Aalto University
School of Business

Information Security Attributes & Securing Organizations

A literature review

Bachelor's Thesis
Antti Määttänen
Aalto University School of Business
Information and Service Management
Summer 2020

Aalto University
School of Business

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi

Abstract of Bachelor's thesis

Author Antti Määttänen

Title of thesis Information Security Attributes & Securing Organizations

Degree Bachelor's degree

Degree programme Information and Service Management

Thesis advisor(s) Liu Yong

Year of approval 2020 **Number of pages** 28 **Language** English

Abstract

Information systems are evolving with rapid pace and it is easier and cheaper for organizations to acquire more systems and digitalize their business. Because of this, Information Security (InfoSec) is increasingly required in organizations. When there are more interconnected systems, databases and applications often accessible online, this leads to more attack vectors and possible security incidents. Incidents can be chained, leading from smaller initial incident into more critical ones, which could be avoided if the first incident did not occur, underlining the need for securing all assets. Regulators are also demanding security under penalty of fines as incentive to secure organizations.

Security researches have continued to propose InfoSec attributes, which are elements of assets that need to be secured. Understanding these attributes helps organizations establish Information Security Management Systems, which are policies and guidelines for mitigating risks. These risks vary from malicious employees to natural disasters, and from espionage to cyber terrorism. Attacks towards humans in organizations are increasing, such as phising or impersonating another employee. Without proper tools and processes, organizations are not even able to tell whether they have had security incidents or not.

With Information Security Management System it is possible to plan, implement, monitor and adjust security policies and controls. This system helps organizations to have comprehensive information security, including details of what security controls are being applied for each asset, how to monitor and detect incidents, and how to recover from them.

Keywords Information Security Attributes, Risk management, InfoSec, ISMS

Table of Contents

List of Figures

List of Tables

1 Introduction

The number of cyber security breaches are increasing and gaining variety. According to a study by Statista, 49% of respondent organizations faced cyber security breaches or attacks once a month or more often (Statista, 2020). This figure was a bit lower on large businesses in 2017 (42%). However, these numbers show that securing information systems, operations and resources are necessary. Information Security will be referred to as InfoSec in this paper, as it is used in the industry, mentioned often here, and IS refers to Information Systems.

InfoSec is defined in ISO 27002 as "preservation of the confidentiality, integrity and availability of information" (ISO/IEC, 2013). Whitman and Mattord (2011) have a broader definition as "the protection of information and its critical elements, including the systems and hardware that use, store and transmit information". Arguably, InfoSec has more elements than confidentiality, integrity and availability, and other elements do vary from organization to organization, thus limiting it to the three attributes is narrow minded.

Nowadays Cyber Security is more commonly used in media than InfoSec. Cyber Security is a subset of InfoSec, consisting only of digital elements within InfoSec. However, security attributes do overlap and more recent goals have been established because of cyber security. If cyber security was stripped away from InfoSec, physical properties, information on paper, hardware, closed networks such as intranets and offline machines would remain. It would not be comprehensive to consider only cyber security within organizations, because digital elements do run on physical hardware, although most attacks come online.

Scientific research combining InfoSec attributes, security planning and implementation, and statistics of InfoSec incidents do not seem to exist, which is what I want to study. Scientific research seems to focus only on one or two of these areas in depth. However, as InfoSec is a wide and unambiguous topic consisting of multiple areas, a study grasping multiple aspects is needed to gain insight from aforementioned topics. Similar studies are conducted by consultancies helping customer organizations plan and implement InfoSec practices according to their own frameworks or established models, but these tend to focus on threats and incidents over the attributes InfoSec consists of.

Intended attacks or unintended security incidents in Information Systems (IS) are harmful in multiple ways. Operations can face complications or downtimes. Organization's assets' security, including physical, digital and human resources could be compromised, causing possible problems in the future. These can all result in revenue or reputation loss, intellectual property theft, unauthorized modifications on data, denial of service, reputation decrease or legal penalties (Schultz et al., 2001).

InfoSec is easily neglected in organizations for multiple reasons, if there are no external reasons to focus on it. Having organizational IS in cloud moves the burden of securing systems to cloud service provider, but organizations still need security policies, as having services in cloud does not provide immunity. It is also easy to think that an organization does not hold anything that is valuable which would interest adversaries, such as credit card details, customer details, intellectual property or similar. Poor security can still halt operations within organizations, if IS gets infected by autonomously spreading ransomware seeking for vulnerable systems online, which you can get rid of by paying to adversary. Knowing the value of organizational assets and resources, and what security issues they might face is the key to establishing security policies and practices to decrease the harms of being a target.

InfoSec might also be driven by external requirements, such as legislation, regulation or stakeholders. Organizations which have consumer data need to comply with General Data Protection Regulation (GDPR). Organizations accepting payment cards as a payment method have their own standard called Payment Card Industry Data Security Standard (PCI DSS). Many countries have their own regulations and legislations as well, such as Finnish requirements about medical devices and equipment (FINLEX, 2010). Multiple standards might require to be applied, and contents of these requirements do vary over time, but so do organizations' systems, processes and operations. Because of this, InfoSec should be continuously inspected, planned, implemented and monitored (Disterer, 2013).

InfoSec is a combination of people, processes and technology. It is something that needs to be considered horizontally through organization, and not only by IT department, as InfoSec consists of everyone's work. Thus, the scope of InfoSec includes people, processes, products, systems and devices, plants, networks, technologies and information. It used to be a strictly technical issue, however, evolvement of computers and networks has extended InfoSec beyond technology (Von Solms and Van Niekerk, 2013).

1.1 Research objectives and research questions

This paper will focus on two research questions:

- Q1: What are the attributes of Information Security, and
- Q2: What are the strategies and challenges for organizations to achieve the information security goals?

The first research question aims to define what are the attributes of InfoSec. The attributes relate to all organizational IS's, resources, processes and assets, and all of these should be secured. It aims to answer what are the things we are trying to maintain. The second question then answers how organizations can keep their IS's secured. It requires policies, management, mindset and education for the whole personnel to mitigate risks properly. Organizational IS is contemporarily very complex, including increasing number of devices and subsystems, some of which might be managed centrally such as workstations, but also unmanaged devices or services such as smartphones or personal file cloud services.

1.2 Scope of research

This paper will cover past research on InfoSec attributes and goals and models which establish these. Some of the attributes might be backed up by information from recent news, but everything will be cited up from academic research or whitepapers. Some attributes will be backed up by references before the 20th century as these have been long established and well-studied then, but other attributes have been proposed more recently.

I will also be looking into InfoSec strategies and how these are established. I'll be using ISO / IEC 27000 -series Information Security Management System (ISMS) as base of it. However, covering the ISMS's comprehensively is not possible, as it is not available for free and its depth goes beyond this thesis to the level of technical implementation. I have to rely on others research and case studies about it. This paper focuses mainly on managemental aspect of implementing ISMS and slightly covering what ISO / IEC 27000 covers, not going into too much of the technical details.

1.3 Methodology

The research was conducted by using Scopus and Google Scholar, preferring Scopus. In Scopus searches were conducted using the topic searched for combined with different variations of "Information Security" as the keyword found from title, abstract or keywords. Search results were limited to area of Computer Science and Business. From the results most cited and most relevant results were used. For example, if the search was conducted for attribute confidentiality, the search query was then the following:

TITLE-ABS-KEY ((information AND sec*) OR (infosec) OR (is)) AND (confidentiality) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "BUSI"))

There were some variations to this. When going deeper into the attributes, such as access control, it is redundant to state InfoSec in the query, as access control always relates to security. In these cases the link to InfoSec was already been established in other studies, stating that access control should be used to implement security.

Chapter 2.2 of "How can organizations establish Information Security?" was studied by searching InfoSec management systems, risk assessment methods, standards and legislation, as well as case studies of implemented InfoSec policies. Statistics of costs of security incidents, sources of incidents and different type of incidents covered in chapter 2.2.3 were obtained from Statista. If the statistics was not created by Statista, I used the original source as my reference after checking the sources.

1.4 Structure of the research

The rest of the thesis is structured as follows. Chapter 2 reviews results from literature review. Section 2.1 covers InfoSec attributes theoretically using examples where required. This section is followed by 2.2. which represents how organizations can establish InfoSec policies and what these are. The attributes stated in 2.1 should be kept in mind when thinking about creating a security policy, as these are the objectives of secure systems. However, the section covers different aspects to be secured according to ISO 27001 standard, and it is covered from managemental perspective rather than technical. Subsection 2.2.3 covers statistics about the type and frequency of InfoSec incidents, giving overview of what incidents organizations are really facing, underlining the importance of InfoSec. Chapter 3 presents discussion about the findings, and how these findings contribute to scientific research and managerial practice.

2 Results

In this chapter InfoSec attributes will be covered first. All organizational IS', assets can have these attributes, but how important these are do vary for each asset and organization. Knowing the different attributes helps to identify their importance and risks related to assets, which are used in processes and operations. If assets attributes are compromised, then the processes and operations relying on them might have a negative impact, assets might get misused or information might end up for unauthorized parties.

After defining InfoSec attributes ISMS's will be covered. These are guidelines and policies which should be enforced and followed to have InfoSec in place (Susanto, Almunawar and Tuan, 2011). Theory of risk is also included, which aids financial decisions regarding security controls. Finally, some statistics regarding InfoSec incidents will be presented, such shares of different type of InfoSec incidents, their costs and frequencies.

2.1 Information Security attributes

Well established goals of InfoSec are confidentiality, integrity and availability. These attributes are also known as the "CIA-triad" or "Security Golden Triangle". These attributes have existed in military operations for thousands of years, and have been attributes of IS for its whole lifetime. Researchers have proposed new models and attributes with more or similar attributes as the CIA-triad is a bit outdated with respect to the contemporary information systems, but the model is still widely used as a base in theory and practice.

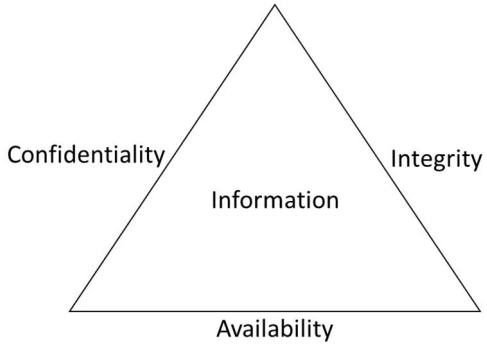

Figure 1. Classical CIA-triad (Qadir and Quadri, 2016, p. 186)

The CIA-triad assumes that Information balances between the three attributes. If one would like to increase confidentiality of information by requiring stronger authentication and encryption of the data, its availability lowers as the information becomes harder to reach, and integrity suffers if subset of the data is encrypted in a way that less people can access it. However, the balancing between the attributes has changed in 21st century, as with modern technologies it is possible to excel all the attributes at the same time.

A very well-reasoned alteration to the original CIA-triad is proposed by Qadir & Quadri (2016). As confidentiality and integrity cannot be achieved without availability, since these attributes do not exist if there is no availability to information, they made availability as the base of whole InfoSec. This extends to other attributes as well, although they didn't state that.

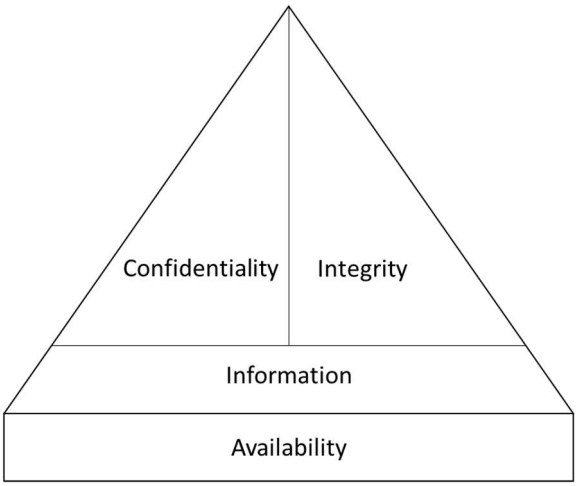

Figure 2. Alteration to CIA-triad proposed by Qadir & Quadri (2016, p. 186)

The exact origin of the "CIA triad" appears to be unknown. That is because the concepts have been existed in military context thousands of years ago, and appliance of these can be seen in the Roman empire 2000 years ago. Example of this would be Julius Caesar using Rot13, in which characters of information are all replaced with the 13th letter in alphabets following the one being replaced, making information unreadable without deciphering it increasing its confidentiality and integrity.

There are some variations of this. Parkerian Hexad (Parker, 1998) introduces Possession or Control, Authenticity and Utility besides the attributes in the CIA-triad (Qadir and Quadri, 2016). Schultz et al. also raises usability as one of key elements, as usability tends to lead to trade-off with security (2001).

Although all of the security goals should be embraced on some level, some industries do focus more on some attributes than others, mainly because of legislation, but also because their business and operations require so. For example, handling and storing medical patient information in the healthcare sector requires high confidentiality. The industry has generally strict guidelines set by governments for the systems, and sanctions if these are not on place (FINLEX, 2010; Stahl, Doherty and Shaw, 2012).

2.1.1 Confidentiality

Confidentiality is defined as "property that information is not made available or disclosed to unauthorized individuals, entities, or processes" (ISO/IEC 27000, 2018). In other words, only authorized users should be able to access information and systems they are permitted to. Compromise of information is referred as a breach. A breach is particularly harmful as once it has happened and information has been gained by unauthorized parties, there are no ways of undoing it.

Confidentiality requires authentication and authorization. Authentication can be done with usernames and passwords, keys and key cards, biometric mechanisms, or shared secrets used between machines. It can also be attribute based, such as user's location or device they are using. Authorization means further granting or forbidding access to information or systems. Without authentication authorization is not possible. Multiple authentication methods can be used and it is referred as Multi-Factor Authentication, as this mitigates with drawbacks of using only a single authentication method further increasing security (He and Wang, 2015).

Confidentiality can be increased through encryption. Encryption means that data is processed through an algorithm with a secret key to a format, which needs to be

decrypted to be used. Encrypted data is obfuscated and unusable by humans or machines without decrypting it with the same secret key. If origin and target of the information both have the secret key, it is not possible for others to read the information.

2.1.1.1 Authorization and Access Control

Authorization can be done with Access Control (AC). AC's can be divided into Role-Based Access Control, Attribute-Based Access Control, Discretionary Access Control and Mandatory Access Control. In AC's the user or system is a subject, and information, system or resources they are trying to access are objects. The difference between the models are in how is subject's access to objects are gained or granted, who is able to decide it and the flow of information. Multiple access control models can exist within one organization, depending on the need.

In Discretionary Access Control (DAC) the owner of the object has full control over the object. This is similar to UNIX or Windows File Systems. They are able to grant permissions to objects and restrict those, such as giving read permission to every subject, but write permission to only administrators. DAC is the most common access control model in general PC's, although confidentiality can be easily lost if the owner of the object makes mistakes.

Rather than each owner of objects granting other subjects access rights, Role-Based Access Control (RBAC) simplifies the process by enabling access control per objects roles. Roles are crafted per teams, units or tasks within organization, and the access to objects is then gained by adding objects to roles. In organizational context, subject will not get direct access right to every relevant object – they only get the roles intended for them, and the role permits them access to the objects. According to a study, RBAC's adoption is increasing in commercial organizations (Loomis and O'Connor, 2010).

Attribute-Based Access Control (ABAC) grants subjects' access to objects per attributes. These can be subject's location, time of the day, the network the subject is accessing from, or device. ABAC is more dynamic than RBAC, but it is more complex to maintain (Rajpoot, Jensen and Krishnan, 2015).

In Mandatory Access Controls (MAC) central administration grants classifications (access control levels) to subjects and objects, such as public information, restricted, confidential or top secret. The most used model is Bell-LaPadula Model (Pavlich-Mariscal, Demurjian and Michel, 2010). Another well-known MAC model is Biba Model (Zhang, Hong and Xiao, 2006). Both of these have split access to read and write

information. Their goal is to restrict the flow of information from down to up, or from up to down (Pavlich-Mariscal, Demurjian and Michel, 2010). These are generally used in governmental organizations, and have little use in commercial organizations.

In Bell-LaPadula Model, developed in 1976, an individual can only read information which is less or equal than the individual's access control level, but the individual can only write information to levels which is more or equal than the individual's access control level. Bell-LaPadula model is characterized by the phrase "write up, read down" (Jiang et al., 2004), and its main goal is confidentiality. It is implemented in military organizations.

Opposite to the Bell-LaPadula Model is Biba Model, developed in 1977. In the model the user can only read information classified higher or equal as user's access level, and write information to levels lower or equal than user's access level. Thus, it is called "read up, write down" (Zhang, Hong and Xiao, 2006). The main goal of the Biba model is to maintain strict information integrity, as when users are able to read highest level classified information, their writings to lower levels would be more homogenous than in Bell-LaPadula Model.

2.1.2 Integrity

Integrity means "property of accuracy and completeness" of the information (ISO/IEC 27000, 2018). Additional definition also exists, stating that "Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware" (Zissis and Lekkas, 2012, p. 586). This also results in unauthorized parties cannot delete, modify or even read data if restricted from public access. AC is key to ensure integrity, which is covered under confidentiality. Biba Model was designed for high integrity, as everyone are able to read data higher than their own classification. By using AC, organizations can achieve greater confidentiality and integrity in their systems.

Auditing operations performed on data helps organizations visibility on who or what altered their data, how it was altered and when. Altering the data may sometimes happen on user error, and auditing helps to fix those errors too. Besides auditing, backups should be taken of valuable data. If data gets altered, lost or corrupted, restoring backups help to reverse the situation, although newest data is usually lost (Wang et al., 2011).

Information is usually not used or modified directly, it is done through software. Software integrity is similar to regular information integrity, but it aims to protect

software from unauthorized deletion, modification, theft or fabrication. These can be intentional or unintentional. In cloud computing, Application Programming Interfaces (API) is often implemented, which might have additional logic to restrict operations based on rules, such as restricting deletion of orders which are not yet billed, or deleting too many records per day (Wang et al., 2011). Similar logic can be applied to desktop software.

Another way to increase integrity through software integrity is to implement encryption. As stated in confidentiality, encryption means that data is processed to a format, which needs to be decrypted to be used. When encryption and decryption lay within software, even authorized users are not able to modify the information without knowing the encryption protocol and secret key used to encrypt the information, requiring all modifications to the information to be done through software. Encryption can also be implemented in shared storages or personal computers, so that unauthorized users cannot use the information without breaking the encryption.

To know if information was altered after the origin of information published it, checksums can be used. They are algorithms used on information to get a code called checksum. When publisher of information releases the information, they can also give checksum of the information. Then receiver of the information runs the same algorithm to see if the checksums match. If the data has been altered in any way, checksum would not match, meaning integrity has been lost (Cohen, 1987). These can be done manually, or implemented via software.

2.1.3 Availability

The definition of Availability is diverse in Computer Science, Information Technology and Applications. It is mostly inspected in the context of performance and functionality of applications and services, hardware and networks. ISO defines Availability as “Property of being accessible and usable upon demand by an authorized entity” (ISO/IEC 27000, 2018)

Availability can also decrease without adversaries. A failure is expected variance, usually visible to the user, for example through an error message, whereas fault is unexpected variance of regular system behaviour. The different types of faults that lower availability are

1) Design Errors: If the system has flaws in it design, it may work unexpectedly. These can occur on hardware and software. These can either be crashes or lowered performance.

2) Hardware Failure: When system faces thermal or mechanical stress, hardware might start failing. Requires replacing or repairing the failing hardware.

3) Overloading the system: These happen when different parts of the systems capabilities are not sufficient to work efficiently. An example would be server sending more traffic to the router than the router can handle. This will increase latency and might cause packet drop, making failures elsewhere.

4) Error while execution: When a program executes, it might face an error, such as server running out of memory. These rarely crashes systems anymore, but lowers availability (Qadir and Quadri, 2016).

Denial-of-Service (DoS) is the main attack threatening availability, decreasing it or making varying degrees of IS unavailable, usually a machine or network resource. There are no built-in mechanisms on the internet to block malicious traffic flow, making this the problem of the target (Cao et al., 2018). DoS can be done in multiple ways. The simplest one is to send large amount of traffic into service or machine exceeding its capability to process it. This can be avoided by increasing hardware and network capability, but also some Content Delivery Networks (CDN) offer DoS protection as a service, such as Cloudflare by routing malicious traffic elsewhere (Cao et al., 2018). It can also be done by exploiting software's or service's own functionalities in unintended ways, such as sending a large number of requests for a larger dataset to be downloaded. This doesn't require much power from the adversary, but it might overwhelm the system. Distributed Denial of Service (DDoS) differs from DoS in that the traffic comes from multiple sources to the target system. The sources are usually network of computers under adversary's control called botnets, which are often acquired as a result of malware or poor security.

The amount of Internet of Things (IoT) devices are increasing in the world, and these devices have lower security than regular systems. These are also harder to patch for security vulnerabilities. In 2016 major Domain Name System provider Dyn was a target of a DDoS attack, making multiple popular sites unavailable in Europe and United States during 21st of October. A botnet called Mirai was used, which spreads from network to network, looking for vulnerable devices, and once it exploits device vulnerabilities, it

starts to spread on its own to next connected devices (Sreekanth, Sri and Vartiainen, 2017). IoT device security is still a hot topic in security research.

2.1.4 Possession

Possession refers to information being under control or in hand of the possessor but not necessarily available for use or known by the possessor. In this context a possessor is always a person, such as user, owner, service provider (Parker, 1995). Possessing information does not require owning the data, it only requires physical access to it. Possession is often used interchangeably with control.

Physical measures are required to maintain control of possession. Computers can be physically locked so that accessing them is hard, and access to server rooms within organization is usually restricted to IT only. Getting into public data storage provider's data centre requires clearances, and operators are only allowed to perform actions they are permitted to. These are physical versions of access control. Insider threats have increased by 47% in the US from 3200 in 2018 to 4716 in 2020, underlining the importance of these controls (Ponemon Institute, 2020).

Nowadays Bring Your Own Device (BYOD) and using organizations devices on free time happens often. These devices usually have organizational data in them besides user's personal data, resulting in data contamination. This might result in unintentionally losing possession over organizations data, such as uploading it to personal cloud storage or lost devices, or organizational backups might include personal data. Users might even lose their devices, losing possession to the organizational data, or even credentials to the organizational systems. Organizations should have control of the devices over the internet, to lock or wipe them remotely (Romer, 2014).

Possession of backups is also important, as they have the same information than organizational databases. Losing backups from theft results in loss of possession and confidentiality. However, if the backups are encrypted, only possession is lost, not confidentiality (Andress, 2014).

2.1.5 Authenticity

Authenticity refers to the verification of origin of information, so that the receiver of the information can be sure that the information came from the sender. It is defined as "property that an entity is what it claims to be" (ISO/IEC 27000, 2018).

Besides checksums covered in integrity, digital signatures can help with authenticity. These rely on public-key cryptography, also called asymmetric cryptography. In public-key cryptography parties have a public key, which they share, and private key. When user A wants to send information to user B, user A signs the information with their own private key. After user B receives the information, they can verify that the information is indeed from user A by verifying the signature with user A's public key. This way the information is digitally signed, although not encrypted. The message from user A could be also encrypted using user B's public key, making it so that user B is able to decrypt it using their own private key.

E-mails have their security mechanisms built on top of original standards. E-mail is older protocol than internet, which doesn't verify if the sender is who they claim to be which is called spoofing, or if the message has been altered during delivery. However, modern email servers and clients have their own verifications to prevent spoofing and tampering. The receiver's email client or web client informs the user if the origin of the email is not the email domains sender. Some of these protections against e-mail forgery include Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication Reporting & Conformance (DMARC) (Hu, Peng and Wang, 2018). These are all implemented on the domain's (such as @aalto.fi) e-mail server using Domain Name Server (DNS) records and public-key cryptography (Leiba and Fenton, 2007). When e-mail is received from a domain, the receiver (nowadays automatically) verifies from the domain it claims to come from that the message is authentic and that the signature matches (Hu, Peng and Wang, 2018).

ISO 7498-2 also states non-repudiation. It means that author of information cannot dispute that they are the origin of the information. If service provides information to some other party, they are not able to tell that the information didn't come from them, when it really did. It is proof of integrity and origin of data with high confidence. This can be seen in blockchain – transactions are confirmed and signed by the origin of the transaction, making it impossible to deny the source of the transaction.

2.1.6 Utility and Usability

Utility refers to usefulness and fitness or resource to some purpose. Usability should also be considered as part of utility, although Parkerian Hexad does not state usability as a security goal (Reid and Gilbert, 2010).

Utility can be lost if information is encrypted, but the encryption key is lost, making decryption impossible. The information has not lost its confidentiality, availability, integrity, possession or authenticity, but the utility is gone as the information is in unusable format (Reid and Gilbert, 2010). Utility is also decreased if information is in a wrong format, or users lack the correct tools to use the resources.

Usability refers to how convenient it is for users to use resources. It has been studied surprisingly little. However, increasing security controls usually decreases usability, as from user's perspective increased security may add additional steps and bureaucracy to their daily work, decreasing their incentive to apply these steps. Human is the weakest link in contemporary security (2018 Global State of Information Security Survey, 2017), and some users might start to skip security protocols to make their work easier. This results in less secure organization, although security controls are in place. Thus, applied security controls should not be able to be skipped. Security with good usability enhances overall security without decreasing overall performance too much.

2.2 How can organizations establish Information Security?

Fully comprehensive and perfect InfoSec does not exist. Some events, such as natural disasters cannot be avoided. Devices and systems evolve and increase, which results in more possible problems. Humans are also part of InfoSec. According to an IBM study, 95% of breaches are initiated by human error (IBM et al., 2015). Additionally, some systems might yet to face their vulnerabilities, they might not be developed or used publicly yet.

InfoSec strategy should be planned from the top down and implemented from the bottom up. This means that management should start planning by considering enterprise leaders, internal audits, business partners, customers and investors on general level. After that organization unique activities need to be considered to fill possible gaps in strategy. Implementation should be done by breaking each process in the strategy into tasks, and finding owner for the process, defining duties and responsibilities for the process, identifying specific tasks, defining completion standards and implementing confirmation process (Jones, 2000). InfoSec is also an investment from management perspective. It is risk management without correct answers, as it is not an exact science (Initiative, 2011).

2.2.1 Risk

Risk can be defined economically as following (Bojanc and Jerman-Blažič, 2008):

$$Risk = Probability\ of\ an\ Event * Business\ Impact$$

Probability of an event is an estimate for how probable it is that an event occurs. These could be any incidents, such as thefts, cyber-attacks or fires at data centre. These are harder to estimate when the target is intellectual property. When the probability is multiplied by the estimated business impact, that is the currency value of a risk.

Risk can be minimized in multiple ways:

- Avoiding risk by decreasing probability of an event through either eliminating the risk (i.e. taking device offline) or applying controls make it occur less (i.e. implementing technologies, tools and processes)

- Transferring the risk responsibility by insuring assets

- Accepting the risk – if the cost to mitigate the risk is higher than what the overall risk would decrease, it can be accepted as a cost of doing business, as the investment is not worth it

Often when organizations face adversaries or disasters, multiple events happen in chain. It might begin from user opening malicious e-mail attachment, leading to losing stored plain text passwords, leading to theft of database. Even if the database has good user control and intrusion detection, the adversary authenticated as the user.

From this imaginary scenario we can derive two points. First, organizations' defence is only as good as its weakest link. Second, in scenarios like these risks are hard to estimate, making ability to benchmark InfoSec investments hard. It is hard to determine the return of an investment on a safety measure, which prevented risks from ever happening, making justification of InfoSec budgets harder.

2.2.2 Information Security Management Systems

ISMS consist of sets of policies implemented by an organization to define, construct and implement, develop and maintain security of their software and hardware assets (Susanto, Almunawar and Tuan, 2011). These policies guide how computer resources can be used by applying controls. Without ISMS security policies and controls might be disorganized and disjointed, thus ISMS gives better overview of policies (Susanto,

Almunawar and Tuan, 2011). The most established ISMS's are ISO/IEC 27000-series standards published by International Organization for Standards (ISO) and International Electrotechnical Commission (IEC) (Disterer, 2013).

These standards range from an overview of InfoSec to establishing InfoSec policies, implementing these, adding security controls and how to secure so called modules, such as human resources, networks or contactor agreements. They to fine technical details. The ISO/IEC 27001 has the best overall framework for establishing InfoSec policy, and organizations can get certified by it (Disterer, 2013). Other policies exist as well, such as Payment Card Industry Data Security Standard (PCI DSS), which is standard for businesses using card payments, or Control Objectives for Information and Related Technology (COBIT). Choosing the right ISMS's depends on multiple factors, such as industry, size of organization, number of locations, country or countries, number of information systems, age of different information systems, handling of confidential data or lack of thereof, to name few (Susanto, Almunawar and Tuan, 2011).

2.2.2.1 ISO27000 -series

ISO27001 requires that organization's management examines risks their IS might be facing. When risks have been recognized, they need to be covered by using InfoSec controls, or by applying other risk treatment such as insurances. These controls and operations to mitigate risks need to be continuous and monitored to improve ISMS (Gillies, 2011; Disterer, 2013). These steps should be aligned with PDCA cycle:

- Plan – Establish the ISMS for organization
- Do – Implement ISMS policies, security controls, processes and procedures
- Check – Monitor the ISMS
- Act – Update and improve ISMS

It has 14 domains covered (Disterer, 2013):

- Security policy – How policies are reviewed and written
- Organization of information security – How responsibilities are assigned
- Asset management – Controls related to assets

- Human resources security – Controls related to employees before, during and after employment
- Access control – Controls for access rights of users, systems and applications
- Cryptography – Controls related to encryption key management
- Physical and environmental security – Controls defining secure areas, protection against threats, entry control, equipment security, waste disposal etc
- Operational security – Controls related to IT production, such as protecting availability and integrity of software, minimize system failures, logging, backups
- Communications security – Controls related to network security and services, messaging, network segregation and Virtual Private Networks
- Supplier relationships – Controls on frames for agreements and supplier monitoring
- Information systems acquisition, development and maintenance – Controls defining how to maintain security in development and acquisitions
- Information security incident management – Controls for reporting weaknesses, ensuring reports are handled in timely manner
- Business continuity management – Controls to counteract interruptions to business activities and recovery
- Compliance – Controls to avoid breaches of applicable laws and regulations, intellectual property protection and licenses

ISO 27002 goes covers descriptions and guides on how to implement controls under the modules vendor independently, resulting in overall InfoSec strategy, policies, controls and processes to secure organizations information. Rest of the series covers the domains thoroughly, including planning and technical implementation for the domain.

2.2.3 Information security incident statistics

A survey conducted in 2017 by PwC, CIO and CSO found out that the average cost of an incident has increased by 58% over 2 years, being 364 USD in 2016 and 578 USD in 2018. However, the number of detected incidents had decreased during the same time by 50% from 6 853 in 2016 to 3 458 in 2018. From these respondents 75% felt confident that they

have the ability to correctly assign attribution to an attack. This means that 25% of the respondents does not have the ability to tell if they were attacked or not.

Other interesting findings from the survey include that current employees cause 30% of security incidents, being the largest source of incidents in their study. This is followed by 26% of former employees, which could have been mitigated by having human resource controls in place. The survey had 9 500 respondents from 122 countries, and it was conducted online (2018 Global State of Information Security Survey, 2017).

In 2019, 49% of organizations stated cybersecurity as their information technology initiative. It is the second most important initiative after Digital transformation (54%). The survey had 303 respondents whom were executives and high-level managers with visibility to their organizations' IT budgets. The respondents' organizations had over 2 000 employees (Flexera Software, 2019).

A study conducted in Norway asked respondents what type of incidents they had faced between 2016 and 2018. The numbers represent the percentage of the respondents who had faced said incident.

Table 1. The amount of incident types organizations in Norway had faced in 2016 and 2018 (n=1500) (source: The Norwegian Business and Industry Security Council, 2018)

Type of incident	% of incidents in 2016	% of incidents in 2018
Virus and/or malware infection	20 %	21 %
Phishing or other social engineering attacks	8 %	18 %
Attempted data breaches/hacking	8 %	13 %
Incidents caused by employees	10 %	11 %
DDoS attacks or threats of these	4 %	7 %
Fraud	2 %	6 %
Computer vandalism	4 %	6 %
IT equipment theft	5 %	6 %
Data breaches/hacking	2 %	5 %
IT resource abuse	3 %	3 %
Breaches of security for information including user, employee, customer or patient data?	0 %	2 %
Penetration of the organization's security systems	2 %	2 %
Incidents caused by outsourcing provider	2 %	2 %
Lost trade secrets through information theft/digital espionage	0 %	0 %

From the survey we can see highest increase was in phising or other social engineering type of attacks. When combined with Incidents caused by employees, we can see that 29% of the incidents were either caused by humans or targeted at humans. These types of incidents are more resilient to technological controls, as humans might not work according to security policies.

The main type of incident is an infection by virus or malware (21% in 2018). These types of incidents are usually not targeted at specific organizations, as they rely on vulnerabilities found on software and services organizations are using, as well as humans opening malicious files. These kinds of incidents might happen to every organization, even though they have no valuable assets. The real number of untargeted incidents is higher in reality, as phising, fraud and theft can all be untargeted by using a large list of possible targets such as e-mail addresses found online, where organization just falls as a victim.

3 Discussion and conclusions

From the findings we can see that InfoSec attributes are well established, but converting risks into monetary value to justify InfoSec IT initiatives is hard. It is positive that legislation force organizations to have InfoSec, and industries do have their own InfoSec models and policies which need to be applied, but only following these does not offer full protection as mistakes are easy to make. InfoSec also requires management's involvement, and making it organizations IT's area solely is not be enough.

InfoSec attributes have been well established for a long time, but evolvement of technology and services shift the importance of individual attributes. Said evolvement does also expose new threats to InfoSec, which security managers and policy planners need to be kept up with. Previously securing only IS's has been sufficient, but

3.1 Implications to research

While there have been previous studies about individual InfoSec attributes, most of the research has been published before 21st century. With the pace of digitalization and evolvement of IS's, older research has more emphasis on traditional CIA-triad and on system-centric approach. There is need to inspect the attributes in contemporary environment, which this paper contributes to. Usability is little researched and rarely mentioned, but emphasis on usability is important as it increases user's security compliance. In the past securing systems only from outside was often mentioned, giving less focus on humans.

This paper also presents fresh data on the share of different incident types and their sources including examples of attacks that have been done. Having this information, it is easy to see which are the main sources and types of incidents to focus in future. Malware including ransomware and viruses are still main incidents, but attacks aimed at humans are increasing. Attacks aimed at humans are less mentioned in previous research, which is a newer challenge in InfoSec.

3.2 Implications to practice

Understanding different attributes is mandatory for creating InfoSec policies. When each of the modules are planned, one has to think what attributes relates to them and how these can be secured. The practical methods to apply security controls were not covered

here, but the elements that need to be secured are covered. With this information and understanding of organizations' IS's, processes and interconnected resources one can start to think about risks considering their organizations assets, and start planning InfoSec policies by their own.

This paper also includes a managerial guideline for establishing or increasing InfoSec policy. The guideline follows the most established model ISO / IEC 27001. Including statistics underlines the importance of the topic. InfoSec should not be neglected, it is easier to recover from incident when the plan and mechanisms for a recovery are established before incidents occur. InfoSec should be an enabler of operations and processes within organization, and good practices allow new ways of operating.

3.3 Limitations and future research

Using literature frameworks might have given more insight over InfoSec attributes. However, InfoSec's definitions are often defined after established models. Because of this, most of the results were agreeing on the attributes. Some alternative InfoSec attributes were modelled, but these tended to have a low number of citations and were basically the same attributes reinvented.

Information on organizational implementation could have had with conducting interviews of security researchers working in the field to give some more insight, especially on how InfoSec is implemented in Finland. ISO standards and their implementations are widely accepted as good practice, but according to ISO, ISO / IEC 27001 certificate has been awarded to 59 organizations in Finland (ISO, 2018), when NASDAQ OMX Helsinki has 129 companies listed (Nasdaq, 2020). Some organizations might follow the standards without buying accreditation for the certificate, but it still leaves question how smaller organizations implement InfoSec, if at all. Studies of incidents in Finland did not exist, Norway being the most similar market cited (Statista, 2018). This leaves room for future research.

This thesis was not country specific, but answers to these questions would be interesting. I do believe that smaller organizations have less controls and processes to detect and mitigate incidents, distorting the results as it is harder to answer surveys of something that one cannot detect.

Evolvement and increasing complexity of IS, technology, devices and networks has not gone unnoticed by adversaries. Causing an incident in a system might be just way of using

it that the developers did not intend it to be used. The damage might be costly, and increasing monetary gains from attacks drive adversaries further. These topics should be studied more, and start research in Finland.

4 References

2018 Global State of Information Security Survey (2017) The 2018 Global State of Information Security Survey. Available at: https://www.idg.com/tools-for-marketers/2018-global-state-information-security-survey/ (Accessed: 19 August 2020).

Andress, J. (2014) 'Chapter 1 - What is Information Security?', in Andress, J. B. T.-T. B. of I. S. (Second E. (ed.) The Basics of Information Security. Boston: Syngress, pp. 1–22. doi: https://doi.org/10.1016/B978-0-12-800744-0.00001-4.

Bojanc, R. and Jerman-Blažič, B. (2008) 'An economic modelling approach to information security risk management', International Journal of Information Management, 28(5), pp. 413–422. doi: 10.1016/j.ijinfomgt.2008.02.002.

Cao, Y. et al. (2018) 'Understanding internet DDoS Mitigation from academic and industrial perspectives', IEEE Access. IEEE, 6, pp. 66641–66648. doi: 10.1109/ACCESS.2018.2877710.

Cohen, F. (1987) 'A cryptographic checksum for integrity protection', Computers and Security, 6(6), pp. 505–510. doi: 10.1016/0167-4048(87)90031-9.

Disterer, G. (2013) 'ISO/IEC 27000, 27001 and 27002 for Information Security Management', Journal of Information Security. Scientific Research Publishing, Inc, 04(02), pp. 92–100. doi: 10.4236/jis.2013.42011.

FINLEX (2010) 'Laki terveydenhuollon laitteista ja tarvikkeista 629/2010'. Oikeusministeriö, Edita Publishing Oy.

Flexera Software (2019) Priorities for tech initiatives in global organizations 2019. Available at: https://www-statista-com.libproxy.aalto.fi/statistics/1106032/top-priorities-it-technology-initiatives/ (Accessed: 19 August 2020).

Gillies, A. (2011) 'Improving the quality of information security management systems with ISO27000', The TQM Journal, 23(4), pp. 367–376. doi: 10.1108/17542731111139455.

He, D. and Wang, D. (2015) 'Robust Biometrics-Based Authentication Scheme for Multiserver Environment', IEEE Systems Journal. IEEE, 9(3), pp. 816–823. doi: 10.1109/JSYST.2014.2301517.

Hu, H., Peng, P. and Wang, G. (2018) 'Towards understanding the adoption of anti-spoofing protocols in email systems', in Proceedings - 2018 IEEE Cybersecurity Development Conference, SecDev 2018. Institute of Electrical and Electronics Engineers Inc., pp. 94–101. doi: 10.1109/SecDev.2018.00020.

IBM et al. (2015) 'Cyber Security Intelligence Index 2015', IBM Security Managing Security Services, p. 24. doi: SEW03039-USEN-02.

Initiative, J. T. F. T. (2011) SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. Gaithersburg, MD, USA: National Institute of Standards & Technology.

ISO/IEC (2013) 'ISO/IEC 27002:2013.pdf', Iec, 2013, p. 90. Available at: www.iso.org.

ISO/IEC 27000 (2018) 'International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Overview and', ACM Workshop on Formal Methods in Security Engineering.Washington, DC, USA, 34(19), pp. 45–55. doi: 10.1016/j.im.2003.02.002.

ISO (2018) The ISO Survey. Available at: https://www.iso.org/the-iso-survey.html (Accessed: 19 August 2020).

Jiang, Y. et al. (2004) 'Security analysis of mandatory access control model', Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 6, pp. 5013–5018. doi: 10.1109/ICSMC.2004.1400987.

Jones, P. (2000) 'Organizational Information Security from Scratch - A Guarantee for Doing It Right', SANS Institute Information Security Reading Room.

Leiba, B. and Fenton, J. (2007) 'DomainKeys Identified Mail (DKIM): Using Digital Signatures for Domain Verification', in.

Loomis, R. J. and O'Connor, A. C. (2010) '2010 Economic Analysis of Role-Based Access Control Economic Analysis of Role-Based Access Control Final Report', Economic Analysis, (0211876).

Nasdaq (2020) Shares - Nasdaq. Available at: http://www.nasdaqomxnordic.com/learn/shares/?languageId=4 (Accessed: 19 August 2020).

Parker, D. B. (1995) 'Possession as an element of information security', Information Systems Security, 4(2), pp. 19–26. doi: 10.1080/10658989509342496.

Parker, D. B. (1998) Fighting Computer Crime: A New Framework for Protecting Information. Wiley. Available at: https://books.google.fi/books?id=k_u_QgAACAAJ.

Pavlich-Mariscal, J. A., Demurjian, S. A. and Michel, L. D. (2010) 'A framework of composable access control features: Preserving separation of access control concerns from models to code', Computers and Security. Elsevier Advanced Technology, 29(3), pp. 350–379. doi: 10.1016/j.cose.2009.11.005.

Ponemon Institute (2020) '2020 Cost of Insider Threats', p. 31. Available at: https://www.observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf.

Qadir, S. and Quadri, S. M. K. (2016) 'Information Availability: An Insight into the Most Important Attribute of Information Security', Journal of Information Security. Scientific Research Publishing, Inc, 07(03), pp. 185–194. doi: 10.4236/jis.2016.73014.

Rajpoot, Q. M., Jensen, C. D. and Krishnan, R. (2015) 'Attributes enhanced role-based access control model', in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, pp. 3–17. doi: 10.1007/978-3-319-22906-5_1.

Reid, R. C. and Gilbert, A. H. (2010) 'Using the Parkerian Hexad to introduce security in an information literacy class', Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10, pp. 45–47. doi: 10.1145/1940941.1940953.

Romer, H. (2014) 'Best practices for BYOD security', Computer Fraud and Security. Elsevier Ltd, 2014(1), pp. 13–15. doi: 10.1016/S1361-3723(14)70007-7.

Schultz, E. E. et al. (2001) 'Usability and security an appraisal of usability issues in information security methods', Computers and Security, 20(7), pp. 620–634. doi: 10.1016/S0167-4048(01)00712-X.

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', Computers and Security. Elsevier Ltd, 38, pp. 97–102. doi: 10.1016/j.cose.2013.04.004.

Sreekanth, A., Sri, P. and Vartiainen, T. (2017) 'Dyn DDOS Cyberattack – a case study', pp. 3–5.

Stahl, B. C., Doherty, N. F. and Shaw, M. (2012) 'Information security policies in the UK healthcare sector: A critical evaluation', Information Systems Journal, 22(1), pp. 77–94. doi: 10.1111/j.1365-2575.2011.00378.x.

Statista (2018) Norway: encountered information security incidents in businesses 2016-2018, Statista. Available at: https://www.statista.com/statistics/994974/share-of-encountered-information-security-incidents-in-businesses-in-norway/ (Accessed: 19 August 2020).

Statista (2020) 'Business cyber security in the United Kingdom (UK)'. Available at: https://www.statista.com/study/39726/business-cyber-security-in-the-united-kingdom-uk-statista-dossier

Susanto, H., Almunawar, M. and Tuan, Y. (2011) 'Information security management system standards: A comparative study of the big five', International Journal of Electrical Computer Sciences IJECS-IJENS, 11(5), pp. 23–29.

The Norwegian Business and Industry Security Council (2018) Information security, privacy and cybercrime.

Wang, Q. et al. (2011) 'Enabling public auditability and data dynamics for storage security in cloud computing', IEEE Transactions on Parallel and Distributed Systems. IEEE, 22(5), pp. 847–859. doi: 10.1109/TPDS.2010.183.

Whitman, M. E. and Mattord, H. J. (2011) 'Principles of Information Security Fourth Edition', Learning, pp. 269, 289.

Zhang, Z. L., Hong, F. and Xiao, H. J. (2006) 'Verification of strict integrity policy via petri nets', Second International Conference on Systems and Networks Communications, ICSNC 2006, 00(c), pp. 6–9. doi: 10.1109/ICSNC.2006.76.

Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', Future Generation Computer Systems. Elsevier B.V., 28(3), pp. 583–592. doi: 10.1016/j.future.2010.12.006.

5 Appendices

5.1 Glossary

- (D)DoS – (Distributed) Denial of Service, an attack in which large amount of traffic is sent to a target, aiming to decrease availability of the target
- ABAC – Attribute-Based Access Control. Subjects access to objects based on their attributes, such as device they are using, their location or network they connected from.
- Breach – loss of confidential information
- Content Delivery Network (CDN) – Network to host websites and their content in multiple geographical locations closer to users. High bandwidth and capacity of network.
- DAC - Discretionary Access Control. Owner of the object decides authorizations for subjects to the object.
- Decryption – Decrypting encrypted information with a secret key, to make it readable and usable.
- Domain Name Server (DNS) – Tells clients such as web browsers the location of websites and servers. Without this websites (aalto.fi) would need to be replaced with IP addresses (104.17.221.22)
- GDPR – General Data Protection Regulation – Guidelines for organizations in EU for using and storing consumer data
- Encryption – Information which is encrypted with a secret key. Decryption with modern encryption method is not possible without knowing the key, making it available only for the key holder.
- IS – Information System
- ISMS – Information Security Management System. Policies, guidelines and controls to maintain information security.
- ISO / IEC 27001 – Part of ISO / IEC 27000 ISMS', a security model to establish comprehensive information security practices. Also, a certificate admitted to organizations practicing the model.
- IT – Information Technology

- InfoSec – abbreviation of Information Security
- IoT – Internet of Things. Devices operating in low power, having usually low processing power, such as sensors. These are connected to organizations information systems online.
- MAC – Mandatory Access Control. Central administration grants security classifications to subjects and objects
- PCI DSS - Payment Card Industry Data Security Standard. ISMS for organizations accepting and processing card payments.
- RBAC – Role-Based Access Control. Subjects access to objects is determined by roles, such as team or tasks subject performs. Objects are under roles.
- Virtual Private Network (VPN) – Method to access organizational network remotely if authorized. The traffic to the organizations network is encrypted, enabling safer use of public and untrusted networks.