"-platforms, taking away the complexity while increasing the convenience for threat actors. The number of incidents and complexity in both defense and attack tactics continues to increase, thereby confirming the trend of previous years (ENISA, 2019).

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	⇧	2. Web Based Attacks	⇧	→
3. Web Application Attacks	⇧	3. Web Application Attacks	➲	→
4. Phishing	⇧	4. Phishing	⇧	→
5. Spam	⇧	5. Denial of Service	⇧	↑
6. Denial of Service	⇧	6. Spam	➲	↓
7. Ransomware	⇧	7. Botnets	⇧	↑
8. Botnets	⇧	8. Data Breaches	⇧	↑
9. Insider threat	➲	9. Insider Threat	⇩	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	⇧	11. Information Leakage	⇧	↑
12. Identity Theft	⇧	12. Identity Theft	⇧	→
13. Information Leakage	⇧	13. Cryptojacking	⇧	NEW
14. Exploit Kits	⇩	14. Ransomware	⇩	↓
15. Cyber Espionage	⇧	15. Cyber Espionage	⇩	→

Legend: Trends: ⇩ Declining, ➲ Stable, ⇧ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2018 with the one of 2017

This dynamically, evolving digital realm inevitably produces a significant challenge to the modern cyber world by naïve user attraction towards innovative technological e-lifestyle, e-services and smart technological gadgets. However, numerous unknowns from the security perspective are also produced in this new and complex mixed digital reality (Minchev, 2016).

An example is the continued increasing use of smart technology, the use of the Internet of Things (IoT), or the Internet of Everything (IoE) (Miraz, Ali, Excell, & Picking, 2015). The implementation of IoT can lead to a variety of security problems (Zhao & Ge, 2013). One of these particular security threats involving IoT and embedded devices was the Mirai botnet who struck several high-profile targets in 2016 with massive Distributed Denial of Service (DDoS) attacks, ad fraud, crypto-mining or any number of applications (Antonakakis et al., 2017).

Resulting from the increased complexity in the field of information security, several researchers and organizations propose frameworks and models for information security governance (Gokhale & Banks, 2004). Von Solms (B. Von Solms, 2006) states that *for good information security there is need for management and leadership commitment, proper organizational structures and necessary policies, procedures, processes, technologies and compliance enforcement mechanisms*.

The ENISA, (ENISA, 2019) calls for the implementation of cybersecurity into organizations their risk management functions and to identify strategies to anticipate and or respond to the fast-evolving threat landscape. This is in line with the Mirai botnet example which took advantage of the lack of security best practices present in Internet of Things architecture (Antonakakis et al., 2017).

To conclude, the only way to keep up with the changing, complex threat environment is not to form a static policy or strategy, but a dynamic process that is capable of adapting to rapidly changing technology and incorporate these ongoing changes in guidance (Miller, 2016).

Insufficient IT knowledge & capabilities

With senior management teams incorporating IT solutions into their core business processes to achieve business value it is crucial that they have the correct knowledge or capabilities to take strategic decisions (Carcary et al., 2016; De Haes & Van Grembergen, 2015). This follows the uncertainties and risks that come from embedding IT in the business.

For example, simply spending millions on security technology can make an executive feel safe, but the major sources of cyber threats are not technological in nature. As with any cyber threat, the first and last line of defense are prepared leaders and employees. Firms need to balance security investments in technological deterrents and human-centered defenses. As these cyber threats continue to

grow, risk management has become an important topic on board-level agendas requiring a proactive leadership approach with sharp decision making on IT-related risk matters (Disparte & Furlow, 2017). Therefore, it is important that the IT security, business and strategic risks are considered with their accompanying consequences, such as priority concerns. Managers require the correct knowledge or capabilities to employ a good security planning process (Kotulic & Clark, 2004).

Furthermore, information security is often seen as a very technical subject and is therefore typically handled on an IT technical, operational level. e.g. IT security controls were implemented on best practices prescribed by vendors, without a direct link to risks or business objectives (Yaokumah & Brown, 2014). The problem with this approach is the lack of a holistic approach towards information security. For information security to be absorbed in the organization, information security knowledge (and awareness) needs to be shared within the organization (Flores, Antonsen, & Ekstedt, 2014).

With the realization that consequences may arise due to misuse of data and information, Information Security governance also has become an important business responsibility with accountability on Board level. As the use of information and data has an enterprise wide impact, I will no longer use the terms "information risk" and "information security", preferring the terms "business information risk" and "Business Information Security (BIS)" (Bobbert & Mulder, 2010; B. Von Solms & Von Solms, 2005).

Intangible results from investing in business information security

Decision makers are aware on the importance of BIS however, due to their lack of technical expertise they often do not want deep knowledge on how their information resources are protected (Sonnenreich, Albanese, & Stout, 2006; Van Niekerk & Von Solms, 2010).

According to Anderson (Anderson et al., 2013), the costs of cybersecurity incidents for a firm are not easy to quantify. For example, you have the direct (monetary) losses as a consequence of a cybercrime (e.g. money withdrawn from victim accounts, time and effort spent to reset account credentials), indirect (monetary) loss due to missed business opportunities and loss of trust in the business and finally the costs in defense where a business attempts to minimize risk by implementing preventive or detective controls against cyber-attacks.

Decision makers want to know how lack of security is impacting their business and what the cost would be to remediate the associated risks (Ruan, 2017). From an executive/Board level perspective an implemented solution needs to be adequate and cost-effective. This is because investing in securing business information often has no direct return on investment (Van Niekerk & Von Solms,

2010). Implementing security often brings a decrease in productivity and a perceived increase in costs. As (Van Niekerk & Von Solms, 2010) state: *"Security is often seen as detrimental to business goals because it makes systems less usable"*.

It is critical that investments in Business Information Security are financially justified and make sense for the business. Ruan (Ruan, 2017), attempts to analyze the economics of information security and states that organizations should spend in the most cost-effective manner to reduce information risks. As such, several attempts to justify investments in information security has been proposed, based on Return on Investment and Net Present Value (Anderson et al., 2013; Gordon & Loeb, 2002; Mercuri, 2003; Rodewald, 2005). But according to Ruan (Ruan, 2017), none of these have been successfully validated with real-world data.

From a strategic perspective it is hard to quantify the resources needed to implement a BIS program as there are a lot of intangible factors. What level of security is adequate for a business? How much risk will an investment in BIS mitigate? What is the right amount of resources e.g. money, time, human capital to invest in BIS? How is the business performing on the level of BIS compared to its competitors?

This prototype-artefact aims to make visible in which branch of Viable Business Information Security should be invested first by conducting a Viable System Diagnosis. Currently this prototype-artefact uses a traffic-light model whether a certain control or objective is in place, in the end, a relative scoring shows the achieved goals within the fields of Security Governance, Security Intelligence, Security Management, Audit & Compliance Monitoring, Security Orchestration and Security Operations.

As a future research opportunity this prototype-artefact could be extended with weighted scoring on control level to help with the creation of a strategic roadmap. The scoring could take qualitative data input (e.g. effort/cost vs impact of control) or quantitative data (displayed in monetary value), however as of current such data and statistics have yet to be adequately collected (Ruan, 2017).

Silo thinking (reductionism) within cyber security

As already established above, cyber systems are complex systems. In fact cyber systems are examples of Complex Adaptive Systems (CAS) (Gandhi, 2014; Holland, 2006). Holland (Holland, 2006), puts CAS forward as systems that involve many components that adapt or learn as they interact.

As Gandhi (Gandhi, 2014) and the Fox-IT report (FOX-IT, 2020) (see: 5.3.1) on a cyber-attack performed on an educational institution make clear, cyber-attacks often are constructed out of more than just a single vulnerability and consist of an entire so-called "attack-chain". This attack-chain, the collision of all

circumstances under which a breach is successful needs to be "whole", as a single defensive countermeasure could in theory break this chain.

Within the field of cybersecurity you often hear analogies to biology, epidemiology, virology such as the terms infection, virus, worms, quarantine, isolation etc. (Betz & Stevens, 2013).

Using these analogies, we can look at how pandemics, just like the SARS-CoV-2 outbreak can be viewed from a holistic approach and how these analogies reflect to the security of information systems. For example during the SARS-CoV-2 pandemic, many nations entered a state of lock-down or quarantine to prevent the further spread of the virus (Li, Romagnani, von Brunn, & Anders, 2020).

One could say that virologists and politicians taking drastic measures such as applying movement restrictions or the isolation and quarantining of individuals or groups take a holistic approach to protect the national healthcare system to prevent the further spread of the virus and prevent a collapse of the healthcare system in which, for example, hospitals no longer have room for the treatment of additional patients (Ivanuša, Mulej, Podbregar, & Rosi, 2015; Li et al., 2020; Tobías, 2020).

Nowadays cyber-attacks have become more complex, often involving a chain of events, referred to an attack or kill chain, prior to the destined goal of a certain malware or virus such as an Advanced Persistent Threat (APT) (Hahn, Thomas, Lozano, & Cardenas, 2015).

Just like the treatment of a pandemic where the economic and national health systems should be considered as a "whole" set of events impacting a country and even the entire world as system in focus, so do we need to consider the organization of security within an organization (Sohrabi et al., 2020).

2.2 Problem statement

The problems stated above lead us to assume that businesses need to incorporate information technology in order to gain value and remain competitive in this digital age. However, due to the limited IT knowledge at the board and executive level, risks resulting from the implementation of IT into business are often forgotten or not calculated for. Another aspect is that organizations, and more specifically senior management, want to see tangible benefits from investments in information technology. An example could be the implementation of a web shop, where management can immediately see the sales on online channels. The implementation of a business information security program relies on securing the confidentiality, integrity and availability (CIA) of the information that comes with digitalization. The security aspect is often forgotten due to this limited management knowledge or because the lack of insights in tangible benefits. Calculating

the return on security investments is difficult as it cannot be measured in exact units, it is also subject to the odds of an incident happening. Management will not see the benefits of this investment until after an incident occurs. On the other hand, security investments could also lead to more efficiency which is also hard to quantify in tangible assets.

We can therefore conclude with the following formal problem statement:

The lack of a holistic approach towards the organization of Business Information Security Governance and Management causes a problem for organizations in an uncertain and eco-system-based environment, which leads to organizations not being viable against this fast-changing threat environment.

2.3 Questions we want to answer

The objective of this master thesis is to deliver a conceptual model and idea which can be used to diagnose the viability of a business information security strategy and define remediating or improvement actions to the current state of the BIS strategy of an organization. On the other hand, this conceptual idea can also be applied to benchmark the cyber security maturity level across businesses, this benchmark can then act as enabler for business information value protection. The main research we ask in this master thesis is therefore: *"How can viable business information security management and governance be organized?"*. Subsequently to ensure the goal of creating this new model we need to answer the following sub-research questions:

- RQ1: How does business information security relate to the viable system model?
- RQ2: What are good design rules to extend the viable system model to diagnose the viability of business information security governance & management?
- RQ3: Which combined set of business information security principles and practices lead to the viable organization of business information security governance & management?

2.4 Research deliverable

The goal of this research project is to come up with a prototype-artefact reflecting the conceptual model and philosophy of "Viable Business Information Security Thinking", which could lead to the design and development of a diagnosing & remediating instrument which can in turn also be used to benchmark the maturity of Business Information Security Governance and Management.

This prototype-artefact has as goal to demonstrate that a holistic approach to the organization of business information security is required for a business to remain viable against a fast adapting threat environment. In this case the prototype-artefact aims to reveal certain blind spots that might be overlooked when looking at security from the more traditional, reductionistic method.

The prototype-artefact, a combination of the Viable System Model with a mapping of best practices in information security enables a comprehensive analysis of a business and can provide an "As-is" status of the organization of business information security within an organization. The mapping of several best practice frameworks and their controls such as COBIT, ISO 27002, CIS aim to provide this holistic view to organize security governance & management by linking them to the Viable System Model.

Further, it provides a basic Viable System Diagnosis, enabling the organization to see a maturity score on Security Governance, Security Intelligence, Security Management, Audit & Compliance Monitoring, Security Orchestration and Security Operations. This Viable System Diagnosis essentially serves as an auditing approach against a minimum set of requirements, or baseline in order to remain viable as a company against the fast-changing threat environment.

This prototype-artefact could in a future research be refined to include weighted scores on control level to include the automated creation of a roadmap taking into account cost and effort, essentially a method to select a priority of "To be" controls with the highest "Return on Security Investment".

RESEARCH APPROACH

3

3 Research Approach

This chapter focusses on the research approach and methodologies used. It will reveal the strategies and methods used to answer the research questions and contribute to the academic knowledge of this thesis. The goal of this chapter is to add academic rigor to this master thesis.

3.1 Introduction

In this chapter I explore the research methodologies which can be used to research the knowledge domain of Viable Information Security Governance & Management. After establishing appropriate research methods to define the knowledge domain this chapter will further examine the research process to formulate an artefact specification aimed at improving the organization of viable information security governance & management. This chapter will outline a basic concept of research strategies and explores which strategies fit in Information Systems research.

3.2 Introduction into research methods

According to Recker (Recker, 2012) *information systems research as a social science is complex, diverse, and pluralistic, meaning that it can take many forms of inquiry, theory and outcomes.* Business Information Security (BIS) research, as an extension to information systems research, can therefore not be conducted according to a predefined research methodology (Bobbert, 2018; Recker, 2012).

In the field of research, we can distinguish two main categories of research, namely quantitative research and qualitative research. A combination of both categories also exists and is referred as a mixed research approach. Hereunder I will describe in short, both main research strategies.

Recker, (Recker, 2012), refers to quantitative research strategies as *quantitative methods describing a set of techniques to answer research questions (…) with an emphasis on quantitative data.*

Quantitative research methods have a focus on implementing measures to study events in the real world, followed by developing a theory and hopefully offering novel, insightful conceptualizations of real-world phenomena. In other words, quantitative research has a strong focus on numbers (Recker, 2012).

Qualitative research methods on the other hand, are designed to assist researchers in understanding phenomena in their context. In contrast with quantitative research, qualitative research methods have a strong focus on text capturing

records of what people have said, done, believed, or experienced about a particular phenomenon, topic or event (Recker, 2012). It helps explore new phenomena which in this research is the case.

A mixed method research approach is a type of research featuring elements from both quantitative and qualitative research. A mixed method research method enables researchers to simultaneously answer confirmatory and exploratory research questions (Recker, 2012).

Design science research attempts to complement mainstream behavioral sciences with a design-oriented research. More specifically the researcher in the field of design science attempts to answer questions relevant to human problems through the creation or modification of artefacts. Within design science research, the creation of "artefacts" lies central as something that is created artificially by humans with the objective of providing new solutions to an important problem or to improve on an already existing research question (Recker, 2012). Johannesson and Perjons (Johannesson & Perjons, 2014) describe design science as [*... the scientific study and creation of artefacts as they are developed and used by people with the goal of solving practical problems of general interest.].* Wieringa, (Wieringa, 2014), describes an artefact as a conceptual design, artificially created to interact with a given problem to help and improve that problem in its given context.

In the design science framework, there are three important bases or cycles toward building an artefact.

The first of which is the relevance cycle which interacts with the problem *environment* constituting of people, organizational structures and technical systems. This essentially creates opportunities to improve the environment.

On the other hand, you have the rigor cycle, also referred to as the *knowledge base*, which provides the materials, theories, prior research, experience, expertise which enables the researcher in achieving (academic) rigor in the design of the artefact.

As mentioned, centrally within design science research lies the creation of design artefacts, in the *design cycle*, this artefact is constructed and evaluated.

Hevner (Hevner, 2007) states in his design science framework, that all three of these cycles must be present and clearly identifiable within a design science research.

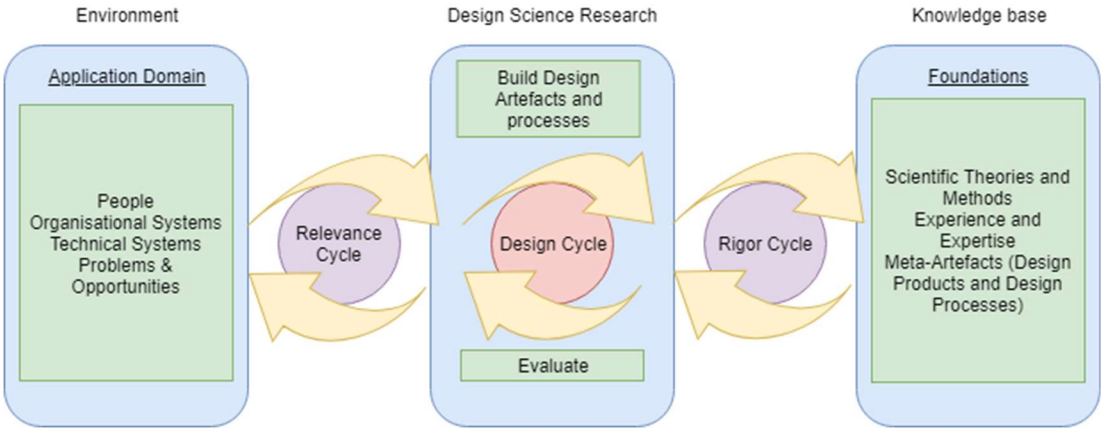


Figure 2: Design Science Research Framework by (Hevner, 2007)

3.3 Design Science Research Strategy

Johannesson & Perjons (Johannesson & Perjons, 2014), proposed a framework to engage in a design science research project consisting of 5 main activities ranging from the problem investigation towards the evaluation of the designed artefact:

Explicate Problem, the Explicate problem activity is about investigating and analyzing a practical problem. This activity relates to the relevance cycle as the problem should be of general interest. Explicating the current state of business information security (or problems in that regards) help make clear why this research attempts to bring forward a change or solution, such as the proto-type artefact constructed.

Define Requirements, the Define Requirements activity outlines an artefact proposal to the explicated problem. In order to fulfill the problems with a solution, the prototype-artefact has certain requirements that need to be fulfilled. In our case a literature research was conducted to define these requirements, mapping the VSM requirements on BIS requirements in an artefact blueprint (Goldes, Schneider, Schweda, & Zamani, 2017).

Design and Develop Artefact, this activity relates to the design cycle in the framework by Hevner. The creation of the artefact addresses the explicated problem and fulfills the defined requirements.

This research is limited to a first design cycle in which a prototype-artefact was constructed based on the Viable System Model and Goldes's (Goldes et al., 2017) artefact blueprint. This research attempted to create a holistic mapping between VSM and the proposed best practice security standards and frameworks.

Demonstrate Artefact, this activity uses the developed artefact in an illustrated or real-life case, often referred to as a "proof of concept", proving the feasibility and viability of the artefact. This proof of concept shows that the artefact can solve an instance of the explicated problem.

As mentioned, this research is limited to the construction of a prototype-artefact, however a single case study was attempted to see if fitting recommendations (based on a traffic light model) come out as a result.

Evaluate Artefact, this activity determines how well the artefact fulfills the requirements and to what extent the artefact can solve the practical problem that motivated the research.

The evaluate artefact phase is out-of-scope for this research project, however in a later research project, this phase could evaluate the finished artefact in a multi-case study and be validated by a GSS research panel.

As mentioned above, due to the time constraints imposed on this research project, the Design Science Research cycle is limited to the phases of: "Explicating the problem", "Defining the requirements", "The design and development of a prototype-artefact" serving as a proof of concept and finally a single case study demonstration of the prototype-artefact.

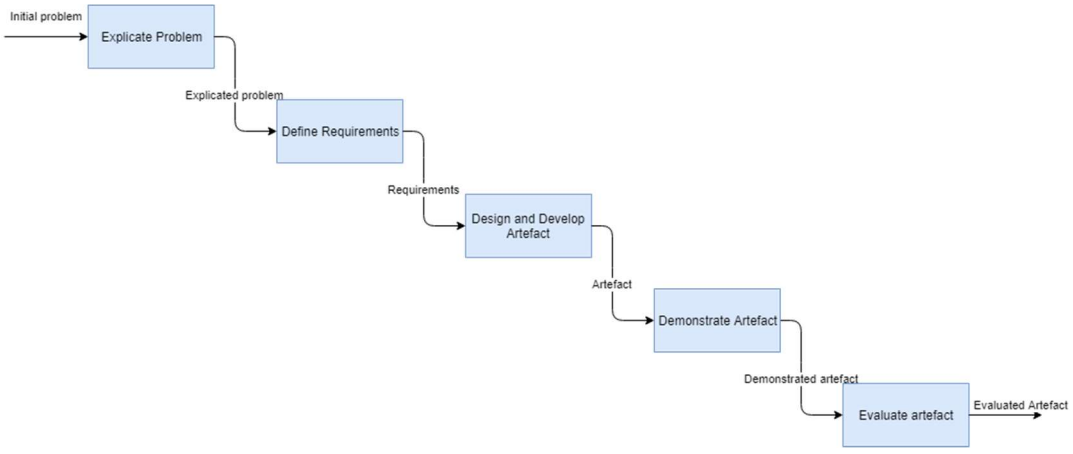


Figure 3: Overview of the method framework for design science research (Johannesson & Perjons, 2014)

3.3.1 Relevant design science research methods and techniques for this research project

The objective for this master research project is to create an artefact design which answers the main research question "How can viable information security

governance and management be organized?". The purpose of this artefact design is aimed at creating an artefact, in a later phase, capable of:

- diagnosing the viability of the business information security within an organization;
- standardized business information security maturity benchmarking between organizations;
- dynamically proposing a remediation roadmap to improve the business information security governance & management of an organization.

Bobbert (Bobbert, 2017) proposes a set of qualitative research methods and techniques within the branch of Design Science Research related to Business Information Security used to gain, capture and transfer knowledge items into the artefact design process.

Accordingly, the following research methods are relevant to this research project.

Explicate Problem	Define Requirements	Design and Develop Artefact	Demonstrate prototype-artefact	Evaluate Artefact
Literature research	Literature research	Creative methods	Expert Opinion	Out-of-scope for this research project.

Table 1: Proposed Design Science Research strategy for this research project

As the scope of this research project is limited to the establishment of the prototype-artefact, the research is limited to the phases "Explicate problem", "Define requirements" and partially "Design and develop artefact". Hereunder we summarized information regarding each step taken or proposed step for future research that may be applied to this research project. Furthermore, we argue why this research approach is applicable to this research project.

3.3.1.1 Explicating the problem with literature research

Before the creation of an artefact, according to Recker (Recker, 2012), we need to establish the knowledge base to provide clear definitions of "information security", "business information security", "business information security management", "business information security governance" and in extent "viable systems", which will act as the lens through which this research project will be conducted. The sub-research question "RQ1: How does business information

security relate to viable systems model?" will help with the creation of the meta-artefact and background knowledge.

RQ1 will be split into the following knowledge questions which will be used in the literature review from both scientific, academic and professional lenses where applicable.

- KQ1a: What is Information Security?
- KQ1b: What is Business Information Security?
- KQ1c: What is the definition of a viable organization regarding business information security?

To understand the environment and the research relevance, the two sub-research questions "RQ2: What are good design rules to diagnose the viability of information security governance & management?" and "RQ3: Which combined set of business information security principles and practices lead to the viable organization of information security governance & management?" will be answered by mapping information security governance and management metrics and practices to the Viable System Model. This list of principles and practices will be constructed by performing an initial practitioner literature research.

3.3.1.2 Delphi Research Method

Due to the time constraints placed on this research, this does not fit into the scope of this master thesis, however this method should be considered to reach consensus on the applicability of the would-be finished artefact by discussing using case studies performed with the artefact.

When the time constraint is less strict, using the Delphi research method, an expert panel of auditing experts could prioritize and score the proposed BIS metrics. Accordingly, an IT security expert panel could prioritize and score the most effective remediating BIS practices.

This allows us to propose new practices and theories, through a multi-iterative process, to form a qualitative view of the environment problem. Bobbert (Bobbert, 2017), proposes to use the Delphi Research method to validate derived best practices with an expert respondent group.

This Delphi Research Method as proposed to finish the prototype-artefact, would help with allocating values on certain controls based on cost and effort, essentially enabling the finished artefact to dynamically create a roadmap for an organization to mature the organization of business information security.

3.3.1.3 Creative methods

For the design and development of the artefact, Johannesson & Perjons (Johannesson & Perjons, 2014) state that research strategies are less important as the primary goal of this design science activity is the production of the artefact and knowledge to the lesser extent. Therefore creative methods, specifically in the case of the creation of this new artefact, brainstorming and collaborative modelling with experts will greatly enhance the relevance cycle of the Hevner (Hevner, 2007) design science framework within this research project.

In this design science research cycle, the combination of practices and metrics will lead to the creation of a prototype-artefact capable of diagnosing the viability of information security governance and management of an organization whilst at the same time proposing remedying actions to improve the viability of the information security governance and management. As such this will answer the sub-research question "RQ3: Which combined set of information security metrics and practices lead to the viable organization of information security governance & management?".

3.3.1.4 Group Support System Research

With the use of GSS research, the researcher can test the proposed artefact against expert opinions in focus groups which also enhances the academic rigor cycle and the relevance cycle. Furthermore, the use of GSS greatly stimulates design thinking and stakeholder collaboration. The ultimate goal of the use of GSS research is to establish group consensus on the proposed artefact and its applicability (Bobbert, 2017).

Group Support System research in a later phase of this research is needed to gain consensus on the mapping between the used frameworks, best-practices, standards and to reduce personal bias on the mapping between these.

However, for the sake of this research project it is considered out-of-scope but should still be listed for future reference.

3.3.1.5 Case Study Research

Due to the applied time constraints on this research project, the "Evaluate Artefact" activity is excluded from the research scope. However, to offer the virtual cohesive research approach, Case Study Research is the proposed research method to gain qualitative insights used to confirm the effectiveness of the proposed artefacts.

Multi-case study research could prove a viable method to gain qualitative data that could be fed to a Delphi research group to discuss the results of the use cases.

3.4 Literature review

3.4.1 Literature review purpose

In any academic research, one of the key tasks is to gather in-depth information surrounding the domain and topics of interest before one can contribute to knowledge relating to the research domain.

According to (Recker, 2012), the key objectives of a literature review in the research process are to acquire knowledge about:

- the domain and topics of interest,
- relevant theories that help you frame questions and phenomena,
- relevant research methods which can be applied to develop new knowledge or build innovative artefacts using Design Science Research or to articulate new research questions.

For this literature review I have opted for an academic literature review to gather the relevant knowledge regarding the research domain of viable business information security and surrounding topics of interest in answering the main research question *"How can viable information security management and governance be organized?"*.

These topics are translated in the following knowledge questions which are answered in chapter 4 "Defining viable information security organization".

- KQ1a: What is Information Security?
- KQ1b: What is Business Information Security?
- KQ1c: What is the definition of a viable organization to the extent of business information security?

3.4.2 Literature review approach

To conduct this academic literature research, academic publications, books and articles were gathered with the search terms found in 3.4.4.

This research mainly used the snowballing technique, where citations from relevant papers were further analyzed. This was particularly useful to gain in-depth knowledge about the Viable System Model created by Stafford Beer (Beer, 1979, 1984, 1985, 1986) and its underlying foundations such as the Law on Requisite Variety, established by R. Ashby (Ashby, 1956). The use of this methodology further helped establish a strong knowledge base about systems thinking.

One of the dangers in this snowballing technique is that when following the citations, the research goes back in time and some papers might not accurately reflect the current state of research conducted in the field of information systems.

On the other hand, this research also used specific search terms, mostly in the Google Scholar library to find niche papers relevant to this research project. These research terms are described below in 3.4.4.

When searching for academic publications with the keywords "Viable Information Security", "Viable information security management" or "viable information security governance" the search brings a limited amount of results. This result is expected as Viable Systems Theory is not often applied in practice due to its underlying complexity (Stephens & Haslett, 2011). Therefore, we will need to broaden our knowledge gathering to include "Viable Systems Theory" and deduct the found knowledge and apply this to the field of business information security.

On the other hand, for designing the artefact and making sure its applicability in practice, practitioner literature research is required. This is to link the academic knowledge, theoretical models and concepts to industry recognized resources. To ensure this applicability of the new artefact based on the Viable Systems Model we will review the Information Systems Audit and Control Association (ISACA) and International Organization for Standardization (ISO) which are both recognized as communities that publish practitioner literature.

3.4.3 Literature review sources

In the search for academic papers, we focused on Google Scholar and the library of the University of Antwerp. Other literature recommendations were also provided from professors at Antwerp Management School.

For example, from the Dean and Professor Steven De Haes in conjunction with Dr. Tim Huygh I received the draft PhD thesis from Dr. Tim Huygh.

The following books were distributed from professors at the Antwerp Management school and helped conducting research in information systems and governance.

- Enterprise Governance of IT (De Haes & Van Grembergen, 2015)
- Scientific research in information systems: a beginner's guide (Recker, 2012)
- An introduction to design science

From Dr. Yuri Bobbert and Talitha Papelard, I've received their book "Critical Success Factors for effective business information security", which combined with the snowball technique led to other relevant papers such as "Improving the maturity of business information security (Bobbert, 2018)".

3.4.4 Literature selection criteria

3.4.4.1 Search criteria Viable System Model and underlying concepts

Researching "Viable Information Security" required thorough knowledge about the Viable System Model, designed by Stafford Beer. In order to gain a deep insight into this model, we used the book "The Heart of Enterprise" by Stafford Beer as literature base. Furthermore, to enhance our knowledge about the underlying concepts (e.g. systems thinking and cybernetics) which are used in the Viable System Model, extensive use of Google Scholar was conducted to find relevant academic papers.

A list of search terms was saved and can be found below.

- VSM
- Viable System Model
- Cybernetics
- Stafford Beer
- Systems Thinking
- Viable Systems
- Management Systems
- Systems Thinking Approach
- Complexity Theory
- System Dynamics
- Holism
- Ashby's Law
- Requisite Variety
- Management Cybernetics

When searching Google Scholar, no age constraint was used as to be able to dive deep in the first concepts which led to the creation of the Viable System Model.

The literature used to gain knowledge about the Viable System Model and its underlying concepts can be found in Annex 1.

3.4.4.2 Search criteria (Business) Information Security

In this research we look at information security from a holistic perspective, due to the use of the Viable Systems approach we took. As such a fitting, up-to-date definition of information security needs to be constructed. Information security can no longer solely be seen as solely "information protection". In order to gain a better understanding of the current interpretation of "information security" in literature, ad-hoc research was conducted using Google Scholar and by using papers granted by professors at Antwerp Management School. Below you can find

the list of search terms that was used to conduct research the evolution from information security to the definition of Business Information Security.

- Business Information Security Governance
- Corporate Governance
- Information security management
- Risk management
- Security governance principles
- Enterprise governance of Information Technology
- IT Governance
- Information security

And in lesser extend we used the above search terms in combination with search terms:

- Viable System Model
- Management cybernetics

In general terms no age restriction was used to conduct this research, however we did try to limit the age to a maximum of 10 years to the date of writing. The lack of age restriction on this subpart of the research was used to clearly show how information security has evolved in a rather short timeframe.

3.4.4.3 Search criteria Viable Information Security

In order to gain a profound knowledge base about Viable Information Security, we conducted a search on the Web Of Science using the library of the University of Antwerp.

We used a search string in order to attempt to find empirical papers which combine the Viable System Model and Information Security.

TS=(Viable System Model and Information Security)
Indexes=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI Timespan=All years

Table 2: Search string used on the Web of Science to support Viable Information Security research

This search string was last used 17/02/2020 which initially yielded 77 results. An initial scanning of the titles of the papers lead to the conclusion that research in the field of information security cybernetics is quite limited. 59 papers of the 77 results were either not relevant as they did not relate to either information

security or viable systems. 15 papers referenced information security of which 9 indirectly used viable system elements such as indirectly referencing the subsystems of the Viable System Model. Only 2 papers directly referenced both the Viable Systems Model and information security, finally the last paper does not directly reference the Viable Systems Model but does talk about the ontology of information security in enterprises and indirectly references concepts of viability.

The results of this search query are attached as Annex 2.

This research project also attempts to make the cybernetic connection from living things to computers, the illustrated example being the analogy of virology, epidemiology regarding the used terms and approaches in both research fields.

For this illustrated example in the problem statement, this research conducted a search on Google Scholar with the follow specific keywords:

- Covid-19
- SARS-CoV-2
- Analogy of cybersecurity with biology
- Lockdown
- Pandemic
- Economy & Covid-19

3.4.5 Conclusion of the literature review

Following the literature research conducted, the conclusion is that the amount of research specifically in the field of viable business information security is very limited.

It seems that following this literature review, the Viable System Model is not often used within the field of Information Security. When skimming through the papers and in the citations, there were few to none reference to the Viable System Model, systems thinking etc.

On the other hand, having gathered thorough knowledge on the Viable System Model , the Law of Requisite Variety and systems thinking (Ashby, 1956; Conant & Ross Ashby, 1970; Holland, 2006; Jackson, 2003; Kast & Rosenzweig, 1972; Mingers & White, 2010; Von Bertalanffy, 1968; Wiener, 1948; Yolles, 1999) ,I must conclude that components of the Viable System Model, are often unknowingly included in academic information security research papers, without the mention or citation of relevant sources.

Using the lens of the Viable System Model could bring forward a new and innovative thinking methodology of looking at the organization of information security. Looking at the organization of business (information) security from its holistic whole, could lead to better governance, actionable security intelligence,

stronger organization of security management, more integration and orchestration of security within systems and a stronger orchestrated security operations.

DEFINING VIABLE INFORMATION SECURITY ORGANIZATION

4

4 Defining viable information security organization

This chapter will contain the theoretical background which is used to establish this thesis aimed at achieving the degree of Master of Science. This chapter will in the first instance create a formal definition for "Business Information Security" which will further be explored in the wider concepts "Business information security management and governance". We will further establish the concept of a systems thinking approach. This idea of "systems thinking" is the fundamental base used in the Viable Systems Model (VSM).

This chapter will thus provide the necessary theoretical background to move from academic literature towards the creation of a practical artefact specification based on the Viable Systems Model for diagnosing, remediating and benchmarking the maturity of Business Information Security Governance and Management within organizations.

4.1 Conceptual model as base for this research

Figure 2 displays the conceptual model used as approach towards this research. This visual representation of the research takes the problem statements from chapter 2 "Introduction" into consideration and maps these to theoretical concepts further explained in this chapter. Further, it provides inside how the artefact specification was established and what the proposed outcome of this research would be.

In the chapters above it became clear that the fast-evolving digital landscape leads to businesses embedding new technologies into their business strategies in the hope of gaining a competitive advantage. This effectively, also leads to an increasing cyber threat landscape with which businesses must cope. This in combination with the lack of IT knowledge on Board and Executive level and the nature of intangibility of IT security (visualized as blue ellipses) leads to the conclusion that organizations must conduct business in an uncertain, complex external environment (visualized as the red rounded rectangle).

The goal of the research, creating the artefact specification to diagnose, remediate and benchmark the viability of business information security governance and management, is based on the Viable System Model (visualized as the green rectangles and yellow diamond). To get to this artefact specification we will map several inputs (purple trapezoids) to the Viable System Model. The goal of the would-be artefact, and more specific its benchmarking outcome, is to create a measure instrument on the maturity of business information security governance and management. This will lead to the conclusion that Business Information

Security can act as an enabler to thrive business and serve as value creator and protector.

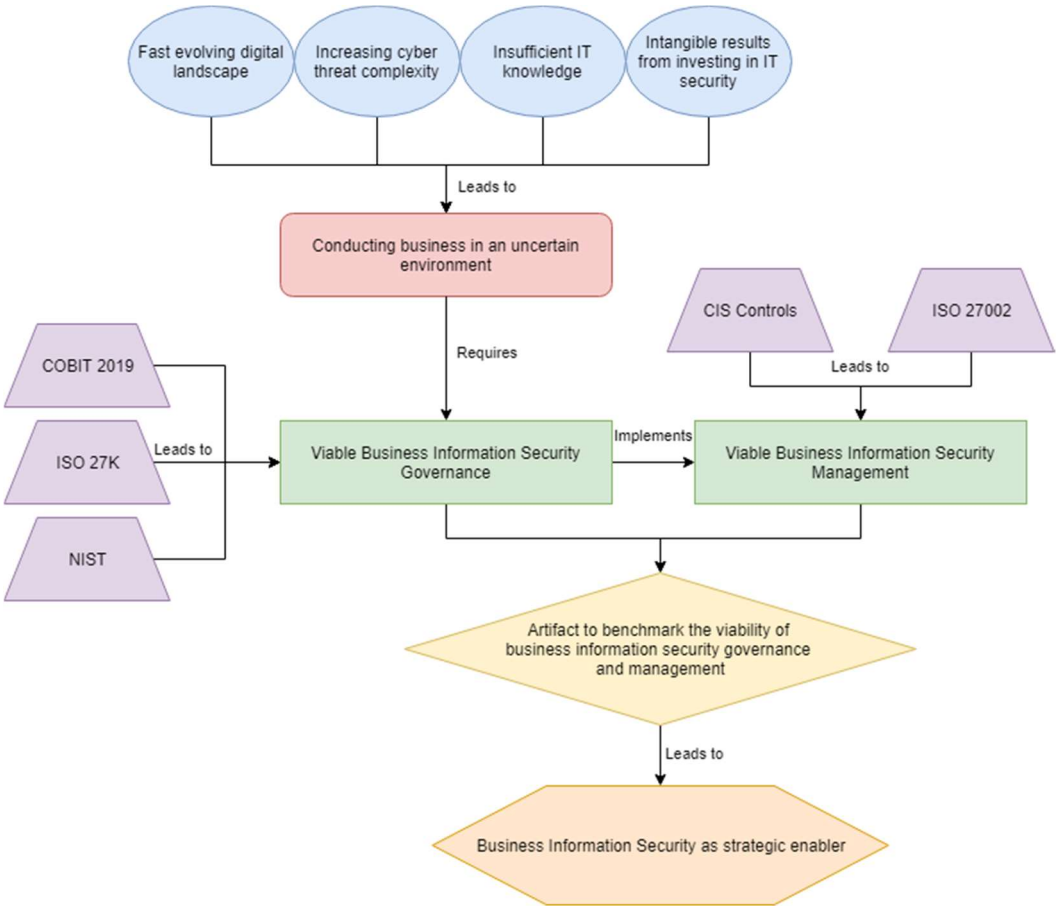


Figure 4: Conceptual model used as fundamental base for this research

4.2 Systems thinking philosophy

In chapter 2, it became clear that for an organization, to remain viable, it must respond to constant evolutions in its external environment by maintaining homeostasis, or in other words maintaining an equal level of internal control versus risk.

Managing and governing this complexity can only be done by looking at the organization from a holistic view. A systems thinking approach can be applied to this research, as systems thinking approaches implies holism by design (Jackson, 2003).

As such we can define a system as a complex whole of which its functioning and designed purpose depends on its interconnected elements and parts (Jackson, 2003; Von Bertalanffy, 1968; Yolles, 1999). The study of this holistic view on systems, referred to as 'holism', offers an alternative to the traditional method for studying systems known as 'reductionism'. This practice of reductionism attempts to analyze and describe a complex phenomenon by identifying its parts, understanding its parts and working up from this understanding to the understanding of the whole phenomenon (Jackson, 2003; Yolles, 1999). Holism, on the other hand according to Jackson (Jackson, 2003) is regarded as, *this phenomenon, or system as you will, is considered to be more than the sum of its underlying elements, the focus is on how this system sustains (itself) in existence*.

This systems-thinking approach is founded in the study of biology, where biological organisms were too complex to be modelled through a mechanistic paradigm, (Yolles, 1999).

Jackson (Jackson, 2003), utilizes two references in which this philosophy of systems-thinking and 'holism' can be traced back to the ancient Greek philosophers, Aristotle and Plato who both established important system thinking ideas. For example, *Aristotle reasoned that the parts of the body only make sense in terms of the way they function to support the whole organism. He later used this biological analogy to consider how individuals need to be related to the State. On the other hand, Plato was interested in how the notion of control, or the art of steermanship (kybernetes) could be applied both to vessels and the State. Using the analogy of a vessel requiring a helmsman, the same was applicable to the State*.

Although this idea of system-thinking has a background in philosophy, biology, control engineering (cybernetics), communication theory and mathematics (Jackson, 2003), it wasn't until the 1950's and 1960's that the concept of systems-thinking was applied to the social sciences, specific to the study of management, leading to the subject domain of management systems (Yolles, 1999).

From the 1970's on, several scholars and researchers started using this systems-thinking approach to study and understand managerial problems which ultimately lead to the creation of several frameworks and models (Jackson, 2003; Yolles, 1999).

Stafford Beer was one of such individuals who used this systems-thinking approach toward his creation of the Viable System Model (VSM).

4.3 The Viable System Model (VSM)

The VSM, drawn upon concepts of both *the science of communications and automatic control systems in machines and living things* (Wiener, 1948) referred to as "cybernetics", and neurophysiology, is a visual representation of "management cybernetics" or "the science of effective organization and communication" (Yolles, 1999).

4.3.1 An entry into the principles of the Viable System Model

Beer (Beer, 1979), used several concepts to design his managerial cybernetical model. As described above, the Viable System Model is a model reflecting a system-thinking approach. Beer in "The Heart of Enterprise", the book in which the model was conceptualized according to cybernetics, defines a **system** as *a group of elements dynamically related in time according to some coherent pattern with a purpose.*

For a system to be viable it has some prerequisites, outlined hereunder.

It is important to consider that a viable system always operates in an uncertain environment made of complexity. Any system needs to maintain homeostasis with their respective external environment, if they are to survive or in other words, remain **viable** (Beer, 1979; Jackson, 2003; Yolles, 1999).

Requisite variety

Ashby's (Ashby, 1956) **law of requisite variety** states that the number of states (variety, the measure of complexity) of the environment, operations and management must equate if a system is to remain viable. From a management cybernetics view, this means that a system implementing its purpose (its operations) needs to be controlled by management to achieve **homeostasis** with its environment. Such a homeostatic system, e.g. a firm, reacts to every change in its environment and must adapt itself to remain 'viable'.

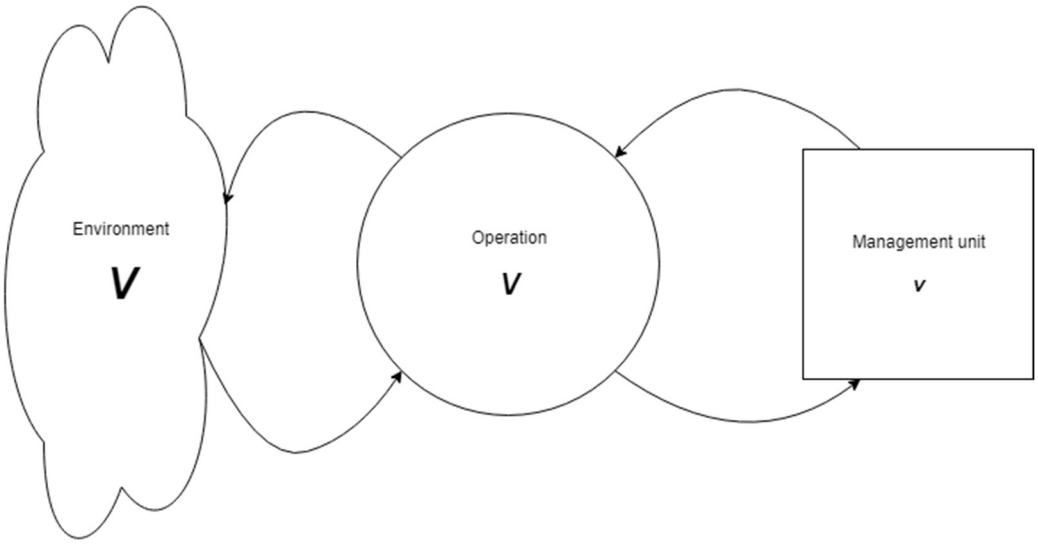


Figure 5: Ashby's Law of Requisite Variety states that varieties tend to equate, as such, management needs to design variety amplifiers and attenuators to establish requisite variety.

The diagram in figure 3 holds 3 key elements, each which has a different level of variety, after a certain amount of operating time, these complexities will equate, either due to natural law, e.g. ignorance, in which the environment will take over, or by management, whose task it is to design the necessary amplifiers and attenuators to establish this variety equilibrium.

This effectively leads to Beer's first out of four principles of organization (Beer, 1979), namely *Managerial, operational and environmental varieties, diffusing through an institutional system, tend to equate; they should be designed to do so with minimal damage to people and to cost.* This is in line with Ashby's law of requisite variety (Ashby, 1956), which tells us that for management to be able to control operations, and these operations to be sustainable within the environment, these varieties must be balanced (Jackson, 2003). We can conclude that the manager should thus act as a variety engineer within the system (Beer, 1979).

The second principle relates to the information channels between the environment, operation and the management unit, these channels need to be able to correctly identify the number of states, variety, they are supposed to transmit within a time factor.

As such Beer's second principle is that *the four directional channels carrying information between the management unit, the operation and the environment must each have a higher capacity to transmit a given amount of information relevant to variety selection in a given time than the originating sub-system has to generate in that time.*

The third principle relates on how information is sent over these channels. However, each of the subsystems have their own 'language' and as such the information requires translation. At the boundaries of these information channels, **transducers** must exist to match the variety of the information with that of the recipient subsystem. As such, *wherever the information carried on a channel capable of distinguishing a given variety crosses a boundary, it undergoes transduction, and the variety of the transducer must be at least equivalent to the variety of the channel (Beer, 1979).*

According to Beer, (Beer, 1979), the culmination of these three principles lead to momentarily requisite variety, and as such the system is deemed viable in that point of time. Therefore, Beer states in his fourth and final principle of organization that *the operation of the first three principles must be cyclically maintained through time, and without hiatus or lags*.

Viability

Academic literature defines a viable system as one that is able to maintain a separate existence by surviving on its own through adaptation (Beer, 1979; Yolles, 1999). As such coping against a dynamic changing environment requires the system to learn, adapt and grow accordingly to establish requisite variety (Beer,

1984). This element of viability is a key principle according to Alqurashi, Wills & Gilbert (Alqurashi, Wills, & Gilbert, 2013) to arrange and manage the organizational systems in a way they merge with defined systems and interrelationships. Indeed, this defined model of interoperability between structures (subsystems) and communication flows (interrelationships) is deemed crucial to business continuity, or in other words, crucial to the viability of the system. As such we can define that a system is viable when it is in a state of 'homeostasis', where it is able to stabilize its internal environment against an adapting external environment.

Autonomy

As prerequisite for a system to be viable, it requires adaptation to dynamic changes in its external environment. This is the role of local management, in which they will act as variety engineer to design variety attenuators and amplifiers to establish requisite variety between the environment, the elemental operation and their management unit. The key in this variety engineering process is that the managerial unit needs autonomy to do so. Mind that this does not mean that the managerial unit receives the freedom to act at will, however they receive the autonomy to act within a certain range of accountability (Alqurashi et al., 2013; Beer, 1979, 1984; Yolles, 1999). This means that the "metasystem", or organization as you will, must intervene only to a degree that is acceptable to maintain cohesiveness in the viable system (Beer, 1979).

Black & muddy boxes

Beer utilizes the cybernetic concepts of "black & transparent boxes" to compare how management control a certain aspect of the operation they try to regulate. A transparent box is a box, or operation as you will, in which all states are clear, observable. The other way around, an 'opaque' or 'black' box is a cybernetic concept in which all states are not observable. Using these cybernetic concepts, Beer proposes a new cybernetic concept, called the "muddy box", in which some of the states are observable but not all of them (Beer, 1979).

Indeed, managers can't possibly be aware of all states of their operation they try to regulate. However, Beer in his book 'Heart' refers to the fact that most managers have at least some sense what happens to the organization. Beer refers to this as managers can manipulate the input to regulate the output of an operation without having the full understanding of it (Beer, 1979).

Recursion

Beer's Recursive System Theorem (Beer, 1972, 1979), states that *any viable system contains and is contained within viable systems*. This is backed by Conant-Ashby's Theorem (Conant & Ross Ashby, 1970) which is a manifestation of the Law of Requisite Variety (Beer, 1986; Conant & Ross Ashby, 1970), stating that *every regulator of a system must be a model of such system*. This is where Beer's Viable System Model gains its power to model a viable system on different levels of recursion whilst maintaining the same definition of these required elements of such a viable system.

As such, the Viable System Model can as such be used to enter a deeper level of recursion, within a black or muddy box, taking away the complexity. Indeed, the use of the Viable System Model essentially acts as a variety attenuator for the system in focus (Beer, 1979).

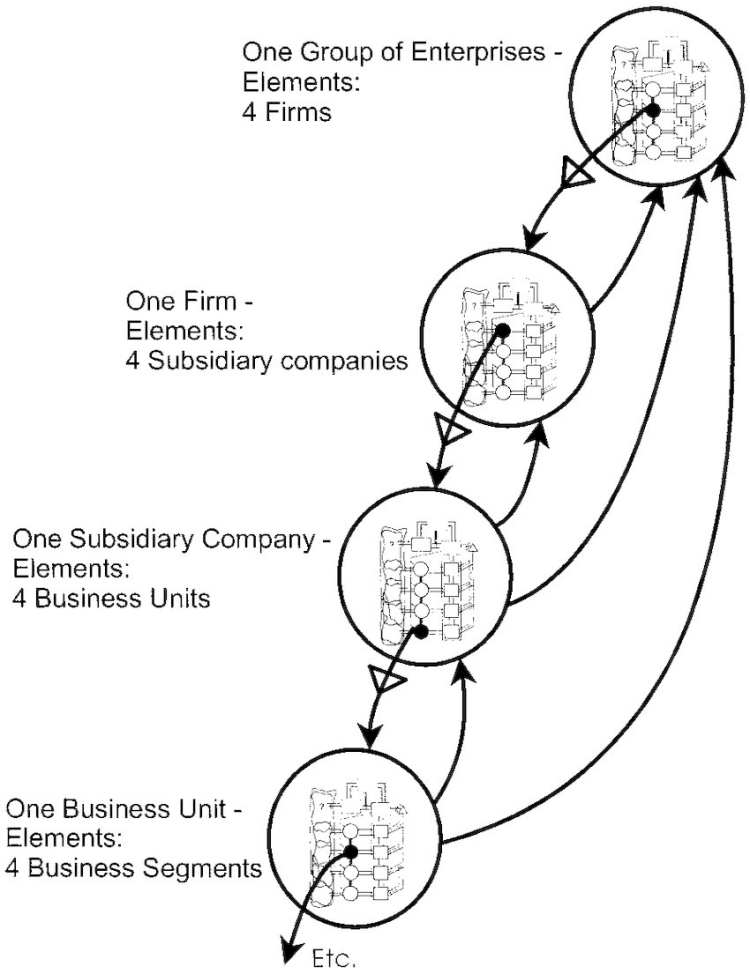


Figure 6: Organization of a corporation as conceived as a recursive process (Beer, 1979)

Beer (Beer, 1979), modelled a viable system as a neurocybernetic model consisting of five subsystems, feedback loops and information flows. Jackson (Jackson, 2003), furthermore, argues that the VSM is applicable to all systems, both to large and small organizations. As a matter of fact, De Haes & Van Grembergen (De Haes & Van Grembergen, 2015) wrote how the VSM can provide a perspective in Enterprise Governance of IT (EGIT) for maintaining homeostasis in a complex, adaptive system. This extends to Business Information Security Governance & Management as both are deemed part of the overall corporate governance (Veiga & Eloff, 2007).

4.3.2 The VSM subsystems

Stafford Beer defines five different subsystems in the VSM, each carrying a task dedicated to maintaining homeostasis within the system in focus. Beer refers to these as System One through System Five (Beer, 1972, 1979, 1984, 1985).

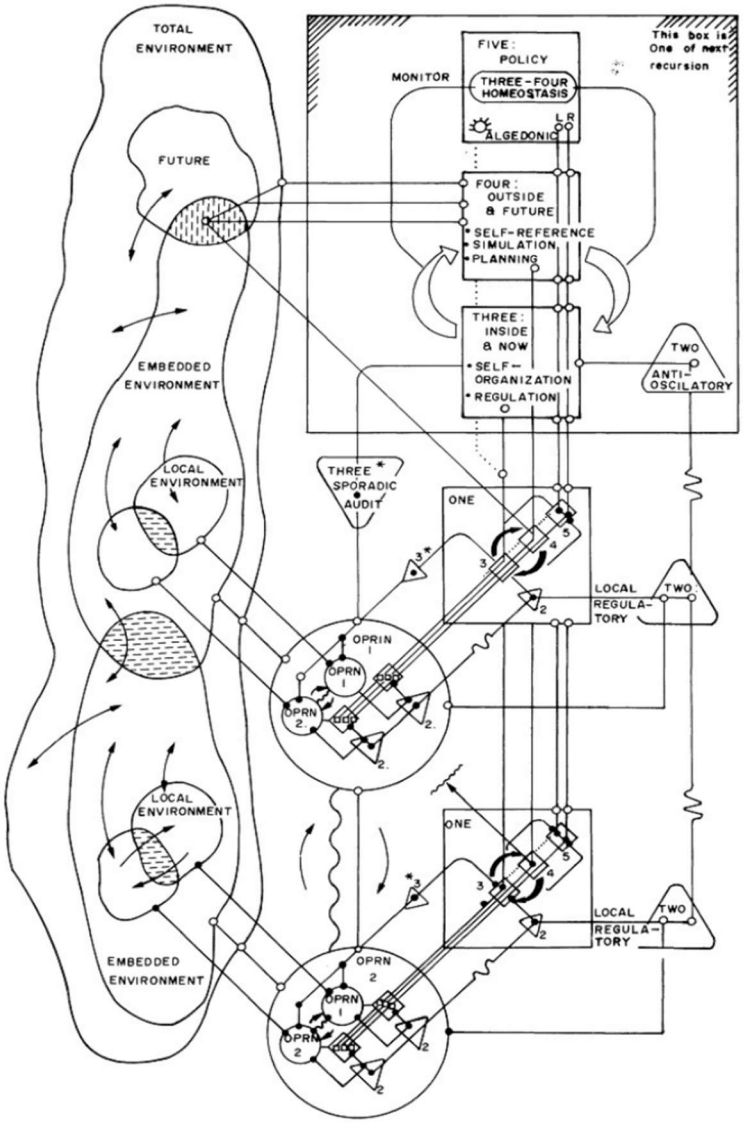


Figure 7: The Viable System Model by Stafford Beer (Beer, 1979)

System One: The operation function

Any viable system requires a purpose, and System One handles this purpose through the operations on local environments and regulated by their local

management units. Essentially System One, is the combination of local variety, the local operations (read purpose) and its local management.

System One thus includes all assets that have to do with the operation and its local regulation (e.g. local management units). Therefore, this System One of the system-in-focus is the combination of all embedded viable systems (Beer, 1979).

All operations within this System One are connected to each other on which organizational forces are at work. These forces might have oscillatory effects on other operations and can act as variety attenuators or amplifiers for which the local management units are responsible (Beer, 1979). This is where Ashby's law on requisite variety comes into management cybernetics and defines the manager as a 'variety engineer' (Ashby, 1956; Beer, 1979).

An important aspect to System One which Beer explains in his book 'Heart', is that System One should have the freedom to act. Indeed, System One should be autonomous, however…

System Two: The orchestration function

The freedom to act should be regulated or constrained, because should each operational unit exercise the freedom to act, without coordination, this would endanger the interoperability of the operational units and thus the viability of the system-in-focus (Beer, 1979).

This is the function of System Two which represents the orchestration between or within the embedded viable systems.

Beer (Beer, 1979) states that proper Systems Two need to be implemented which can deal with the left-over complexity with which System One cannot deal, however they should only minimally limit the freedom in which System One can operate. Furthermore, System Two is not a "commandeering" function, it provides the information to System One within which borders it can express its freedom. Indeed, System Two coordinates and orchestrates the operations of System One by providing "guidelines".

*System Three and Three *: The executive & audit function (inside, now)*

System Three of the Viable System Model consists of two main functions, namely the executive function referred to as System Three, and a monitoring or auditing function often referred to as System Three *.

System Three, or the executive function, has the responsibility to maintain systemic cohesion between the operations of System One of the system-in-focus, doing so however, without undermining the autonomy of System One. System Three can use two methods to establish this systemic cohesion, either by direct

interaction with the local management units of System One through the command axis or channel, or by adapting System Two. Furthermore, System Three is informed by System One's operations by the command axis which is also used for performance reporting. We can therefore state that System Three is the managerial function of the inside and now of the system-in-focus (Beer, 1979).

System Three *, or the auditing function, can directly interact with the operations of System One of the system-in-focus to gain information from System One's operations. System Three can then assert the performance reporting done by System One against its reality. System Three *, can by utilizing the outputs of the audit, call for modifications of System One by using the command axis. The auditing function of System Three ensures the accountability of System One and helps sustain internal homeostasis (Beer, 1979; De Haes & Van Grembergen, 2015).

System Four: The planning function (outside, then)

Just like any viable system, it is contained in an environment expressing variety on the system-in-focus. The managerial functions of Systems One, Two and Three aim to cope with that variety by performing variety engineering, utilizing variety attenuators and amplifiers to stabilize the internal environment of the system-in-focus. However, as we can find in Ashby's law on requisite variety(Ashby, 1956), variety or complexity will assert itself onto the system-in-focus if no actions are undertaken.

This is where System Four comes in, System Four defines the outward looking, future minded function of the system-in-focus. It supports adaptation, mutation, learning evolution, survival-worthiness, or in other words viability (Beer, 1979).

System Four is directly connected to the environment with the function of identifying opportunity and threat. Evidently, System Four is directly involved in strategic planning and works together with System Three for integration by using the balancing the inward view of System Three and the outward looking view of System Four(Beer, 1979, 1985).

System Five: The identity function

System Five monitors the integration loop between System Four (future) and System Three (present) and handles with the excessive variety generated. As such System Five is the ultimate decision maker within the system-in-focus (Beer, 1979). Therefore, we can derive that System Five is accountable that the system-in-focus remains viable by adapting to its external environment by maintaining cohesion between all its subsystems.

4.3.3 The VSM communication channels

The Viable System Model, next to the subsystems mentioned above, also consists of communication channels to ensure the holistic view of the system-in-focus.

Communication with the external environment

The Viable System can communicate with its environment, more precisely the embedded systems of System One are directly connected to their local, embedded environments. Furthermore, System Four is directly linked to the environment to express its identity and purpose but also to 'scan' the environment for opportunity and threat to anticipate the future and plan organizational change (Beer, 1979).

The command axis channels

The resource bargaining channel establishes the communication line which is used to agree on the degree of autonomy between subsystems, e.g. System One and its metasystem. Beer uses the correlation of Senior management and Junior management as examples (Beer, 1985).

The accountability channel is used to balance out the resource bargaining channel, in which System One reports on the performance of its operations to the metasystem (Beer, 1979, 1985).

The intervention channel can be used by the metasystem to intervene at the management level of System One. It can be used to enforce decisions from the metasystem towards System One and its operations (Beer, 1985; Huygh, 2019).

Balancing the present and future with the System Three and Four variety loop

To balance out the contradictory functions of Systems Three (present) and Four (future), there is a special communication tool, referenced as the Three-Four variety loop. It's function represents a management center according to Beer with its role as the strategic planning 'organ' of an organization. This organ constitutes change or adaptation of the system-in-focus against the environment in which it operates. Furthermore, this organ is overseen by System Five, which monitors the interaction between System Three and Four and aims to maintain the identity of the system-in-focus (Beer, 1972, 1979, 1985; Huygh, 2019; Huygh & De Haes, 2019).

Alarming the metasystem, the algedonic signal

Lastly, the Viable System Module has a way for System One to directly reach System Five in case immediate action is required. Beer refers to this communication line as the 'algedonic' signal, which passes crucial information from System One to the identity function (System Five), when there is an issue that impacts the purpose and thus viability of the system-in-focus (Beer, 1979, 1985; Huygh, 2019).

4.3.4 Review of the Viable System Model in literature

The Viable System Model (VSM), receives both praises and critiques in academic literature.

The VSM looks at the organization from a functional approach, decoupled from the organizational charts and persons. The model merely looks at the organization and verifies if the necessary function required to remain viable are present, no matter who is performing them. This enables to discover the organization's critical variables and install mitigating homeostats to ensure equilibrium (Leonard, 2009). Another example lies in the recursive nature of the VSM. In a viable system, the same relationships are found through the functions of each subsystem. Take a large corporation for example, the VSM offers a methodology to implement functional decentralization and holism, in which the relationships between the functions remain the same, be it a single store or the corporation in its whole (Espejo & Gill, 1997; Leonard, 2009). This is supported by the fact that VSM can be used to establish a 'common language' or 'transducer of variety' throughout the corporation (Espejo & Harnden, 1989).

Schwaninger (Schwaninger, 2006) claims that the VSM is a tool which can be used to reorganize and design organizations and enterprises. Van Caspel (Van Caspel, 2013), however proposes that we should take the claims of Schwaninger and other researchers with a grain of salt as in his opinion the VSM is solely a functional model. Indeed, the VSM can be used to diagnose the functional workings of an enterprise or organization, but for the design we need to combine the VSM with other knowledge or design rules (Van Caspel, 2013).

Another important criticism is that however VSM can proof its use in diagnosing the organization, it does require thorough knowledge about the functioning of the organization to map the organization to the VSM (Espejo & Harnden, 1989; Hildbrand & Bodhanya, 2015; Schwaninger, 2006; Van Caspel, 2013).

Another essential element to consider in a research involving a VSM diagnosis is that during an interview to gather information, the interviewee will not be familiar with the language used within the Viable System Model, therefore interview questions need to be very hands-on and practical (Hildbrand & Bodhanya, 2015). However, utilizing applied VSM questions in the interview to create the Viable System Model, can help to gain a comprehensive understanding of the

organization under research. This however, poses another potential problem as the research on practical implementations of the VSM is rather limited for novice VSM users (Hildbrand & Bodhanya, 2015).

4.3.5 Motivation to use VSM in this research

As personal reason I wanted to use the VSM as a lens in this research to expand my knowledge on management cybernetics and how I could apply this theory to practice. In particular I can value how Beer (Beer, 1972, 1979, 1984, 1985) managed to construct a model based on the biology of a living organism and apply this to organizational theory. In particular, the way the VSM is structured like an autonomous nervous system and how it can be applied to organizations.

The choice to utilize the Viable System Model within this research is motivated in literature because of its usefulness in diagnosing the functions of an organization and detect problems threatening its viability (Beer, 1985; Hildbrand & Bodhanya, 2015; Van Caspel, 2013). And however, VSM has its limitations, it can be extended by mapping the VSM with additional knowledge which will then act as design rules.

As such the goal to answer the main research question "How can viable information security governance & management be organized?" would require a mapping of the Viable System Model with design rules proposed by practitioner literature.

4.4 What is Information Security?

In modern times, data and information is often called the new "gold" or "oil" for doing business, as such information and more in generally, data, are considered an invaluable asset to the enterprise. The International Organization for Standardization (ISO) describes Information Security as the process to protect this asset against the loss of availability, confidentiality and integrity, often referred to as the "CIA Triad" (International Organization for Standardization, 2013, 2014).

The Information Systems Audit and Control Association ("ISACA") refers to Information Security as the act of maintaining the confidentiality, integrity and availability of information. Defining "information security" as information assurance, ensuring that the information is not compromised when critical issues arise.

Both organizations utilize the CIA triad at their core to define information security. Therefore, it is crucial to explain these 3 core concepts.

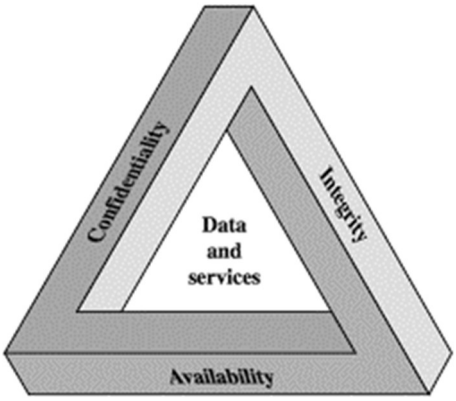


Figure 8: The C.I.A triad as industrial standard (Whitman & Mattord, 2011)

Confidentiality, often intertwined to the concept of "privacy, but in nature not to be used interchangeably", is the attribute of information to assure the information is not made available or disclosed to unauthorized third parties such as individuals, entities or processes. Confidentiality is thus a component of privacy to assure data protection from unauthorized viewers.

Integrity, specifically data integrity in the terms of information security, is the attribute of information to assure that the information is accurate, complete and has not (unknowingly) been modified by an unauthorized third party. Some definitions go further to include non-repudiation and authenticity (R. Von Solms & Van Niekerk, 2013).

Availability is the attribute to information to assure the information is available when it is requested upon. This essentially means that the underlying information systems and security controls in place are functioning correctly so the information may be accessed (Isaca, 2019).

In addition to the CIA triad, the International Standardization Organization (ISO) defined additional information security concepts, namely **authenticity, accountability, non-repudiation, reliability and auditability** (International Organization for Standardization, 2014).

Information security often used to be a matter of internal affairs, however with the digital evolution and the rise of networking and the internet, more and more stakeholders became involved. It is thus of no doubt that any organization needs to protect their information assets adequately as information has become the new gold on the market so to speak. And as the information technology evolves over time, so does the need for adapted information security. Where information security used to be a matter of simply implementing technical or even physical

mechanisms such as locks to secure the information storage of an organization adequately, nowadays a key element in information security is implementing managerial and administrative controls (R. Von Solms, 1998).

Von Solms and van Niekerk (R. Von Solms & Van Niekerk, 2013), even propose to make a distinction between traditional information security and cybersecurity. Information security is the act of securing the information as an asset whilst cybersecurity goes beyond and is the act of securing the vulnerabilities which exist inherently due to the use of ICT.

In short, information security is thus the act of securing a critical business asset from possible threats and vulnerabilities (International Organization for Standardization, 2014; B. Von Solms & Von Solms, 2005; R. Von Solms & Van Niekerk, 2013).

4.5 What is Business Information Security?

Information Security Management (ISM) has become a strategic issue for business leaders. Therefore, ISM should be a part of the Information Security Governance of an organization (SH Solms & Solms). Even as early in 1984, McFarlan (McFarlane, 1984) already recognized the importance of information technology for an organization to remain competitive in the market. And as mentioned earlier in this paper, the embedding of information technology in the core business strategies has its risks for which executive management and the board are accountable. This in combination with the wider understood impact and risks of not adequately protecting the IT resources and assets lead to the inclusion of Information Security Governance (ISG) as an overall part of Corporate Governance (Ruighaver, 2004).

Information Security Governance has become a discipline to mediate business risks, crucial for the protection of critical business information and its related information technology. In fact, this protection must now be seen as an integral part of wider business protection. Therefore, Von Solms introduced the term Business Security as it seems to be the best term to relate the fact (B. Von Solms & Von Solms, 2005).

As such Information Security Management has become a strategic issue for business leaders and due to its changed nature, taking a more business oriented role, Bobbert (Bobbert, 2018) proposes the term “Business Information Security”. Primarily since Business (legal entity within the firm) is the owner of the data and needs to collectively –together with IT- determine the risk appetite and required security control mechanisms to manage (mitigate, transfer (e.g. insure) or accept the risk while maintaining accountability for it. A definition continued in this research.

4.6 Viable Business Information Security Governance & Management

Soomro (Soomro et al., 2016) established that business information security needs a more holistic approach with the involvement of board, top level management, participation of managers from all business functions. Business information security is a business issue and as such it should be given appropriate attention, and not only from a technical point of view (Soomro et al., 2016; B. Von Solms & Von Solms, 2005; Williams, 2001).

Systems thinking and in extend the Viable System Model rely on this holistic view and as such the use of the Viable System Model can be a methodology used to conduct research in the field of business information security governance & management (Alqurashi et al., 2013; Gokhale & Banks, 2004; Huygh, 2019; Soomro et al., 2016).

A business information security management system can be viewed as holistic and sustainable when applying Beer's viability principles (Espejo & Harnden, 1989).

An overview of the VSM concepts applied to Business Information Security can be found hereunder.

Security Operations, or the operational function include the primary business information security activities which directly interact with the external threat environment. The subsystems may include endpoints connecting to the internet, firewalls, mobile devices, or applications such as antivirus and advanced threat protection software (Gokhale & Banks, 2004; Goldes et al., 2017).

Security Orchestration is the coordinating system including information channels to ensure that System One works harmoniously. A security incident event management (SIEM)-tool, security policies, custom threat indicators are variety attenuators who all have an anti-oscillatory function and help coordinate the business information security management (BISM) system (Alqurashi et al., 2013; Gokhale & Banks, 2004; Goldes et al., 2017).

Security Management is responsible for maintaining internal control over the BISM system. It is responsible for the resource allocation for the business information security operations (System One). Furthermore, system three monitors and analyses the primary tasks of the BIS operations and the coordination function of System Two (e.g. by defining security policies) (Alqurashi et al., 2013; Gokhale & Banks, 2004; Goldes et al., 2017).

Audit & Compliance monitoring, is the compliance monitoring function sporadically used by Security Management to ensure compliance of Security Operations with the defined information security policies and that the coordination function is able to maintain cohesion between the different layers of security operations and activities (Alqurashi et al., 2013).

Security Intelligence & planning is the business information security intelligence function. It is responsible to identify new emerging threats from the external environment that might impact the organization. Furthermore, System Four is responsible for the security strategy of an organization. A well-known example of System Four would be the chief information security officer (CISO) function (Alqurashi et al., 2013; Bobbert, 2018; Gokhale & Banks, 2004; Goldes et al., 2017).

Security Policy & Identity, policy, is the ultimate decision maker who provides clarity on the direction the organization should take. Its main goal is to steer the BISM system as a whole by providing a certain risk appetite so that threats and business opportunities are balanced. It is also responsible for establishing a security aware culture within the organization (Alqurashi et al., 2013; Goldes et al., 2017).

In terms of security, the communication channels defined in the Viable System Model are used to transfer information regarding information security events between the information security systems (One up to Five). **The command axis** for example consists of the **intervention channel** for when System One, Security Operations, can't cope with the changes in its related environment, it will seek a response from System Three (Security Management). On the other hand, Security Operations will have to report on security events to the Security Management system through the **accountability channel**. Furthermore, the **resource bargaining channel** can be used by Security Operations to ask resources from the Security Management system. For security events that require immediate attention, Security Operations can use the **algedonic signal** to escalate and demand a decision from System Five, Security Policy & Identity, when the event impacts the risk appetite of the organization (Alqurashi et al., 2013; Gokhale & Banks, 2004).

Maintaining internal stability is established with the **System three-four variety loop**, the security intelligence & planning system (System Four) scans the external environment to identify changes in the threat landscape and formulates a plan to implement and maintain the security of the organization. The Security Management system implements this plan whilst maintain cohesion within the organization. Finally System Five, responsible for establishing the security identity within the organization monitors developments between Security Planning and Security Management and makes the final decisions regarding the long-term business information security direction (Alqurashi et al., 2013; Gokhale & Banks, 2004).

A graphical representation of this model can be found hereunder.

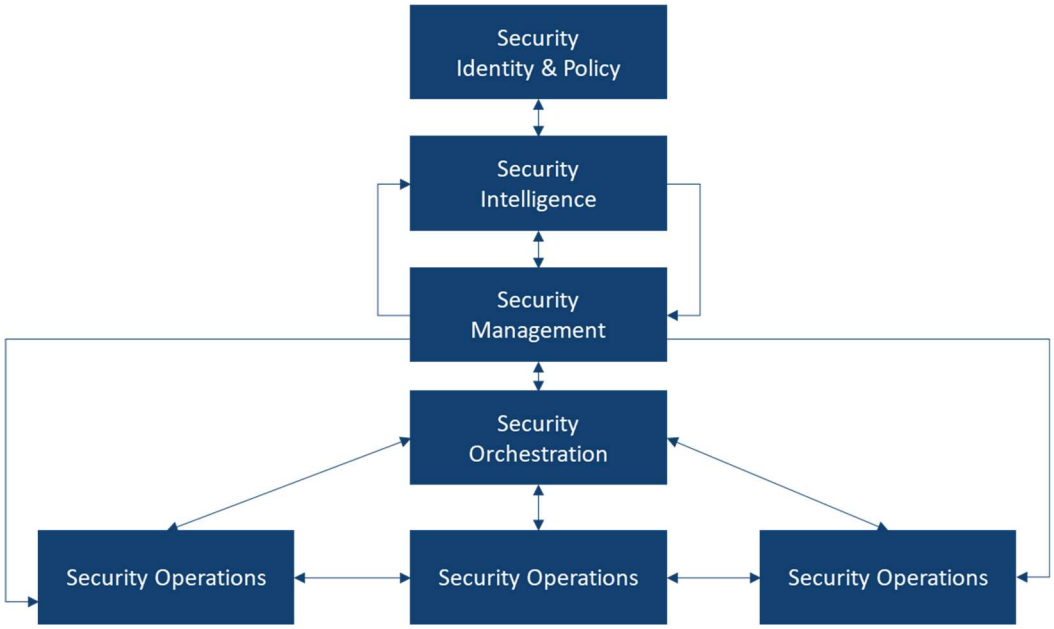


Figure 9: The proposed Viable Business Information Security Model (Own work)

The **link with the external environment** is not explicitly mentioned in the above model but remains a critical link in order to be able to organize viable information security governance & management in an enterprise context. The Security Intelligence function has a direct link with the external threat or technology environment in order to capture new data on threats that could affect the organization, or new methods and technology that could be considered in the enterprise strategic security plan.

VIABLE BUSINESS INFORMATION SECURITY THINKING

5

5 Viable Business Information Security Thinking

In this chapter, the application of Viable Business Information Security Thinking is further explained, moving away from the academic rigor to applying this thinking methodology in a practical mindset.

5.1 Constructing a viable Business Information Security Management System (vBISMS)

As established in chapter 4, this research takes into account the holistic nature of the Viable System Model to look at organization of business information security as a complex whole (Jackson, 2003). In order to construct a viable business information security management system this research will follow the blueprint constructed by Goldes (Goldes et al., 2017) which fulfills the design requirements for the artefact specification for a viable business information security system. In this paper , Goldes attempts to integrate multiple existing and generally accepted frameworks and guidelines for information security management systems, such as the Cyber Security Framework (CSF) by NIST, the Center for Internet Security (CIS) controls, the ISO 27001 standard, the Information Risk Assessment Method IRAM2 by the Information Security Forum, the Open Web Application Security Project (OWASP) test guide and finally COBIT.

Goldes (Goldes et al., 2017) revisits and reflects on each of these frameworks or best practices and maps these to the design requirements of a viable (business) information security management system. According to Goldes, the design requirements for such a system are the following.

- A viable business information security management system has a **risk-based design**.
- A viable business information security management system must accommodate **federation** of information processing.
- A viable business information security management system needs to be able to feed on external input and **integrate** them into a holistic business information security solution.
- A viable business information security management system must be capable of self-improving to adapt whenever controls fail to exert full strength on the relevant IT or information assets.

Furthermore, Goldes maps the standards, frameworks or sets of best practices on the design requirements for a viable (business) information security management system. Eventually, Goldes maps the five systems of the Viable System Model on the set of design requirements for a viable (business) information security system.

If we combine the 2 mappings of Goldes we can assume that the following proposed frameworks, standards and best practices can be applied to the respective system of VSM to implement Viable Business Information Security.

	Risk-based design	Federation	Integration	Self-improvement
Security Operations	-	-	-	-
Security Orchestration		NIST CSF OWASP	SANS CSC	
Security Management	ISO 27001 ISF IRAM2		SANS CSC	
Security Intelligence	ISO 27001 ISF IRAM2		SANS CSC	COBIT
Security Policy & Identity	ISO 27001 ISF IRAM2			

Using this mindset, we attempted to map the individual framework controls on each other. However, we must consider the limitations of the frameworks. For example, the Open Web Application Security Project (OWASP) test guide describes a testing framework to conduct the security of the software development life-cycle process, but does not support generalization to the broader process perspective to establish an information management system (Goldes et al., 2017).

Security Operations, surprisingly, was left out by Goldes during his mapping of the design requirements and the frameworks. However, if you think about it, security operations, by example an endpoint detection & response system, is implemented by security management and is orchestrated to work alongside other security solutions, as such a specific framework for “security operations” does currently not exist.

In this created mapping we included ISO 27001, COBIT 2019 and the Centre for Information Security controls. The OWASP testing guide was left out from this mapping due to the limitation as it does not support the generalization to a broader process to establish an ISMS. IRAM 2 was left out as the framework is a members-only methodology, however, after contacting the managing director of the Internet Security Forum we received the latest ISF standard of good practice which could be included in the mapping of the frameworks, this was however not done due to the time constraint put onto this research as this good practice framework includes 338 pages full of controls to be mapped.

Bias is, however, another limitation that needs to be considered when mapping these frameworks to the Viable System Model as a lot of this mapping can depend on interpretation of the researcher. In order to reduce as much bias as possible this mapping used inspiration from the NIST Cybersecurity framework to orchestrate the mapping of the other design rules of the artefact.

However, the mapping of the controls to the Viable System Model may serve as an initial methodology (viable system diagnosis) to quantify the viability of an organization.

5.2 Viable System Diagnosis with the draft artefact

The created draft artefact consists of:

- 83 controls, diagnosing System Five (Security Policy),
- 34 controls, diagnosing System Four (Security Intelligence),
- 85 controls, diagnosing System Three (Security Management),
- 47 controls, diagnosing System Three * (Audit & Compliance monitoring),
- 75 controls, diagnosing System Two (Security Orchestration),
- 60 controls, diagnosing System One (Security Operations).

5.2.1 Expert opinion on "Viable Business Information Security Thinking" and the prototype-artefact by Marcel de Haan

In order to validate our conceptual model of the Viable Business Information Security philosophy, and its protype-artefact implementation, this research asked the expert opinion of Marcel de Haan. Marcel de Haan has a wide-ranging area of expertise during a professional career of 28 years, ranging from Information Technology Auditor, to ICT manager, Business Analyst, Project Manager, Program Manager and Business Information Security Officer Assurance. Furthermore, Marcel de Haan is accredited with the Certified Information Systems Auditor certification by ISACA. Marcel de Haan is an expert in security frameworks due to his role where he introduced security frameworks such as the ISF framework to raise the maturity level of information security within NN-Group.

As mentioned, the interview had as main goal to receive a critical reflection and expert opinion on both the conceptualization of the Viable Business Information Security philosophy, as well as the first design cycle of the prototype-artefact as result from this design science research project.

In this interview we validated the fact reductionistic thinking within the field of information security often results in a false feeling of security, and that it is still the most commonly used methodology of looking at information security. This is because we often tend to tackle complex problems by simplifying them resulting in "check-list" based approaches without thinking and realizing what the impact on the organization is of implementing, firewalls, antivirus systems, etc.

During this interview, we discussed the created Viable Business Information Security Model and its underlying functions. Marcel de Haan validated the approach and philosophy behind the model and agreed with the holistic approach taken towards information security.

In order to discuss the model, we clarified how we constructed the prototype-artefact. We discussed Goldes's design rules for a Viable Information Security

Management System. Marcel confirmed these 4 design rules and how they are mapped to the Viable Business Information Security model.

When deep-diving into the construction of the prototype-artefact, we also discussed the difficulty of creating framework mappings because as Marcel de Haan stated, a lot of frameworks operate on a different 'layer' and often do not directly match on control level.

Marcel de Haan states that he indeed misses the ISF framework, as he thinks this would immensely benefit the mapping, as it would be the main contributor of the risk-based design principle, put forward by Goldes. Unfortunately, after contacting the managing director of the ISF, we were not allowed a license or approval to include the ISF standard in this research.

Marcel de Haan has confirmed that the mapping of this these frameworks on VSM could serve as a sort of Viable Business Information Security baseline, in order to benchmark, diagnose and propose recommendations. On the other hand, due to the nature of current frameworks which often lack this embedded risk management approach to map these models towards the constructed Viable Business Information Security model. One of the main limitations as observed by Marcel was the lack of how organizations would be able to work with this risk appetite, as this is in practice one of the major difficulties organizations face. Currently the framework mapping lacks what Marcel de Haan refers to as a "process-layer" for the continuous improvement of information security processes. One of the reasons is that these frameworks have a certain mismatch by nature, as these frameworks each operate on a certain layer. The frameworks complete each other but might have some overlap. Our prototype-artefact reaches on them but doesn't go into more depth.

The main conclusion from the interview is that the constructed Viable Business Information System Model and its philosophy is a viable methodology for looking at information security. However, the framework mapping would highly benefit from a methodology of prioritization based on the risk appetite from an organization. Therefore, this prototype-artefact requires further enhancements in order to be usable for its intended purposes.

5.2.2 Testing the prototype-artefact in a macro view

The prototype-artefact was tested at an anonymous company. All controls mentioned above were discussed with several stakeholders at the company and were discussed with the company's CIO. You can find the result of this viable system diagnosis below in the table.

The scoring of the artefact was done by handling a simple traffic light protocol

Viable System Function	Score	Relative score
System Five (Security Policy)	46 / 83	55.4 %
System Four (Security Intelligence)	25.5 / 34	75 %
System Three (Security Management)	45.5 / 85	53.5%
System Three * (Audit & Compliance monitoring)	27.5/ 47	58.5 %
System Two (Security Orchestration)	39 / 75	52 %
System One (Security Operations)	35.5 / 60	59.2 %

Table 3: Viable System Diagnosis Score

Hereunder you can find some high-level recommendations aimed at "Company A" which could improve their viability score.

Viable Business Information Security System Function	**Recommendation(s)**
Security Policy & Identity	Establish a formal ISMS Create and maintain business continuity plans Establish a formal risk appetite Create an incident scoring prioritization schema based on the risk appetite
Security Intelligence	Conduct continuity plan training Use, share and keep security knowledge within applicable departments up to date to maintain the security skills of personnel
Security Management	Document formally established ISMS Document business continuity response action plans and communication lines Manage identity & logical access Implement segregation on different levels
Audit & Compliance monitoring	Implement network monitoring and network data collection Conduct incident scenarios & test the business continuity plans Test data recovery plans
Security Orchestration	Establish rules for allowed business support tools, applications and software Implement standardized, secure configurations Orchestrate security by segregating networks based on security and manage these with dedicated networks & computers
Security Operations	Encrypt data on removable and portable devices Implement automated scanning tools

Table 4: High level recommendations to Company A after the Viable System Diagnosis

5.2.2.1 Validation of the results with the CIO of Company A

The results of this Viable System Diagnosis of Company A were discussed with the CIO of the company in question.

During this research, the concept of Viable Business Information Security Thinking was presented as a keynote at one of Beltug's N-Sights. The CIO of Company A was present during this webinar and during the interview we validated the graphical representation of "Viable Business Information Security Thinking". The CIO of Company A did confirm that the use of such a framework can help with maturing the baseline of security, required to keep the business viable.

Regarding the proposed recommendations that were the result of this Viable System Diagnosis, the CIO said that for most of them ideas, plans or projects are in start-up phase. Confirming that the outcome from the Viable System Diagnosis identified the attention points at Company A.

Furthermore, during the interview, we slightly touched upon the possible future research opportunities and expansion of this framework. The focus was on how prioritization would be embedded to enable (semi)-automatic roadmap creation for an organization. The main concern matches the feedback from the interview with Marcel, which is the difficulty of embedding the design factor of the risk-based design. But having this sort of a model in a way would help with the decision-making process to prioritize security investments. The CIO mentioned this seemingly is becoming a trend as certain security related software also provide security recommendations based on risk, impact & cost of implementation.

The fully transcribed interview (in Dutch) with the CIO of Company A can be found in Annex 4: Transcribed interview with CIO of Company A (Dutch only).

5.3 Introducing Viable Business Information Security thinking

The concept of viable business information security as used in the draft artefact is an application of what I like to call as Viable Business Information Security thinking. A concept much wider than just this artefact, but a way of looking at the organization of security within an enterprise on both macro and micro level.

For example, using the drafted artefact, we are looking at the macro level of the viability of the security organization within a system (e.g. an enterprise). This macro view allows us conduct a viable system diagnosis as introduced in chapter 4 Defining viable information security organization. This viable system diagnosis as shown, can be used as a first diagnostic tool on which recommendations can be built to improve the viability of an organization, reflecting the concept of variety engineering and attaining requisite variety (Ashby, 1956; Beer, 1972, 1979, 1985).

However, the same thinking methodology can also be applied when looking at a micro level of business (information) security, this correlates with the Viable System Model principle of recursion.

5.3.1 Applying Viable Business Information Security to a ransomware attack chain

As established in the section above, the concept of this Viable Business Information Security thinking can not only be used for execution a Viable System Diagnosing on the corporate system-in-focus but also to lower level recursions such as directly on an attack / kill chain.

An attack or kill chain, is a step by step process aimed at compromising the confidentiality, integrity and availability of a system. The word "chain" describes that a single failure (chain link) can destroy the entire process. A cyber kill chain is depicted with seven stages, namely reconnaissance, weaponization, delivery, exploitation, installation, command & control, actions on objectives, often referred to as persistence (Mihai, Pruna, & Barbu, 2014).

Hereunder you can find an attack chain example of a ransomware attack.

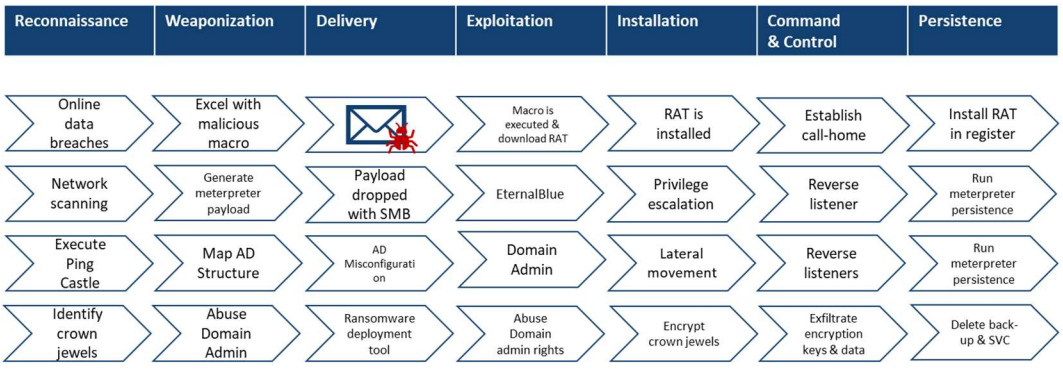


Figure 10: Example ransomware kill chain

You can find an illustrated model of how this thinking methodology in 4.6 Viable Business Information Security Governance & Management.

To make the concept and aforementioned model of viable business information security thinking more practical, this section will analyze the ransomware attack that occurred at an educational institution in 2019.

5.3.1.1 Incident introduction

The university held a symposium in February 2020 following a cyber-attack involving ransomware, a type of malware which can take files and computers hostage by encrypting them. These files and/or computers can only be decrypted using a decryption key. During this symposium, the institution and consulting company Fox-IT presented the root causes of patient zero and the lessons learnt from this cyber incident.

This university decided to provide full transparency on this incident for other organizations to learn from this incident. In doing so, they published the symposium and the finalized (partially pseudonymized) report from Fox-IT.

5.3.1.2 Incident timeline

Hereunder you can find a short summary of the incident timeline of the ransomware attack which occurred at the targeted educational institution.

Timeframe	Action
16th of October 2019, 12:52:28	A link in a phishing email was clicked and downloaded an Excel file containing a macro. This macro was executed and downloaded a remote access trojan (SDBBot).
16th of October 2019, 19:35:03	The attacker used the remote access trojan to install a meterpreter shell, in order be able to manually interact with computer systems of the victim.
17th of October 2019, 17:33:22 & 17:40:33	Possible abuse of the EternalBlue exploit to compromise the first initial servers and further rollout the meterpreter tool.
20th of October 2019, 19:00:33 & 19:02:45	Further exploitation of servers vulnerable to EternalBlue and roll-out of the meterpreter shells.
24th of October 2019, 11:38:50	Use of Powersploit to scan networks and find vulnerabilities on hosts.
24th of October 2019, 11:41:25	**Powersploit hack tool detected by Microsoft Defender.**

24th of October 2019, 15:17:57	Use PingCastle to map the active directory (AD) structure and find AD related vulnerabilities.
21st of November 2019, 13:06:22	Use EternalBlue to compromise another server and (unconfirmed but stole the password of a domain admin).
21st of November 2019, 13:19:53	Compromise of domain controller with domain administrator account, use of Cobalt Strike, Meterpreter and execution of PingCastle.
19th of December 2019, 14:49:25	Use of ADFind to create an overview of processes, services on servers and workstations.
19th of December 2019,	**Mimikatz hack tool was detected by antimalware solution. No action was taken as solution was in observe/auditing mode.**
19th of December 2019, 14:44:58	**Cobaltstrike was detected by antimalware solution. No action was taken as solution was in observe/auditing mode.**
23rd of December 2019, 17:53:52	Roll-out of the ransomware.
23rd of December 2019, 17:55:46	**Including alerts of ransomware found by the antimalware system.** Attacker removes anti-malware solution and disables built-in protection.
23rd of December 2019, 18:26:51	Ransomware execution started.
23rd of December 2019, 18:56:34	267 servers are encrypted by the ransomware, including critical systems such as domain controllers and back-up.

Table 5: Incident timeline ransomware attack

According to both the symposium and the forensic analysis report, provided by Fox-IT, during the entire kill chain there several indicators of compromise. These were marked in bold in the table above. According to the symposium, individuals who received the initial phishing email also reported this by using the internal procedure at the institution.

5.3.1.3 Applying Viable Business Information Security Thinking to a ransomware case

We can use the combined knowledge of VSM, our prototype-artefact, inherent knowledge on information security and the already established recommendations from Fox-IT in the report to propose actions against a ransomware attack. We've mapped both the recommendations from the FOX-IT report and listed the references from the Viable Business Information Security Cross model in the table below.

	FOX-IT	**Viable Business Information Security Cross Model reference(s)**
Security Policy & Identity	Handle the principle of least privilege Implement a patch management policy / procedure Establish an incident response plan Establish a data recovery plan	SP001: A yearly evaluation of the governance system. SP002: Monitor the governance system & compliance to the governance system SP005: Utilize a risk rating process in order to direct risk management. SP006: A yearly evaluation of resource management used for security. SP009: Communicate management objectives, direction and decisions made regarding security. SP011: Establish roles and responsibilities for security. SP030: Ensure responsibilities and authorities for roles relevant to security are defined, allocated, assigned and communicated. SP031: Determine the need for internal and external communications relevant to the ISMS SP034: Define a set of policies, approved by management, which are published and communicated to employees and relevant parties. SP051: Establish and maintain a configuration repository and baseline and limit access to scripting tools. SP055: Define classification schemes for incidents and service requests which includes a prioritization schema. SP056: Investigate, diagnose and allocate all incidents. SP057: Define a business continuity policy, the objectives and its scope. SP058: Maintain business resilience by implementing redundancy to meet availability requirements.

		SP059: Manage backup arrangements with the inclusion of a backup policy and backup test plan. SP062: Manage endpoint security by disabling workstation to workstation communication. SP064: Manage endpoint security by disabling peer-to-peer wireless network capabilities on wireless clients. SP068: Manage user identity and logical access by changing default passwords. SP069: Manage user identity and logical access by using a password management system, ensuring the use of high quality, unique passwords. SP073: Manage user identity and logical access by establishing a documented and reviewed access control policy based on business and IT security requirements. SP079: Manage sensitive documents and output devices by encrypting sensitive information at rest.

Security Intelligence	Provide security awareness training	SI004: Maintain an understanding of the enterprise environment in the context of information security. SI005: Monitor and scan the technology environment to find appropriate security solutions. SI006: Assess the potential of emerging technologies and innovative ideas in the context of information security. SI007: Maintain the skills and competencies of personnel SI017: Identify and classify sources of information for governance and management of IT security, including a skills gap analysis to improve knowledge repository. SI018:Organize and contextualize information into knowledge by performing a skills gap analysis. SI019: Organize and contextualize information into knowledge by delivering training to fill the skills gap. SI021: Organize and contextualize information into knowledge by implementing a security awareness program.

		SI022: Use and share knowledge to train workforce on identifying social engineering attacks. SI025: Use and share knowledge to train workface on identifying and reporting incidents. SI031: Manage the environment by maintaining appropriate contacts with relevant authorities. SI034: Protect against malicious software by implementing detective, preventive and recovery controls combined with appropriate user awareness.

Security Management	Implement a centralized configuration management database	SM004: Evaluate risk management yearly. SM007: Define and implement infrastructure, services and applications to support the governance and management system of IT security. SM008: Manage continual improvement of the IT security management system. SM009: Develop an enterprise architecture vision on IT security. SM013: Maintain security portfolios. SM014: Manage benefits achievement from IT security. SM015: Prioritize the resource allocation to establish, implement, maintain and continually improve the information security management system. SM019: Provide input to the continual improvement of information security services. SM025: Collect security related data, ensure adequate log storage and ensure log facilities are protected against tampering and unauthorized access. SM026: Collect data & event logs in a central log management tool, record user activities, exceptions, faults, information security events and regularly review them. SM035: Manage data backup and restore arrangements. SM046: Identify and record current assets in order to maintain an accurate and up-to-date inventory of all technology assets, including hardware, with the potential to store or process information.

		SM054: Manage critical assets by maintaining an inventory of sensitive information. SM057: Establish and maintain a configuration model in order to establish secure configurations. SM063: Define classification schemes for incidents and service requests in order to document incident response procedures. SM064: Define classification schemes for incidents and services requests to assign job titles and duties for incident response. SM066: Investigate, diagnose and allocate incidents to decide if the incident is to be classified as information security incident. SM068: Develop and implement required business continuity response for information security during an adverse situation. SM069: Manage backup arrangements by protecting backups, creating backup copies of information, software and system images. Test backups regularly. SM070: Manage backup arrangements in order to ensure that all backups have at least one offline backup destination. SM072: Manage user identity and logical access by maintaining an inventory of administrative accounts. The allocation and use of privileged access rights shall be restricted and controlled. SM073: Manage user identity and logical access by ensuring the use of dedicated administrative accounts. The use of utility programs (services) that might be capable of overriding system and application controls shall be restricted and controlled. SM078: Manage roles, responsibilities, access privileges and levels of authorities in order to segregate conflicting duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets. SM079: Ensure traceability and accountability for information security events. SM080: Establish a monitoring approach for information security.

		SM084: Follow up on recommendations and actions.

Audit & Compliance monitoring	Implement a log monitoring system such as a SIEM and regularly tune this solution.	ACM004: Collect data by activating audit logging. ACM005: Collect data by activating detailed logging such as user activities, exceptions, faults and information security events. Regularly review these logs. ACM006: Collect data by enabling DNS query logging. ACM007: Collect data by enabling command-line audit logging. ACM008: Collect data by configuring monitoring systems to record network packets. ACM009: Collect data by deploying network-based IDS sensors. ACM010: Collect data by enabling the collection of Netflow and logging data on network boundary devices. ACM011: Collect data by decrypting network traffic at proxy. ACM012: Collect data by enforcing the detailed logging for access or changes to sensitive data. ACM013: Analyze risk by regularly reviewing logs. ACM027: Exercise, test and review the business continuity and disaster recovery plans by conducting periodic incident scenario sessions for personnel. ACM028: Exercise, test and review the business continuity and disaster recovery plans by conducting regular external and internal penetration tests. ACM029: Exercise, test and review the business continuity and disaster recovery plans by performing periodic red team exercises. ACM030: Review, maintain and improve the continuity plans at regular intervals in order to ensure that they are valid and effective during adverse situations. ACM031: Manage backup arrangements by testing data on backup media regularly in accordance with an agreed upon backup policy.

		ACM033: Manage user identity and logical access by monitoring attempts to access deactivated accounts. ACM035: Manage user identity and logical access by having asset owners reviewing users' access at regular intervals. ACM036: Manage vulnerabilities and monitor the infrastructure for security-related events by comparing back-to-back vulnerability scans and obtaining information about technical vulnerabilities in a timely fashion to address the associated risk. ACM038: Review the effectiveness of business security process controls at planned intervals.
Security Orchestration	Block, the use of unsigned macro's from being opened in email clients Add high level privileged users to the "Protected Users" group Implement a log monitoring solution which is fed by all security related applications in use	SO003: Manage vendor risk by ensuring that software is supported by the vendor. SO004: Manage vendor risk by including requirements to address information security risks associated with ICT services in agreements with suppliers. SO008: Maintain a risk profile and regularly tune a SIEM to fit this risk profile. SO024: Establish and maintain a configuration repository and baseline by utilizing application whitelisting. SO025: Establish and maintain a configuration repository and baseline by implementing the whitelisting of libraries. SO026: Establish and maintain a configuration repository and baseline by implementing application whitelisting of scripts. SO031: Protect against malicious software by centralizing anti-malware logging and providing appropriate user awareness. SO032: Manage and control network and connectivity security to protect information in systems and applications by subscribing to a URL-categorization service. SO033: Manage network and connectivity security by logging all URL requests, event logs recording user activities exceptions, faults and information security events. Regularly review these logs. SO034: Manage & control network and connectivity security by using DNS

		filtering systems and event logs recording user activities exceptions, faults and information security events. SO035: Manage & control network and connectivity security by implementing DMARC and enable Receiver-Side verification. SO036: Manage & control network and connectivity security by blocking unnecessary file types. SO037: Manage & control network and connectivity security by sandboxing all email attachments. SO038: Manage & control network and connectivity security by managing network devices using multi-factor authentication and encrypted sessions. SO039: Manage & control network connectivity security through a dedicated network. SO040: Manage & control network and connectivity security by denying communications with known malicious IP addresses. SO041: Manage & control network and connectivity security by denying communication over unauthorized ports. SO042: Manage & control network and connectivity security by segmenting the network based on sensitivity. SO045: Manage endpoint security to appropriately protection information in electronic messaging by ensuring only using fully supported browsers and email clients. SO048: Manage endpoint security by enabling operating system anti-exploitation features or deploying anti-exploit technologies. SO049: Manage endpoint security by configuring devices to not auto-run content. SO052: Manage user identity and logical access by using multi-factor authentication for all administrative access in accordance with the access control policy and the secure log-on procedure. SO053: Manage user identity and logical access by using dedicated workstations for all administrative tasks.

		SO054: Manage user identity and logical access by using dedicated machines for all network administrative tasks. SO055: Manage user identity and logical access by requiring all remote login to use multi-factor authentication in accordance with the access control policy and secure log-on procedure. SO057: Manage user identity and logical access by requiring multi-factor authentication in accordance by the access control policy and secure log-on procedure. SO071: Secure information assets by protecting media containing information against unauthorized access, misuse or corruption during transportation.

Table 6: Viable Business Information Security Recommendations ransomware case for an educational institution

5.3.1.4 Interview with the CISO of the University hit by ransomware

First of all I'd like to thank you for the opportunity for this interview. It is a rare event that when a company or institution is so open when they have been struck by cybercrime, to communicate so openly about it. I think this has opened a lot of opportunities for other companies or institutions to think about their security.

Having studied at the University of Maastricht for a few months during the module of Corporate Governance during my masters, and having developed a certain bond with the university, may I ask, how is the University currently doing, has everything been resolved so far?

Currently the university is doing good, we have more new registrations of students compared to last year, however these events probably don't relate to each other. Also another important factor to take into account is that one crisis was followed by the other. The first being the cyber crisis, the latter being the corona crisis.

This means we have to put a strong effort into video & conference tooling & online educational tooling. So both crises and the required follow-up are running parallel currently. We can currently manage, but the people from the IT department are experiencing a lot of pressure. In terms of the cyber incident, we have implemented strengthening measures and there is an audit, assessment ongoing

to verify the effectiveness of the action plans and to validate that the investments of the remediation plans are in proportion to the risks to be mitigated.

The university gave the authorization to FOX-IT to publicize the detailed report of the ransomware events at the University of Maastricht, how do you feel about this?

First of all, I would like to rephrase this question. It was not that the University gave authorization to Fox-IT to publicize the report. It was the other way around, we decided, quite fast, to publicize this report and let the community benefit from our lessons learned. This because we are a public institution. So we are subject to the legal principle of public administration. This means that the data regarding this incident can be requested by journalists. We have 25.000 users, including some of which are internal journalists which wouldn't be afraid to score a scoop. So we assumed that all internal communication would automatically become external communication. In that regards we assumed that we wouldn't be able to keep certain details secret from the incident, so we chose to make these public, even, and probably the most difficult of all, details concerning the payment of the ransom fee. But it was still a difficult topic to discuss. But it was Fox-IT that had concerns in regards of being this transparent, as they had never experienced such a request.

So even in the report, it was quite difficult what to include and what would be left out. A specific example was details on backup arrangements. The press stated that our back-ups were gone, but our central research database of 2 petabytes was left completely untouched, so in that sense you can hardly say that all our back-ups were gone.

So in that sense we wanted to include these details to provide facts. So when Fox-IT stated that servers were encrypted, we would state that only Windows Servers were encrypted, the Unix-based servers were unharmed. Including these facts helped people without context with reading the report to fully understand the scope of the incident.

Personally I was in favor for this level of transparency because I'm also in favor of sharing knowledge and data. But we kept monitoring if the right nuance was being included in the report.

Because there's a strong difference between "we don't have something well documented" or "we didn't do something well".

But it was entirely our decision to be this transparent, and perhaps it was even a nice lessons learnt for Fox-IT on communicating this transparently.

Another university was also hit with ransomware, if they would have been just as transparent and shared the indicators of compromise, we would have seen that our university received the same email, except we didn't know. When we got hit

with the ransomware, we've shared these indicators with colleague-universities and one of them responded they "crawled through the eye of a needle", because the hackers also already got in up to a certain point.

Prior to the events of the ransomware outbreak, did you feel there was a right level of resources and awareness for cybersecurity?

It was a combination of factors. We used the momentum of the GDPR to put some more pressure on the cybersecurity topic. Before, there was not that much administrative attention, because nothing had happened yet. Funding mainly went to the primary institutional processes such as education and research and less to the supporting services. I was also temporary the Data Protection Officer, during which I gave some presentations on cybersecurity and privacy.

In that period we also worked on a national level to identify the cyber threat landscape in SURF context (www.SURF.nl). I communicated the outcome thereof to our Quality & Risk Board, which enabled us to have some action points on our roadmap. An example being the implementation of a SOC, which would have started in January 2020, unfortunately a bit late. Another topic was software-defined networking in order to be able granularly segment our network, which was also planned for 2020. This was a longer term project however due to the scope. However, "thanks" to corona, we were able to install the hardware the first half of 2020 without hindrance. On the soft-ware side however we need to go in more discussions with the business side. With these project there were also FTE's included. E.g. Initially we asked 3 FTE's for our UM-SOC, but only received 2. However, budgets have been raised and we are now looking for that third FTE.

So we did have certain things on our roadmap. Such as a pilot for two-factor authentication.

So I just already mentioned three security measures that were started before the incident.

In addition I was 'relieved' from my GDPR function, in order to fully focus on the security side.

So the attention was there up to a certain degree, but perhaps a bit late.. We worked on new security governance, security by design, by default. This new governance was ready in October before the incident. The timing of the ransomware was very unlucky. there was also a reformation of IT going on during the past years, such as moving to an agile methodology, product ownership, multidisciplinary teams, ... So this required a new method of thinking. So there was a focus on functionality whilst security came more secondary in that aspect.

So yes the timing definitely wasn't in our best interest.

Being a CISO myself and luckily not having to had dealt with such malware before, how did you live and cope during the ransomware outbreak?

Personally I didn't have a lot of issues to cope with the incident. Don't get me wrong I still believe it was a grave incident. But I quickly turned my mentality into "Okay, the incident happened, what do we do now?". When I first got on-site, I immediately saw the severity of the incident, we took some first actions. So we didn't wake up our extra technicians, because they would require that rest for the long days to come.

So yea, basically everyone did overtime during this period. During these times it was no exception to be in the office for 10 hours and working 15 hours. Luckily I don't require too much sleep, I have short nights, but I sleep well. In the end, you just worked a lot of hours in that period.

I had also concerns on a personal level, in order ensure that the colleagues didn't go too far in their involvement, because they wanted to work and help, but they couldn't. But we wanted to make sure that he was fully rested and in shape as we would require his role on a later date so that other people could take a break for a few days.

But of course it's very personal how you would react as a person on such a situation.

How fast did you react to include Fox-IT? As there were indications of the grave severity.

We also have a CERT team which I also chair. So when someone detects a problem, another person should be included at minimum. This in order to never take individual decisions or actions. And then you start documenting the actions take, include more stakeholders.

In this case the IT director was also made aware quite fast along three technicians from our UM-CERT team. And later on the evening I was asked to go on-site due to the severity of the situation. We knew that it was ransomware, we shut-down the network, … After a short briefing, we called the SURFcert team (https://www.surf.nl/surfcert-247-ondersteuning-bij-beveiligingsincidenten), we tried nomoreransom.org, and then we called Fox-IT because they have a 24/7 helpdesk to check whether they still had tips for us and if our actions were the right things to do.

And we asked if they had the resources to help us with the intervention. We also decided to involve the Crisis Management Team, so the morning after we discussed the situation within the Crisis Management team and decided to call in the help of external experts.

Luckily we have a lot of skilled people, knowledgeable of ethical hacking and forensics. These are the same people you require to detect what happened, to document what happened and to repair what happened. But you can't do everything at the same time. We needed extra hands. On the other hand Fox-IT was quickly able to put extra sensors in the network, able to grant us 24/7 monitoring. So you do this in a sort of emergency contract. So we used both their experience but also their manpower.

After the events of the ransomware attack, has the awareness on the importance of cybersecurity changed in any sense?

Yes 100%, security will receive more attention on the agenda. The executive board will still question whether or not an investment is required, but if the experts advise something that is really necessary, they will take the appropriate action as advised.

Of course they will keep challenging whether or not the cost and/or investment is justified, but if it really is necessary we are allowed to work out a proposal and the discussions on what a solution would cost follow later.

So yes, the mentality has changed, we are less questioned on whether or not to implement a tool, the first approach now is to investigate and find a solution when this is deemed necessary by the experts.

And what major changes has the university undergone in order to prevent another attack of this scale?

For one, we quickly decided to implement a new baseline hygiene for our servers. We created traffic matrices from these servers and implemented them. The extra segmenting of the network on hardware level, and soon on software level. Segmentation of administrative rights and the structures of Active Directory have been adjusted according to the recommendations.

The incident response plan, data recovery plan could do better, but that was something that was already on the radar. We already did crisis management exercises prior the cyber-attack. Which led to the decision to work on a blue print for ICT incidents in the incident response plan, just as we have other specific blueprints which are niche to our educational and research operations. So we already had our CERT team, but we still needed to find the time to write this specific cyber incident blueprint.

And of course the example of the external audit and assessment we started. I think the incident response as such worked, but in terms of data recovery, before the incident we focused too much on online, redundant backups. We now created an extra backup in the cloud, which took 3 days in order to complete. But in order to restore this would take 7 days. So we need to make a strong distinction between data recovery objective and recovery time objective.

We also will start next week with some new awareness campaigns linked to the publication of the Higher Education inspection report and with some short statements and stories. And extra awareness programs for managers and IT staff. And in times of corona, we already used this situation for some extra security communications for safe homeworking.

And we are also looking into extra tools to register new processes enacted on servers and to identify our crown jewels.

Of course, we are also working on the implementation of our SOC with the 2 FTE', and the hiring process for a third has started. We are also investigating for a SOC on national level in a managed service.

We are also investigating how we can tackle macros, such as only allowing signed macros, but nowadays cybercriminals also sign their macros. And the warnings are usually ignored because people don't read them as the warning seems innocent. So we are looking at removing administrative access, but some people require them to perform their research. So we could investigate in privileged access management, but this would require an additional investment.

According to the public FOX-IT report there were several security mechanisms and controls in place, what do you think was the cause that the malware was able to spread?

The phishing mails had some minor differences so they were falsely identified as a double and no follow-up action was not performed on this second web URL. When the mails were reported, some people already clicked, but the web URL's were blocked later. So when the service desk saw the malicious warning, they mentioned that the web URL's were already blocked, which was a misinterpretation.

So there was a large stack of unfortunate events which lead up to the initial infection of malware with a macro. In the second phase, we didn't detect the lateral movement due to an insufficient level of logging and monitoring. We did not have the additional network sensors at the time. Nowadays we are better alerted of such suspicious behaviors.

With 25000 people we can't prevent phishing, we have to ensure that they can damage the organization as little as possible.

In regards to the malware alert which was detected and removed, it was seen as a 'positive'. So the interpretation was that the virus scanner did its work, but it was still a signal that something was wrong. I also want to emphasize on the timeline of the ransomware deployment and encryption. In half an hour the ransomware distribution software was deployed and another half an hour later, the 276 Windows servers mentioned in the report were encrypted. So we were never going to be able to take manual action to shut down the network in time. And on

the other hand, we wouldn't shut down the entire network, just because a virus was detected.

We should have been able to detect it during the lateral movement phase. And we should perhaps also add more importance and weight when investigating phishing mails, asking whether or not users have clicked, etc.…

Would you agree that a more holistic approach, with a more orchestrated security approach would counter these advanced threats, taking the integration and correlation of security alerts as example?

Yes indeed and I believe that monitoring, logging and good use cases integrated on your systems can help. And of course automation should also be in balance, because I don't want to wake up at night for false positives.

Also the business model from ransomware has changed over the years, where they first encrypted individual devices. Where in the older cases of ransomware hackers just wanted some quick money, restaging a device and restoring a back-up was enough. They now target and manually perform complex actions to encrypt organizations, bypassing several layers of defense.

Finally using the research I conducted, I created a framework mapping and applied the publicly available information on the ransomware case, do you think the recommendations are of value to the university?

Personally, I don't like to have these kind of lists. We have a database of minimum actions to do, but even then I receive questions like "What do I really need to do", because it is still to vague. I went through your recommendations quickly, and there are no things in there that seem wrong, but they remain on a too high level to implement with concrete actions.

I get the theoretical setting of these recommendations, but they still need to be translated in concrete actions that can be by the question "what do I need to do?".

This may be interesting for profiles such as CISO's, but for management this might be too difficult to translate into concrete actions.

CONCLUSION, LIMITATIONS AND FUTURE RESEARCH OPPORTUNITIES

6

6 Conclusion, Limitations and Future Research Opportunities

This chapter describes the final conclusions, answers, limitations and the future research opportunities to the research questions. The aim of this research was to answer the main research question "How can viable business information security governance & management be organized?". The initial target result of this research was to construct an artefact specification which could help organizations in the viable organization of their information security management and governance.

However, based on our literature study, case study and dissection of a real-world malware outbreak example, this research ended up with a new vision towards the organization of business information security.

From my own practical experience, IT security was often divided between certain specific branches such as "end-point", "Mobile device", "Cloud", "Web", "Email" security, to name a few examples. However, with this research now in mind, I've stepped away from thinking in these "security silos" and moved on by looking at the organization of business information security at a holistic level.

6.1 Conclusion

This research attempts to bring together the practice and academic worlds to create an artefact specification and draft artefact. This draft artefact should be able to diagnose, propose remediations in order to organize "viable" business information security. Furthermore, this draft artefact should be able to provide a benchmark methodology for organizations.

In order to provide an answer to our main research question this research was split up into three sub-research questions found hereunder.

- How does business information security relate to the viable systems model?
- What are good design rules to extend the viable system model to diagnose the viability of business information security governance & management?
- Which combined set of business information security principles and practices lead to the viable organization of business information security governance & management?

To answer the first sub-research question "*How does business information security relate to the viable systems model?*", we answered the following three knowledge questions which were used to conduct a literature research.

- KQ1a: What is Information Security?
- KQ1b: What is Business Information Security?

- KG1c: What is the definition of a viable organization regarding business information security?

What is Information Security?

The literature research conducted describes information security as a process to protect information assets against the loss of availability, confidentiality and integrity, and is expanded with the protection of the authenticity, accountability, non-repudiation, reliability and auditability of this assets. Information security has a strong focus on the protection of information assets and should be considered a segment of the wider definition of cybersecurity. The digital landscape has, furthermore, evolved to a point where more stakeholders and valuable assets beyond information are included in attack chains as can be seen in the public case of the University of Maastricht.

What is Business Information Security?

Following the digitalization of information, their carriers and stakeholders, information security management has become a strategic issue. The implementation of new technology in business processes brings the accountability and risks of using this technology and the accompanying security requirements to the strategic level within an organization. As such information & technology (IT) security alongside its governance and management has become a discipline to prevent materialization of business risks accompanied using technology and information.

We can formally define Business Information Security as the required discipline within an organization in order to tackle strategic issues which exist due to the use of information technology and aimed at protecting the strategic drivers and value creation from a business.

What is the definition of a viable organization in the context of business information security?

In order to propose a formal definition for a viable organization in the context of business information security we need to consider the following elements which make up the proposed Viable Business Information Security Model.

The viable security organization:

- interprets security as part of “business security” as a whole, with a holistic lens;
- has and receives the means to organize its security operations to directly interact with threats and take autonomous actions within a certain framework of autonomy;

- has the capability to orchestrate business security by coordinating and integrating its security operations;
- has the capabilities and resources in order to maintain internal control (homeostasis in cybernetic terms), cohesion, and compliance over the organization of security in the organization, and where needed to quickly adapt in response to the latest security intelligence;
- has a complete overview of the applicable security intelligence concerning the organization, meaning both the threat environment which could impact the organization, but also about the security posture and possible remediations;
- has a well-defined risk appetite, can make well-informed decisions, provides strategic direction of the organization of information security and establishes a security aware culture.

An organization is thus viable in the context of business information security when the organization is autonomous, self-learning and improving itself based on actionable intelligence considering a well-defined risk appetite.

In order to establish the design rules for our draft artefact, this research conducted a literature study on viable business information security. This is a rather new field of study within information security which was proven by the search results. Nonetheless, this research found an artefact blueprint with design rules to establish a prototype-artefact. The elements mentioned above almost, if not completely match with the design requirements proposed by Goldes (Goldes et al., 2017).

The risk-based design requirement from Goldes for an information security management system, matches with our Security Policy & Identity function, which should establish a well-defined risk appetite.

The federation requirement matches with the Security Orchestration function in order to be able to coordinate and integrate the Security Operations and facilitate processing of information related to security.

Goldes also explicitly mentions the self-improvement and adaptability requirements which match with our Security Management and Security Intelligence functions and their variety loop.

This research attempted to use these design rules to construct a draft artefact with respect to the blueprint established by Goldes by using NIST as orchestration framework to map the SANS CSC, COBIT 2019 and ISO 27001. Which answers the third, and final sub-research question "*Which combined set of business information security principles and practices lead to the viable organization of business information security governance & management*".

Which brings us to answer on the main research question "*How can viable business information security management & governance be organized?*".

Viable business information security management & governance can be reached by applying the concept of viable business information security thinking which implies:

- looking at security through a holistic lens;
- granting autonomy to security operations;
- orchestrating security by coordinating & integrating security operations;
- having actionable Security Intelligence from both your internal as external security posture;
- defining policies according to the risk appetite of the organization.

6.2 Limitations

The research conducted was challenged by several limitations which need to be considered. First off, the time constraint limited us to stay on a fairly high level when working on the use cases to provide a practical realization of this viable business information security thinking methodology. Due to the fairly new approach embedded in the field of security, a lot of time was used to establish this viable business information security thinking methodology with rigor.

For the creation of the draft artefact we were not able to include all Goldes's proposed principles, practices and frameworks, either because of this time constraint or because the frameworks were not publicly available such as the Internet Security Forum's IRAM2.

Although this research used the NIST framework to map the individual controls on the Viable System Model, it is still subject to bias and personal interpretation. Due to the novelty of this research field within security, we were not yet able to conduct a GSS research to confirm the mapping of our proposed Viable Security System Cross Reference Model.

In this research sometimes we refer to the viable system in focus. One of the limitations is that most of the recommendations by the proposed Viable Security System Cross Reference model are aimed at the enterprise level. Because the Viable System Model is recursive in nature this research attempts to propose a thinking methodology which could be used in lower level recursions such as security application level.

Some of the recommendations are quite vague and could benefit from a GSS research session to propose alternate wording in order to clarify the meaning of certain controls. However, in most cases, this is a limitation, in nature to the frameworks utilized.

6.3 Future research opportunities

Viable Business Information Security Thinking is a new playing field in the discipline of security, the result of combined knowledge from the academic, more theoretical world and from a practical side, using industry best-practices.

This research would benefit from refining the Viable Security Cross Reference Model by conducting GSS research and establishing consensus on the mapping of the frameworks. On the other hand, multiple case studies should be conducted to confirm the workings of the draft artefact as we were limited to a single case study due the time constraint.

The Viable Security Cross Reference Model could be enhanced with more concrete advise and a priority scoring.

Another research opportunity would be conducting seminars explaining this Viable Business Information Security thinking philosophy and conduct a survey research in order to understand how security decisions are influenced.

ANNEXES

Annexes

1. Annex 1: Literature Research: VSM and its underlying concepts
2. Annex 2: Literature Research: Web of Science search string results
3. Annex 3: Viable Security System Cross Reference Model
4. Annex 4: Transcribed interview with CIO of Company A (Dutch only)

Annex 1: Master thesis timeline

Date	Progress / Change	Actioned by
15/03/2019	Master thesis proposal sent to Dr. Hans Mulder.	Kevin Bollengier
17/03/2019	Feedback received from Dr. Hans Mulder.	Dr. Hans Mulder
18/3/2019	Feedback received from Dr. Yuri Bobbert.	Dr. Yuri Bobbert
26/3/2019	Feedback problem statement	Dr. Yuri Bobbert
15/4/2019	Skype session problem statement	Dr Yuri Bobbert, Dr. Hans Mulder, Kevin Bollengier
22/4/2019	Update problem statement, added research on return on security investment, cybersecurity economics and viable systems.	Kevin Bollengier
20/5/2019	Feedback master thesis	Dr. Yuri Bobbert
10/6/2019	Additional content added for the chapter "Background" for the literature review.	Kevin Bollengier
12/6/2019	Additional content added on the design science approach handled during this thesis.	Kevin Bollengier
13/6/2019	Feedback on Design Science Research	Dr. Yuri Bobbert
14/6/2019	Feedback on Design Science Research with additional papers	Dr. Yuri Bobbert
16/6/2019	Feedback on Design Science Research with additional papers.	Dr. Hans Mulder
17/6/2019	Formal research proposal sent to promotors.	Kevin Bollengier
14/7/2019	Update on master thesis sent to promotors.	Kevin Bollengier
15/7/2019	Feedback on the research questions	Dr. Hans Mulder
15/7/2019	Feedback on the entire thesis so far.	Dr. Yuri Bobbert
16/7/2019	Feedback on thesis structure and cyber security in the literature review.	Dr. Yuri Bobbert
17/7/2019	Feedback on problem statement.	Dr. Yuri Bobbert
12/8/2019	Added content in the chapter "Backgound" specifically regarding the Viable System Model.	Kevin Bollengier

9/9/2019	Feedback moment.	Dr. Yuri Bobbert, Kevin Bollengier
9/9/2019	Latest version of Master thesis sent to Dr. Yuri Bobbert.	Kevin Bollengier
30/9/2019	Master thesis update sent to promotors. (Further additions on the VSM and how VSM can be applied on Business Information Security).	Kevin Bollengier
12/10/2019	Full thesis review.	Dr. Yuri Bobbert
25/10/2019	Feedback moment at Antwerp Management School.	Dr. Yuri Bobbert, Kevin Bollengier
28/10/2019	• Added a reference to the NIS Directive. • Added an example of increasing threat complexity under the problem definitions (IoT, Mirai botnets)	Kevin Bollengier
29/10/2019	• Added the conclusion that organizations need an adaptive process or strategy to cope with the changing threat complexity.	Kevin Bollengier
4/11/2019	• Added additional context to the problem surrounding the lack of IT security knowledge and capabilities.	Kevin Bollengier
9/11/2019	• Add more body to the literature review	Kevin Bollengier
21/11/2019	• Some minor refactoring in chapter 4.1.2	Kevin Bollengier
22/11/2019 – 30/12/2019	• Create prototype of artefact	Kevin Bollengier
01/01/2020 - …	• Refactoring of artefact into V2	Kevin Bollengier
3/03/2020	• Added Literature Research Method	Kevin Bollengier
15/03/2020	• Design science research: requirements definition	Kevin Bollengier
30/04/2020	• Finalized use-case and demonstration of artefact on ransomware case of an educational institution	Kevin Bollengier
02/05/2020	• Conclusion, Limitations & Future Research Opportunities	Kevin Bollengier
09/05/2020	Design applied to thesis	Kris Geluykens
21/05/2020	Added more research on silo-thinking within cybersecurity in the problem statement.	Kevin Bollengier
28/05/2020	Final comments by promotor resolved	Kevin Bollengier

04/06/2020	Interview and validation of recommendations with CIO of Company A	Kevin Bollengier
08/06/2020	Interview and expert opinion with Marcel de Haan on the model and framework application	Kevin Bollengier
09/06/2020	Added the interview transcription with CIO and summary of the interview with Marcel de Haan.	Kevin Bollengier
10/06/2020	Interview and validation of recommendations to an educational institution, hit by ransomware	Kevin Bollengier
11/06/2020	Transcribed interview with CISO of university added to the research project	Kevin Bollengier
12/06/2020	Final comments from promotor implemented	Kevin Bollengier

Annex 2: Literature Research: VSM and its underlying concepts

Author	Year	Title	Journal	Reference Type	Topic
Alqurashi, Ezzat; Wills, Gary; Gilbert, Lester	2013	A Viable System Model for Information Security Governance: Establishing a Baseline of the Current Information Security Operations System		Conference Proceedings	VSM
Aubin, Jean-Pierre; Bayen, Alexandre M; Saint-Pierre, Patrick	2011	Viability theory: new directions		Book	VSM
Beer, Stafford	1972	Brain of the firm: the managerial cybernetics of organization		Book	VSM
Beer, Stafford	1979	The Heart of Enterprise		Book	VSM
Beer, Stafford	1984	The viable system model: Its provenance, development, methodology and pathology	Journal of the operational research society	Journal Article	VSM
Beer, Stafford	1985	Diagnosing the system for organizations		Book	VSM
Beer, Stafford	1986	Recursions of Power	Power, autonomy, utopia	Book Section	VSM
Burgess, Nicola; Wake, Nicholas	2013	The applicability of the Viable Systems Model as a diagnostic for small to medium sized enterprises	International Journal of Productivity and Performa	Journal Article	VSM
Espejo, Raúl; Gill, Antonia	1997	The viable system model as a framework for understanding organizations	Phrontis Limited & SYNCHO Limited	Journal Article	VSM
Espejo, Raúl; Harnden, Roger	1989	The viable system model: interpretations and applications of Stafford Beer's VSM		Book	VSM
Espejo, Raúl; Reys, Alfonso	2011	Organizational systems: Managing complexity with the viable system model		Book	VSM
Gokhale, Girish Bhagwan; Banks, David A	2004	Organisational Information Security: A Viable System Perspective	AISM	Conference Proceedings	VSM
Hildbrand, Sandra; Bodhanya, Shamim	2015	Guidance on applying the viable system model	Kybernetes	Journal Article	VSM
Lenoard, Allenna	2009	The viable system model and its application to complex organizations	Systemic Practice and Action Research	Journal Article	VSM
Schwaninger, Markus	2006	Design for viable organizations: The diagnostic power of the viable system model	Kybernetes	Journal Article	VSM
Stephens, John; Haslett, Tim	2011	A set of conventions, a model: An application of Stafford Beer's viable systems model to the strategic planning process	Systemic Practice and Action Research	Journal Article	VSM
Van Caspel, F	2013	VSM as a Tool for Organizational Change: A Critical Examination		Generic	VSM
Yolles, Maurice	1999	Management systems: A viable approach		Book	VSM
Ashby, W Ross	1956	An introduction to cybernetics		Book	Cybernetics
Conant, Roger C; Ross Ashby, W	1970	Every good regulator of a system must be a model of that system	International Journal of Systems Science	Journal Article	Systems Thinking
Jackson, Michael C	2003	Systems thinking: Creative holism for managers		Book	Systems Thinking
Kast, Fremont E; Rosenzweig, James E	1972	General systems theory: applications for organization and management	Academy of Management Journal	Journal Article	Systems Thinking
Mingers, John; White, Leroy	2010	A review of the recent contribution of systems thinking to operational research	European Journal of Operational Research	Journal Article	Systems Thinking
Von Bertalanffy, Ludwig	1968	General System Theory		Journal Article	Systems Thinking
Wiener, Norbert	1948	Cybernetics or Control and Communication in the Animal and the Machine		Book	Cybernetics

Annex 3: Literature Research: Web of Science search string results

savedrecs_source.xlsx

Annex 3: Viable Security System Cross Reference Model

Viable%20Security%2
0System%20Cross%2(

Annex 4: Transcribed interview with CIO of Company A (Dutch only)

Kevin Bollengier	CIO Company A
Dus eigenlijk om het interview kort te kaderen, je hebt die keynote gezien bij Beltug. Wat ik dus eigenlijk gedaan heb is dat idee van die Viable Business security gaan uitwerken vertrekkend vanuit een soort academisch model die ik heb toegepast op informaticabeveiliging. Dit om security eigenlijk te gaan opdelen in 5 (6 met inbegrip van Audit & Compliance Monitoring) gebieden, namelijk Security Governance, Security Intelligence, Security Management, Audit & Compliance Monitoring, Security Orchestration en Security Operations. Dit omdat heel vaak mensen te kleinschalig naar security kijken, zoals naar een product, zonder hierbij stil te staan wat die implementatie precies betekend voor de algemene verbetering van de security van een bedrijf. Een voorbeeld komt uit die security vendor wereld, zoals in de wereld van anti-malware. Het hebben van een traditioneel antivirus is namelijk langer voldoende, er zijn nog verschillende zaken die er naast moeten geplaatst worden om beschermd te zijn tegen zeg maar een ransomware aanval. Dit is eigenlijk het voorbeeld die ik gebracht heb bij Beltug over de ransomware aanval bij een universiteit Dan is natuurlijk de vraag, hoe moet ik security op dat algemene niveau gaan implementeren om te zorgen dat een bedrijf zich kan weren tegen cybercriminaliteit. Met dat idee heb ik een mapping gemaakt tussen security frameworks en best-practices maar ook meer organisatorische frameworks zoals COBIT. COBIT kan helpen met het indelen van je bedrijf en IT, maar zal geen concreet security advies geven. COBIT zal bv. zeggen dat je aan endpoint security management moet doen, maar niet hoe je dit moet doen. Hiervoor kijken we naar frameworks zoals de CIS Controls die we gebruikt hebben in onze eerdere maturiteitsmeeting, en de ISO 27k standaard. Deze frameworks treden dan iets meer in detail over de implementatie van hoe je die security operations kan doen op dit gebied. Met dit prototype-artefact heb ik vervolgens een vergelijkbare oefening gedaan zoals onze Beltug maturiteitstest met een trafficlight	

model (0; 0,5 of 1) om te verifiëren of een control al dan niet geïmplementeerd is. Dan heb ik die percentages uitgerekend en gaan kijken waar de grootste gaps waren, en deze gaps heb ik naar jou doorgestuurd om deze nu even kort te valideren.	
	Nee, oke dit is goed. Anders moet je even je scherm delen?
Dus zo ziet het model er eigenlijk uit.	
	Ja dat heb ik gezien.
Dat zijn dan inderdaad die 3 frameworks die ik afgestemd heb op die 3 kennisgebieden van security zal ik maar zeggen. En zoals je kan zien heb ik bij elke individuele control een 0, een half of volledig punt toegekend naargelang dit al dan niet in voege is bij Company A. Het resultaat van deze oefening is een lijst met recommendations op deze 5 (6) gebieden. De eerste recommendation bij Security Governance is enfeite het implementeren van een information security management systeem. Dat we gaan werken naar security standaarden. Een van de grote zaken hieronder zijn de business continuity plannen, een formeel risk appetite vast leggen. Gaan uitdrukken welk risico op cyberveiliging het bedrijf bereid is te nemen. Zoals bv. bij een ransomware aanval. betaalt het bedrijf of niet, welk budget wordt er voorzien om de kosten van dergelijke cyberaanval te voorkomen.	
	Ik denk, om even op uw eerste vraag te antwoorden. Zo'n framework gebruiken om onze security te maturen. Op zich is dat niet slecht, da's uiteindelijk je rode draad die je moet hebben. Ja alles wat je zegt rond business continuity, dat is waar we op dit moment naar de markt kijken, want wat we vandaag liggen hebben is gewoon onvoldoende. Wat we voornamelijk hebben is business continuity in de operationele zin van het woord, hoe verkoop ik morgen nog filmtickets op een manuele manier. Maar we weten ook dat het business continuity plan die we hebben maatschappelijk heel moeilijk is om te blijven te verkopen. Vandaar dat we ook beslist hebben om daar een volgende stap in te nemen, en vind ik het ook niet slecht om

	de discussie al eens te doen, in het geval van een case. Wat gebeurt dan, kunnen we preventief bepaalde budgetten approven? Of welke bedragen zouden wij bereid zijn om te betalen in geval van een case? Dat we op z'n minst weten hoeveel we bereid zijn om te investeren in security of hoeveel betalen we aan hackers mocht dit ooit voorvallen. Ik denk dat er veel preventief kan gebeuren in plaats van reactief, op het moment van een 'hit' en je hebt deze discussies niet gehad dan ben je te laat. Wanneer je deze discussies op voorhand gehad hebt, dan heb je bij wijze van spreken nog een warme koffie naast u staan omdat je dan rustig kan blijven denken en iets meer tijd hebt. In de heat of battle is de vraag of je dan veel opties hebt op dat moment. In alle eerlijkheid moesten ze mij op de stoel gezet hebben voor een beslissing te maken bij die universiteit voor 250k euro te betalen, denk ik dat ik het meteen gedaan zou hebben. Maar misschien als ik er rustiger of genuanceerder had over kunnen nadenken had ik misschien een andere beslissing genomen. Dus ik denk dat de punten die je oplijst in dit eerste verhaal op zich wel goed zijn om er mee aan de slag te gaan, of dat we tenminste al de eerste stappen gezet hebben, of dat we wisten dat deze punten op de radar stonden. En laat ons ze nu maar uitwerken.
Om nu dat tweede puntje, security intelligence, dat gaat over dat je op het juiste moment intelligentie hebt waarop je meteen acties kan gaan ondernemen. Zoals bv. een continuity plan, dat je zo'n oefening doet met de CEO rond de tafel, een round the table simulatiespel speelt waarbij je gaat kijken hoe de mensen die rond de tafel zitten gaan reageren op bepaalde gebeurtenissen die zich voordoen. En dit kan gebruikt worden om even stil te staan om te kijken hoe mensen zouden reageren in een echte ransomware of dergelijke situatie. Zodat mensen bij zo'n gebeurtenis niet rond de tafel zitten en dan nog moeten gaan nadenken over de te nemen acties.	
	Nee da's waar, maar aan de andere kant, ik denk dat de eerste vraag is wie we rond de tafel moeten zetten, met welke rollen en verantwoordelijkheden, zo dat het duidelijk is dat iedereen die rond de tafel zit zijn rol

	duidelijk kent om zijn verantwoordelijkheden op te nemen. Als ik bij wijze van spreken enkel rond de tafel zit om notulen te nemen, dan moet ik daarbij niet nadenken, da's gewoon typen. Als ik kijk naar onze woordvoerder bijvoorbeeld, waarbij we kijken hoe we dergelijke situatie uit de pers kunnen houden, of hoe we dergelijk incident naar de pers moeten begeleiden, dan weet deze persoon op voorhand ook haar rol en kunnen we daar preventief wel bepaalde zaken in opvangen. Ook die security intelligence, ja hoe meer je natuurlijk weet, hoe meer je kan analyzen en hoe beter je een beslissing kan gaan nemen. Als dit ons meer intelligentie, impact gaat geven in de case in the time to solve of de time to recover, dan denk ik inderdaad om dat op die moment aan die tafel te hebben.
Eigenlijk wat dan met zo'n simulatie bedoeld wordt is dat men waarheidsgetrouw dergelijk incident naspeelt en kijkt hoe iedereen zijn rol en verantwoordelijkheden opneemt.	
	Ja dat zit in het plan die we hebben uitgestuurd, maar eerst moeten we naturlijk definiëren wie aan die tafel gaat zitten en dan moeten we het inderdaad gewoon iets doen. Want ik ben er van overtuigd, de eerste keer dat we door dit script of scenario zullen lopen dat dit niet perfect zal zijn. We zullen waarschijnlijk nog 10 opmerkingen of verbeterpunten hebben. Ik denk dat de tweede en derde keer zullen beter zijn. Ik hoop natuurlijk dat we dergelijk document nooit nodig zullen hebben, maar wanneer je het nodig hebt hoop ik natuurlijk dat het plan matuur genoeg is om het daarmee te doen.
Dan het tweede punt bij security intelligence is dat het persoon die in dienst is op de hoogte is van security skills. Dit in de ruime zin, zoals het herkennen van phishing mails maar ook bijvoorbeeld developers die security best practices kennen en weten van development. Want we zijn daar wel mee bezig, maar deze heb ik expliciet nog eens opgenomen omdat we naar die nieuwe website aan het kijken zijn, ook naar eventuele nieuwe technologie aan het kijken zijn en dat we daar ook kunnen kijken naar een soort training om het	

development team te ondersteunen in het veilig ontwikkelen in deze website.	
	Ja zeker en vast kan nooit geen kwaad.
Dan bij security management in het verlengde van het gebruik van die frameworks, heb ik ook het documenteren daarbij opgesomd. Daar zijn we in principe ook wel mee bezig, maar het is ook handig om de "papierwinkel" te hebben wat we allemaal hebben uitgebouwd van security measures zoals onze policies en hiermee ook te kijken hoe ver we staan bij het uitbouwen van het securityverhaal van Company A.	
	Ja, daar denk ik dat we slim moeten kijken, ik ben de eerste persoon die zal vragen om policies. Ik zal ook de eerste persoon zijn om te zeggen dat we moeten documenteren wat we gedaan hebben. We moeten vooral zien dat geen documenten creeëren om slechts enkel documenten te creeëren. Ik wil maar zeggen bijvoorbeeld, een asset management systeem op papier zetten is onbegonnen werk aangezien dit zodanig snel verandert. Ik wil maar zeggen bijvoorbeeld, net zoals een firewall config, of dat we die moeten documenteren. We moeten even kijken of het zich automatisch up to date houdt op dat moment. Daar ben ik sowieso een heel grote fan van. Maar sowieso een policy, je moet daartegen kunnen testen van wat je denkt dat die policy doet tegenover wat de policy in realiteit doet. Maar hiervoor kun je bijvoorbeeld bepaalde richtlijnen documenteren waardoor zodoende dat we hierop achteraf wel kunnen auditen zoals bv. tegenover een wachtwoordbeleid en dergelijke. De grootste uitdaging hierbij Kevin volgens mij is relatief oke denk ik, maar natuurlijk wat brengen we hiervan opnieuw terug naar onze end-users.
Nee dat klopt, maar dat is natuurlijk eerder naar een compliance standpunt toe, dat mocht er toch iets gebeuren, zoals een datalek en de autoriteit vraagt hoe de organisatie van security bij Company A in elkaar zit, dat hebben we natuurlijk ons gedocumenteerd information security management systeem gebaseerd op een bepaalde standaard. En dan kunnen we deze vertaalslag maken op ons te verdedigen wat we allemaal invoege hebben gebracht.	
	Ja dat klopt.

Dan opnieuw in het verlengde van het business continuity plan da's natuurlijk het documenteren van een actieplan en communicatielijnen. Hoewel van eenzelfde aard, dit ligt meer bij het management stuk dan bij definieren van die policies.	
	Ja klopt.
Dan als volgende denk ik wel een grote, is natuurlijk het managen van identities en logical access. Dat gaan echt over het identity en access management verhaal. Hierbij zouden we een nieuwe tool of applicatie gebruiken zodat dit op een automatische manier kan gebeuren.	
	Ja, ik denk vooral dat, daar moeten we zeker nog op investeren. Ook zeker op dat offline verhaal. Mochten we zowel offline als online die identies kunnen koppelen dat zou zeker een meerwaarde kunnen zijn.
Dan ook segregation, hierop zijn we ook reeds aan het werken. Da's het segmenteren van responsibilities. Een voorbeeld hier kan zijn het splitsen van ons domein voor sales, voor hq en dergelijke. Maar ook kijken naar hoe we netwerken enzo kunnen opdelen.	
	Ja. Da's waar, dat kan zeker en vast.
Dan audit & compliance monitoring. Dat gaat dan eerder naar het auditen en zorgen dat de security loopt zoals het hoort volgens de opgelegde plannen, policies enzovoorts. Daarop kwam die network monitoring naarboven en het verzamelen van network data. Dit ligt dan in het verlengde van onze recente implementatie van ons EDR systeem waarop we natuurlijk reeds heel wat data hebben van onze endpoints. Maar het zou interessant kunnen zijn om deze te correleren aan onze events en data van ons network an sich. Dus op switches, firewalls heen enzo.	
	Gaat uw SIEM daar geen rol inspelen?
Ja dat klopt. Da's een onderdeel van deze audit & compliance monitoring tak.	
	Ik wil maar zeggen, als we de logs van network, firewalls en ATP verzamelen. Dan hebben we toch drie milestones om iets met deze data te doen, nee?

Ja zeker en vast, da's ook de reden dat dit punt als een van de belangrijkste naar boven-kwam.	
Ik denk ook dat volgend punt, die incident scenarios, belangrijk zijn aangezien we dat opgenomen hebben met de partners voor een voorstel te ontvangen. Of business continuity plannen gaan testen aan de hand van die red of purple teaming. Dus eigenlijk echt iemand die zonder enige aankondiging probeert binnen te geraken bij Company A. En ziet hoe ver hij kan geraken en natuurlijk hoe onze incident management en business continuity daarop gaat reageren.	
	Ik ben eens nieuwsgierig. Alé, ik wil maar zeggen ja, we zijn er naar aan het kijken, ik denk misschien dat we dat dieper en meer moeten doen. We hebben dat in het verleden ook wel al es gedaan. Ik denk dat deze oefening iets breder zal gaan. Maar ik ben vooral eens benieuwd wat er gaat uitkomen in alle eerlijkheid. En inderdaad hebben we het gezien, hebben we het niet gezien. Hebben onze monitoring systemen het gealarmeerd of niet dus ja. Ik ben curieus.
En dan heb ik daar als verlengde ook de data recovery plans bijgezet. Ook omdat we net het ganse backup verhaal klaargezet. Het is op zich nooit geen slecht plan om eens zo'n test te doen. Stel dat er toch iets zou gebeuren, met een ransomware aanval, of er gaat data verloren, hoe snel en in welke mate zijn we in staat tot het terugzetten van een laatste status van onze data?	
	Ja, moeten we zeker testen. En vooral hier denk ik, wat testen we, testen we 1 op 1, 1 op alles. Da's natuurlijk een scope kwestie, maar ik denk dat we daar inderdaad beter in kunnen doen ja.
Dan het puntje security orchestration, da's eigenlijk security samen kan hangen (integreert) met operationele kant. Dus hoe onderling security tools met elkaar intrageren. Hoe ze data kunnen correleren, aan elkaar. Maar ook hoe ingebouwde security tools, zoals in het operating systeem de security kunnen gaan verbeteren. Dat gaat ook over configuraties bijvoorbeeld. Dus het aanzetten van bepaalde settings in je computer, die automatisch zorgen voor een sterker beveiligingsbeleid. Daar heb ik inderdaad het opzetten van regels voor allowed business support tools, applications en software opgenomen. Dit	

omdat op dit moment nog veel mensen eigen software kunnen gebruiken, waarop IT enfeite geen controle heeft. Dat we ook niet weten wie welke software aan het gebruiken is, wat die software precies doet, van waar die software ook komt. En in het verlengde hiervan het gebruik van standaard, veilige configuraties om uiteindelijk een volledige lockddown te doen van onze toestellen.	
	Tja, dat moeten we gewoon doen. Da's ook onze visie. We moeten daar enkel een goede snelheid in kunnen vinden. Ik denk met het her-imagen van heel wat toestellen, zoals de upgrade van Windows 7 naar Windows 10, hebben we heel wat sales toestellen al kunnen meenemen. Ik denk dat we nu vooral op de laptops moeten focussen. Dat zijn uiteindelijk ook de mensen die het meeste met die devices werken. En daar moeten we ook de juiste snelheid in kunnen vinden om alles dicht te zetten.
Ja klopt, en dan het laatste puntje van die security orchestration is het segmenteren van netwerken op basis van het security niveau die nodig is, zoals de kritische zaken in je netwerk zoals het projectienetwerk. Je wilt bijvoorbeeld niet dat tijdens een voorstelling van een film, daar iets gebeurd. Dus dat de aansturing van de projecteren in een apart netwerk gebeurd met een sterker beveiligingsbeleid dan bv. het office network, waar we ook onze back-up hebben en daar naar beveiliging toe, sneller kunnen terugschakelen naar een vorige status van data bv. En dat we ook een dedicated netwerk of toestel gaan gebruiken voor management van netwerken en computers. Daar bedoel ik mee dat we niet zomaar administratieve accounts toelaten op persoonlijke werkcomputers, omdat die credentials gecached kunnen worden in het geheugen van die computer.	
	Ja, ik denk dat we daar duidelijk hebben uitgeschreven wat we willen in alle eerlijkheid, met die segmentatie. Ik denk dat we die accounts aan het "dichtknijpen" zijn. Die dat we denken ofdat we weten, zijn we aan het verifiëren. Ook alle service accounts komen in aparte OU's te zitten, met aparte beschrijvingen. Ik bedoel, ik denk dat we op account niveau reeds heel hard aan het segmenteren zijn. En ook op networking niveau, zijn er wel al een paar ideeën hoe we dit nog beter kunnen doen. Want inderdaad het P&S netwerk en sales netwerk kunnen we

	gescheiden houden moesten we dat willen. Zeker een punt.
En dan is er nog een punt dat mensen niet meer met administratieve accounts kunnen inloggen maar bv. een speciale jumpserver voorzien wordt. En al het administratieve werk op een dedicated toestel gebeurt, zodat nooit een admin wachtwoord in een computer kan terechtkomen.	
	Ja, je hebt een punt. Maar first things first, segmentatie op zich uitvoeren is al een eerste stap. En dan orchestratie hoe je van het ene netwerk naar het andere gaat. Ja je hebt daar zeker een punt.
En voor het laatste, security operations. Ik denk dat we daar reeds heel sterk ingezet hebben met onder andere onze ATP tools, die we zowel op office en clients hebben opgezet. Maar bijvoorbeeld, het encrypteren van data op devices, omdat die verloren kunnen gaan. Maar ook het gebruiken van automatische scanning tools om toestellen op ons netwerk te gaan ontdekken.	
	Dat kan, we gaan meer en meer mobiel werken. Nu ik denk sowieso wel, dat onze core en high-confidential data moeilijker op laptops terecht zal terechtkomen. Klantenbestanden zoals onze lijst van de CRM tool, download je niet zomaar efkes op je laptop. Je download niet zomaar sales data op je laptop. Ik wil maar zeggen, de data die we geclasseerd hebben als high, zit op zich volgens mij wel oké. Langs de andere kant, alles wat betreft mobile devices, moeten we zeker nog doen. Want er zijn ook wel documenten die bepaalde waarde hebben voor een bedrijf, die we ook liever niet op straat liggen hebben in alle eerlijkheid. Dus ik denk dat we daar met de komst van OneDrive en dergelijke al veel gedaan hebben. Maar wat betreft het encrypteren van devices, daar kunnen we inderdaad nog veel verder ingaan dan we nu doen. Klopt.
Dusja en dat laatste punt, die scanning tools, gaat dan over het ontdekken van mogelijke rogue devices enzo. Dat we daar sneller gaan weten wat precies op ons netwerk zit.	
	Ja, da's een leuke. Da's het bos en de boswachter zeker? Of de stroper en de boswachter?

	Nee goed, wat is nu de volgende fase in dit project, of dit document?
Dus we zijn er al aan mee bezig, dus het was de bedoeling om te kijken of dit overeenstemt met de problemen of actiepunten bij Company A moeten gebeuren. Dan weet ik dat de antwoorden die uit deze Excel echt punten zijn die bruikbaar zijn voor Company A. Of toch punten zijn, waar de er toch enige aandacht voor nodig is. En dan kan ik met die validatie verder werken voor mijn onderzoek.	
	In alle eerlijkheid, er staan geen punten op die mij verrassen in alle eerlijkheid. De meeste punten die hier naar boven komen zijn dingen waarover we al gesproken hebben of, waar we een intentie tot het opstarten van een project voor hebben. Voor andere punten zijn er al zaken opgestart, zijn lopende. Dus dat zit wel goed denk ik. Dus voor mij kan je hier zeker mee verder werken.
En in een volgende fase, stel dat er toch ooit een doctoraat zou bijkomt. Dan is het de bedoeling dat deze Excel verder uitgebreidt wordt met extra model. Dat heet dan return on security investment. Omdat we dan eigenlijk al die actiepunten een waarde kunnen geven op effort versus impact. En daarmee een automatische roadmap laten ontwikkelen voor een bedrijf. Dus eigenlijk dat de acties voor het minste geld, tijd of spent maar met het hoogste resultaat voor de verbetering van beveiliging naar boven komen.	
	Ja, daar ben ik toch benieuwd naar hoe je dat gaat doen. Want da's een leuke discussie. Want naar effort en manpower internally, daar kan je heel snel schatten wat je kost is, of je kan assumpties maken hiervoor die dicht bij de realiteit zullen liggen. Ik denk het moment dat je de impact van dergelijke zaken moet gaan meten. Dat lijkt me toch een hele moeilijke, in de zin van, wat neem je mee in scope, wat neem je niet mee in scope. Onze business is heel fluctuerend. Een storing bijvoorbeeld, op een maandag of dinsdag, veel minder effect zullen hebben dan op een zaterdag of zondag. Ja, ik denk niet dat het onhaalbaar is om er een model achter te krijgen, of tenminste een model erachter te krijgen die een goede beeldvorming is van de realiteit waardoor je beslissingen beter kunt nemen. Ik bedoel, 300%. Vandaag hebben we dat niet. Ik denk dat we vandaag kijken naar investering van manpower en tijd,

	en dergelijke om juiste beslissingen te nemen. Ik denk dat we iets minder kijken naar business impact spelen omdat het minder gekwantificeerd is.
Nee dat klopt, het zou ook de bedoeling zijn om in de eerste fase, met kwalitatieve cijfers werken, zoals minnetjes en plusjes. Want het kwantificeren van die uitgaven is zeer moeilijk. En da's ook zeer eigen aan een bedrijf of sector. Maar om toch een hulpmiddel te bieden aan een bedrijf, zou dat een van de stappen zijn die we kunnen aanbieden om toch op een snelle manier een roadmap te maken met de meest impactvolle punten.	
	Nu, je ziet wel, dat de tools die we gebruiken, ook die richting aan het uitgaan zijn. Als je ziet welke recommendations er nu reeds uit onze ATP komen bijvoorbeeld. Ik weet ook niet hoe een Microsoft met zijn producten zal blijven evolueren, maar je voelt dat ook wel. Ook naar patchings toe, staan er scores naast. Ik denk dat dat op een iets hoger niveau met een Sentinel ook wel kan om uit te wijzen waar we naar moeten kijken. Dusja op zich kan het wel.
Ja en dat zou dit document proberen toepassen op een gans bedrijf met zijn security. Dat zal nooit gaan op een niveau van je moet dit bedrag investen en je zult zoveel veiliger zijn. Het gaat hem echt over, welke zaken kunnen we doen, met interne manpower of met budgetten om te zorgen dat de security score van deze 6 punten stijgend evolueert.	
	Het is ook een living system, de markt staat niet stil, het bedrijf staat niet stil, er komen nieuwe mensen bij. Da's een constant levend gebeuren. Je moet niet constant uw policies aanpassen, maar je ziet wel, dat de bedreiging van 2 of 3 jaar geleden, helemaal anders is dan de situatie waarin we ons vandaag bevinden. Dus het is echt een levend verhaal, we hebben een 32-punten plan tegen ransomware. Ondertussen zullen dat er wel al 42 zijn, omdat we telkens als we een punt aftikken, we weer iets nieuws ontdekken om te verbeteren. Da's ook hoe we er moeten naar kijken. Maar ik denk wel, you'll never be done with security. We moeten constant blijven investeren, maar de vraag is natuurlijk, en da's waarmee iedereen zich bezig houdt, da's op welk tempo en met welke middelen blijf je als bedrijf vooruitgang boeken. Dusja als we de komende 5 jaar niets voorhebben van incident zal ik zeer blij zijn,

	dat betekent dan voor mij dat we het goed gedaan hebben. Maar voor hetzelfde geld wordt je 2 keer 'gehit' op eenzelfde jaar. You never know. Het staat niet in de sterren geschreven. Ik denk dat gewoon moeten identificeren en dergelijke frameworks en documenten helpen ons, om de juiste areas of attention te identificeren. En ik denk dat het dan aan ons is om de juiste punten bespreekbaar te maken binnen onze organisatie en daarvoor de juiste middelen vrij te maken. Ik denk dat we de laatste jaren genoeg hebben geïnvesteerd in security, of voldoende. Maar de vraag is, was het genoeg, en dat weet je natuurlijk nooit. Heden heb ik gelijk gekregen, maar misschien dat ik morgen ongelijk krijg. Maar de manier waarop we ermee bezig zijn. Ik denk alles is bespreekbaar. Ik bedoel we laten ons nu opnieuw begeleiden met een externe partner om dergelijke modellen en om deze domeinen meters te maken. En zelfs opnieuw, met die red, blue of purple teaming ben ik opnieuw benieuwd. Wat komt daaruit? Daar gaan opnieuw inzichten uitkomen die we wel of niet op onze radar hadden.
Ja nee klopt, dan zou ik je alvast willen bedanken voor efkes dit te valideren en voor je extra input. Dan kan ik nu aan de slag gaan om hiermee aan de slag te gaan. En dan hoop ik dat we binnen het jaar samen hiervan nog enkele punten kunnen van afwerken.	
	Dat hoop ik ook in alle eerlijkheid.

List of figures

List of tables

Bibliography

Alqurashi, E., Wills, G., & Gilbert, L. (2013). *A Viable System Model for Information Security Governance: Establishing a Baseline of the Current Information Security Operations System*, Berlin, Heidelberg.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300): Springer.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Kallitsis, M. (2017). *Understanding the mirai botnet.* Paper presented at the 26th {USENIX} Security Symposium ({USENIX} Security 17).

Ashby, W. R. (1956). An introduction to cybernetics.

Beer, S. (1972). *Brain of the firm: the managerial cybernetics of organization*: Wiley.

Beer, S. (1979). *The heart of enterprise* (Vol. 2): Wiley Chichester.

Beer, S. (1984). The viable system model: Its provenance, development, methodology and pathology. *Journal of the operational research society, 35*(1), 7-25.

Beer, S. (1985). *Diagnosing the system for organizations*: John Wiley & Sons Inc.

Beer, S. (1986). Recursions of Power. In *Power, autonomy, utopia* (pp. 3-17): Springer.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue, 44*(2), 147-164.

Bobbert, Y. (2017). On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering. *International Journal of IT/Business Alignment and Governance (IJITBAG), 8*(2), 28-41.

Bobbert, Y. (2018). *Improving the maturity of business information security.* University of Antwerp,

Bobbert, Y., & Mulder, H. (2010). A research journey into maturing the business information security of mid market organizations. *International Journal of IT/Business Alignment and Governance (IJITBAG), 1*(4), 18-39.

Bollengier, K. (2018). *Wat is de impact van de GDPR op de IT-processen van een internationale onderneming?* (Bachelor in Applied Computer Sciences - Computer & Cybercrime Professional Bachelor Thesis), Hogeschool West-Vlaanderen, Vlaamse Scriptiebank. Retrieved from https://www.scriptiebank.be/sites/default/files/thesis/2018-07/BachelorProef_Kevin_Bollengier_Final.pdf

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management. *IT Professional, 18*(2), 22-30.

Conant, R. C., & Ross Ashby, W. (1970). Every good regulator of a system must be a model of that system. *International journal of systems science, 1*(2), 89-97.

De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of IT. In *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5* (pp. 11-43). Cham: Springer International Publishing.

Disparte, D., & Furlow, C. (2017). The best cybersecurity investment you can make is better training. *Harvard Business Review*, 2-4.

ENISA. (2019). *ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends*. European Union.

Espejo, R., & Gill, A. (1997). The viable system model as a framework for understanding organizations. *Phrontis Limited & SYNCHO Limited*.

Espejo, R., & Harnden, R. (1989). *The viable system model: interpretations and applications of Stafford Beer's VSM*: Wiley.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (2016a).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016/679 C.F.R. (2016b).

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & security, 43*, 90-110.
FOX-IT. (2020). *Reactie Universiteit Maastricht op rapport FOX-IT*. Retrieved from Maastricht:
Gandhi, G. (2014). *Complexity theory in Cyber Security*. Article. The University of Warwick. Researchgate. Retrieved from https://www.researchgate.net/publication/263652176_Complexity_theory_in_Cyber_Security
Gokhale, G. B., & Banks, D. A. (2004). *Organisational Information Security: A Viable System Perspective.* Paper presented at the AISM.
Goldes, S., Schneider, R., Schweda, C. M., & Zamani, J. (2017). *Building a viable information security management system.* Paper presented at the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF).
Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457.
Hahn, A., Thomas, R. K., Lozano, I., & Cardenas, A. (2015). A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection, 11*, 39-50.
Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems, 19*(2), 4.
Hildbrand, S., & Bodhanya, S. (2015). Guidance on applying the viable system model. *Kybernetes, 44*(2), 186-201.
Holland, J. H. (2006). Studying complex adaptive systems. *Journal of systems science and complexity, 19*(1), 1-8.
Huygh, T. (2019). *Investigating IT Governance through the Viable System Model.* (Doctor of Philosophy Doctoral dissertation), University of Antwerp,
Huygh, T., & De Haes, S. (2019). Investigating IT Governance through the Viable System Model. *Information systems management, 36*(2), 168-192.
International Organization for Standardization, I. E. C. (2013). Information technology – Security techniques – Code of practice for information security controls. In *ISO/IEC 27002*: International Organization for Standardization, International Electrotechnical Commission.
International Organization for Standardization, I. E. C. (2014). Information technology — Security techniques — Information security management systems — Overview and vocabulary. In *ISO/IEC 27000*: International Organization for Standardization, International Electrotechnical Commission.
Isaca. (2019). *CISA Review Manual, 27th Edition*: Information Systems Audit and Control Association.
Ivanuša, T., Mulej, M., Podbregar, I., & Rosi, B. (2015). Requisite Holism of Behavior When Facing Complexity of Pandemic Diseases–New Trends in Healthcare Information System (HIS). *Series Title: Social Responsibility Beyond Neoliberalism and Charity*, 105.
Jackson, M. C. (2003). *Systems thinking: Creative holism for managers*: Wiley Chichester.
Johannesson, P., & Perjons, E. (2014). *An introduction to design science*: Springer.
Kast, F. E., & Rosenzweig, J. E. (1972). General systems theory: Applications for organization and management. *Academy of management journal, 15*(4), 447-465.
Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.
Leonard, A. (2009). The viable system model and its application to complex organizations. *Systemic Practice and Action Research, 22*(4), 223-233.
Li, C., Romagnani, P., von Brunn, A., & Anders, H.-J. (2020). SARS-CoV-2 and Europe: timing of containment measures for outbreak control. *Infection*, 1.
McFarlane, F. W. (1984). *Information technology changes the way you compete*: Harvard Business Review, Reprint Service.
Mercuri, R. T. (2003). Analyzing security costs. *Communications of the ACM, 46*(6), 15-18.
Mihai, I.-C., Pruna, S., & Barbu, I.-D. (2014). Cyber kill chain analysis. *Int'l J. Info. Sec. & Cybercrime, 3*, 37.

Miller, K. L. (2016). What We Talk About When We Talk About "Reasonable Cybersecurity": A Proactive and Adaptive Approach. *FLA. BJ*, *90*, 23, 23.
Minchev, Z. (2016). Cyber Threats Identification in the Evolving Digital Reality.
Mingers, J., & White, L. (2010). A review of the recent contribution of systems thinking to operational research and management science. *European journal of operational research*, *207*(3), 1147-1161.
Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2015). *A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT).* Paper presented at the 2015 Internet Technologies and Applications (ITA).
Recker, J. (2012). *Scientific research in information systems: a beginner's guide*: Springer Science & Business Media.
Rodewald, G. (2005). *Aligning information security investments with a firm's risk tolerance.* Paper presented at the Proceedings of the 2nd annual conference on Information security curriculum development.
Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & security*, *65*, 77-89.
Ruighaver, A. (2004). *Developing a framework for understanding Security Governance*. Paper presented at the 2nd Australian Information Security Management Conference.
Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.
Schwaninger, M. (2006). Design for viable organizations: The diagnostic power of the viable system model. *Kybernetes*, *35*(7/8), 955-966.
Sohrabi, C., Alsafi, Z., O'Neill, N., Khan, M., Kerwan, A., Al-Jabir, A., . . . Agha, R. (2020). World Health Organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19). *International Journal of Surgery*.
Solms, S., & Solms, R. Information Security Governance.
Solms, S., & Solms, R. (2008). *Information security governance*: Springer Science & Business Media.
Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), 45.
Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.
Stephens, J., & Haslett, T. (2011). A set of conventions, a model: An application of Stafford Beer's viable systems model to the strategic planning process. *Systemic Practice and Action Research*, *24*(5), 429-452.
Tobías, A. (2020). Evaluation of the lockdowns for the SARS-CoV-2 epidemic in Italy and Spain after one month follow up. *Science of The Total Environment*, 138539.
Van Caspel, F. (2013). VSM as a Tool for Organizational Change: A Critical Examination. In: Retrieved July.
Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, *29*(4), 476-486.
Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information systems management*, *24*(4), 361-372.
Von Bertalanffy, L. (1968). General system theory. *New York, 41973*(1968), 40.
Von Solms, B. (2006). Information security–the fourth wave. *Computers & security*, *25*(3), 165-168.
Von Solms, B., & Von Solms, R. (2005). From information security to… business security? *Computers & security*, *24*(4), 271-273.
Von Solms, R. (1998). Information security management (1): why information security is so important. *Information Management & Computer Security*, *6*(4), 174-177.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102.
Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*: Cengage Learning.
Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine*: Technology Press.

Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*: Springer.
Williams, P. (2001). Information security governance. *Information security technical report, 6*(3), 60-70.
Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Business Systems, Governance & Ethics, 9*(2), 50-65.
Yolles, M. (1999). *Management systems: A viable approach*: Financial Times Pitman Publishing London.
Zhao, K., & Ge, L. (2013). *A survey on the internet of things security.* Paper presented at the 2013 Ninth international conference on computational intelligence and security.