Risks in a digital collaborative business environment

Julius Ketonen

2019 Laurea

Laurea-ammattikorkeakoulu

Risks in a digital collaborative business environment

Julius Ketonen
Degree Programme in Security Management
Bachelor's Thesis
May, 2019

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor's Thesis

Julius Ketonen

Risks in a digital collaborative business environment

Year 2019 Pages 26

This thesis was created for Collaxion, in the support of the DBE Core project. The purpose of the work was to identify and answer questions relating to security risks faced by the system. The results of this work are intended to be used in further development of DBE Core system and minimising the risks facing it.

This thesis is qualitative in design and is primarily focused on the resilience of various parts making up the system, particularly in regard to its cognitive and social dimensions. The data has been gathered through the use of desk research and a security literature review.

The results of the thesis show that the risks faced by the system are typical information security risks (incl. social engineering), legal (data ownership) and the unexpected developments of security risks in emerging technology (blockchain) in the form of "black swans".

The development suggestions include education against social engineering, vetting of partners and stakeholders.

Keywords: collaborative, data, risk, industry

Laurea Ammattikorkeakoulu **Tiivistelmä**
Degree Programme in Security Management
Opinnäytetyö

Julius Ketonen

Riskit digitaalisessa, kollaboratiivisessa liiketoimintaympäristössä

Vuosi 2019 Sivumäärä 26

Tämä opinnäytetyö on tehty Collaxion yhtiötä varten, DBE Core projektin tueksi. Työn tarkoituksena on ollut selvittää ja vastata kysymyksiin liittyen kehitettävän järjestelmän turvallisuusriskeihin. Tämän työn tuloksia on tarkoitus käyttää järjestelmän edelleen kehittämisessä ja mahdollisten riskien minimoimisessa.

Tämä opinnäytetyö on muodoltaan laadullinen ja keskittyy pääasiassa järjestelmän eri osien resilienssiin, erityisesti sen kognitiivisessa ja sosiaalisessa merkityksessä. Tieto on kerätty ehdokaskartoitusta ja turvallisuusalan kirjallisuutta käyttäen.

Opinnäytetyön tulokset näyttävät että järjestelmän haavoittuvuudet ovat opinnäytetyön kontekstissa tyyppillisiä tietoturvariskejä (ml. käyttäjän manipulointi), laillisia esteitä (tiedon omistajuus) ja ilmestyvän teknologian aiheuttamat arvaamattomat turvallisuusmuutokset ”mustien joutsenien” muodossa.

Kehitysehdotuksena on annettu opetus käyttäjien manipulaatiota vastaan, yhteistyökumppaneitten ennakkotarkistus ja eri osa-alueitten standardisointi (sopimukset, toimintatavat yms.).

Asiasanat: Kollaboratiivinen, data, riski, teollisuus

Table of contents

1 Introduction

This thesis was created for the company Collaxion, and in extension the DBE Core project, with the purpose of exploring risks faced by a collaborative business environment, a digital business network of various stakeholders. These risks are primarily looked through social, legal, cognitive and organisational factors. The research questions of this work were:

- What are the primary risks CBE activity will face?
- Are some risks unique to a CBE?
- What can be done to mitigate the risks?

First the framework of the work is introduced, in which the background, key concepts and the theory guiding this work will also be shown. Underneath this heading will be the basic classification of sources and the theory guiding the form this work has taken, the DBE Core project itself along with its objectives, and the basics of the proposed digital collaborative business environment. This will allow us to understand the structure to be analysed, with the relevant implications for the industries involved. Then the system structure of the Collaborative Business Environment was described in a simple way, with technical details (code, hardware etc.) left out as they are not within the scope of this work. Legal framework within which cloud storage exists will also be explored. Due to the nature of the project, this will primarily focus on the company perspective rather than the individual person, with some overlap involved. This includes discussion on international and national legal frameworks to illustrate the differences between them.

Secondly, the methodology and various elements that compose the body of this work are presented. This will include the tools of analysis and their use as related to the topic. By using the available tools of analysis, the information presented will be brought together and concrete examples of risks will be brought forward. These will be taken from the various touched upon topics of the work, such as the risks relating to legal issues, information security and so on.

Thirdly, suggestions for development will be presented, addressing the issues that are identified by the methods described above, accompanied by suggestions for future development. This will be followed by the conclusions this work has ended upon. The author's self-reflection on the work is left as the last chapter.

2 Framework and background

With the digitalisation of society, businesses are faced with ever more competition due to digitalization, as the digital economy becomes ever more omnipresent (Ahokangas, Lehtimäki,

Helaakoski & Peltomaa 2015, 8). The phenomenon has brought forth the automatization of production, bringing with it new challenges in areas such as employment, engineering and what concerns this work, security management. While things such as the transformation of manual labour into automatized labour is becoming more common, it has also brought with it an increasing information flow. What is happening is the creation of an increasingly connected "information sharing economy" with new business models (Collaxion 2017).

The increase of data flow and the demands it puts on the integrity and accuracy of the data bring out certain risks (Ismail 2018). What this work was particularly interested in, was the sharing of information between multiple stakeholders, the altering of the data shared in real-time and possible problems caused by this, regarding the duties and responsibilities of everyone involved. These problems can include everything from copyright disputes to differences in procedure between the different stakeholders (Roche 2014, 1-6).

The introduction of technologies such as cloud storage and blockchain makes the question of data ownership a central object of concern. Industries found that in a more demanding market that constantly increased in complexity, creating collaborative networks was far more efficient to the more traditional static organisations, since the nature of logistics and supply chains have changed in their fundamentals (Ahokangas, Lehtimäki, Helaakoski & Peltomaa 2015, 6). The exact nature of the risks of cloud storage have been documented by Roche (2014, 1-6), but creating a digital ecosystem for the Finnish industries is a new venture and the exact risks should be analysed specifically for the purposes of this new system. The DBE Core project was created to facilitate the creation of such a system.

2.1 Knowledge base

The basis of the knowledge comes from multiple sources. The system being in development, and due its many parts creates need for a varied base, therefore sources often consider one aspect of the topic by itself, rather than the specific whole. The literature will include both physical and electronic sources, mostly the latter due to the ease of access. Other articles, such as news stories are also included in the following categories.

The electronic sources will contain:

- The ISO 31000 standard
- Relevant material found in various services
- Confidential project files

Physical sources:

- Security and risk management literature
- Research method literature e.g. Taylor, Bogdan & DeVault
- Other sources in security management

The above was a concise explanation of the types of sources used and next there will be explanations on the theory and key concepts driving this work. These are the CBE system that this paper specifically is focusing on, blockchain technology and finally the legal implications of such a system. These will give basic understanding on top of which the analysis and conclusions of this work are built on.

2.2 DBE Core

The purpose of the Digital Business Ecosystem Core project is explained on the DBE Core website as:

"DBE Core enables the integration of business processes by the aid of API integration. It can be widely used in the areas of sales, sourcing, procurement, logistics and transaction-based financing. With our solution, you can save up to 4% to the bottom line by automating. We offer an agile supply chain with transaction-based banking that generates new working capital by supply chain financing. Information exchange, accurate data and quick integration are just a few of our benefits. DBE Core is based on global established standards." – DBE Core, 2018

In other words, it attempts to integrate the major functions shared by various industries to create an "ecosystem" where all the business to business activity is handled digitally. The global established standards in question are the relevant ISO/IEC standards and project guidelines. This will allow the creation of a common customer message across the various participating industries as everyone can be guaranteed to use the same standards (Collaxion 2018).

As a system does not exist at present, anyone who manages to create the first one will be in a prime position to define the rules and practices of such an environment (Collaxion 2018). This also means that concerns about the handling of confidential data and proprietary information has taken centre stage. This is highlighted by the General Data Protection Regulation, which explicitly deals with the storage and use of private data (Gdpr-info 2018).

2.3 Collaborative Business Environment

The primary idea of the CBE is to have a shared cloud system as the core, security provided by blockchain technology. Each stakeholder has access to the information that is relevant to their function, stored in the cloud. The access is controlled by the stakeholder's interface, which is standardized across all the companies involved. Therefore, while everybody has the

same program, the type of information that is available is determined by the individual company (Collaxion 2018).

For example, if a factory needs a new part to repair a machine, it would first identify its need to the system and place an order. Then any company that supplies these parts would be able to see this order, give their estimate of cost and other suggestions. Once accepted, it is possible that a specialised technician is needed to install the part. This information would be available to any that can supply this form of technician and so on. The company that started the process can follow each step and so can the companies that fulfil the order, building trust and predictability. Due to the nature of the digital environment, everyone will be able to see the information necessary, as a change in information can be seen by all involved (Collaxion 2018). Business can therefore collaborate on various suitable fronts without losing their individual competitive edges (Ahokangas, Lehtimäki, Helaakoski & Peltomaa 2015, 6).

The system would allow the efficient flow of information from business to business, while at the same time guaranteeing information security by compartmentalising (Ahokangas, Lehtimäki, Helaakoski & Peltomaa 2015, 6). All involved will therefore have a fast, practical and secure way of sharing information, minimising the unpredictable factors relating to issues such as procurement. Figure 2 illustrates a simplified way the CBE is structured:

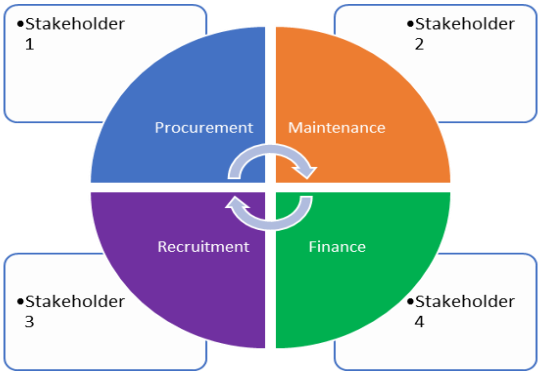

Figure 1: CBE Structure

In the next part, blockchain is explained and how it is used as a way of verification and security in the proposed environment. This is used to create a record of all transactions that happen in the system.

2.4 Blockchain

The underlying structure and security of the system is based on blockchain technology, made famous by the introduction of Bitcoin. While the actual technical details of the system are outside of the scope of this work, a short explanation of what a blockchain is, is vital. This is to assist the identification of security risks and the understanding of the topic.

Blockchain at its most basic level, is a chain of blocks containing information of transactions. Due to the inherent nature of its structure, every block is connected to every other block that comes both before and after it, making the modification of the information extremely difficult (IBM 2018). This would require the modification of every single block, a tremendous task as a single chain can grow to be incredibly large, as demonstrated by the growth of the Bitcoin blockchain (Statista 2018). Figure 3 below illustrates the basic structure of a blockchain.

Figure 2: Blockchain structure

The security of the blockchain, and therefore the DBE Core system at large, is based on its encryption and the decentralisation inherent in the technology. Any tampering immediately voids the security key used to access a single block and alert is sent out to the rest of the network. Unless a huge amount of processing power is used, altering a large blockchain in its entirety would be an almost insurmountable task, although not impossible (Van Wirdrum 2018).

The introduction of blockchain into the digital economy is changing the nature of business and the practice of law. Whether it be through “smart contracts” where assets can be transferred instantly when certain conditions are met or a business that wants to verify where a part of a machine came from. This way a record of the transaction will always be there to be found (Altman 2018).

2.5 Legal and Contractual concepts

The legal elements concerning the described system had one specific focus in this work, information ownership. The information will be passing through multiple systems and will be changed according to the needs of the situation (maintenance requirements, spare part orders etc.). This puts the question of data ownership and the risks relating to such issues in a central place among corporate concerns.

It should be noted that the legalities are not limited to the companies, but also to its individual customers. With the introduction of the General Data Protection Regulation (GDPR), which will mandate certain standard privacy practices across the EU, one of the major

changes is the assignment of a Data Protection Officer responsible for the management of the private data (Gdpr-info 2018).

Roche (2014, 1-6), has split the general legal issues of a cloud system in several categories. Of these, three relevant ones will be presented here. They are:

The ownership of data is primarily controlled through contracts between several actors, which defines their rights and duties regarding data and its storage. The complexities brought forward are primarily created by the different parties using the same information and possibly even changing it. Generally, whoever creates the data has automatic ownership of it unless stated otherwise in a contract. An example of this could be the numerous forms of terms and conditions that are attached to various services and software.

Another problem caused by the nature of cloud data, is the physical location of the actual servers. The rules regarding data storage are therefore determined by national law, not international, which can make delivering a service far more difficult as the experience varies from country to country. One remedy to this problem was the introduction of common regulations and practices such as the GDPR in the EU/ETA countries.

The modification of data presents a challenge regarding the legal nature of data ownership. While the original data may have been the property of its creator, or the creating organisation, any modification done by another organisation or individual changes can cause problems. Is the original creator still the owner of the data in question, or is it transferred to the modifier in full or in part? The details of the contract are therefore of paramount importance, as they define exact status of each party regarding their handling of the information created or given to them (Chima 2016).

2.6 ISO 31000 Risk Management Standard

The ISO 31000 standard provides organizations with a general framework for managing risk. As already established, risk is identified as the effect of uncertainty on objectives, therefore risk *management* are the activities used to control risk. The standard is designed as a set of guidelines, meant to fit into an organization regardless of its industry or field (ISO 2018). The standard's risk management process is split into five stages:

- To establish context, is to understand where exactly the standard is to be applied. This includes everything from scope to the stakeholders involved.
- Next is the identification of risks. What, where, why and how are the questions regarding the risks involved.

- Risk analysis begins after the identification. This can be done through a variety of methods, but for the purposes of this report we will be focusing on the method suggested by Linkov et al. in the “Analysis Framework” section.
- Evaluating the risk is to determine whether a risk is acceptable or not, requiring further action
- Treating the risk is the final step, in which the risks are dealt with by the application of appropriate measures

This is a continuing process throughout, which does not actually end. After reaching the treatment stage, this process will circle back to the first step. Throughout the process, communication and constant monitoring is performed (ISO 2018).

The standard states:

“Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is ‘risk’” – ISO 31000

It should be noted that the standard’s definition of “risk” is not exclusively tied to a negative outcome, rather it brings in to focus the uncertainty of the conclusion of a specific event (ISO 2018). For example, an important business decision might be risky, since its eventual consequences are unknown at the time it is made, due to lack of planning or preparation.

Figure 3 illustrates the risk management process used in the ISO 31000 model:

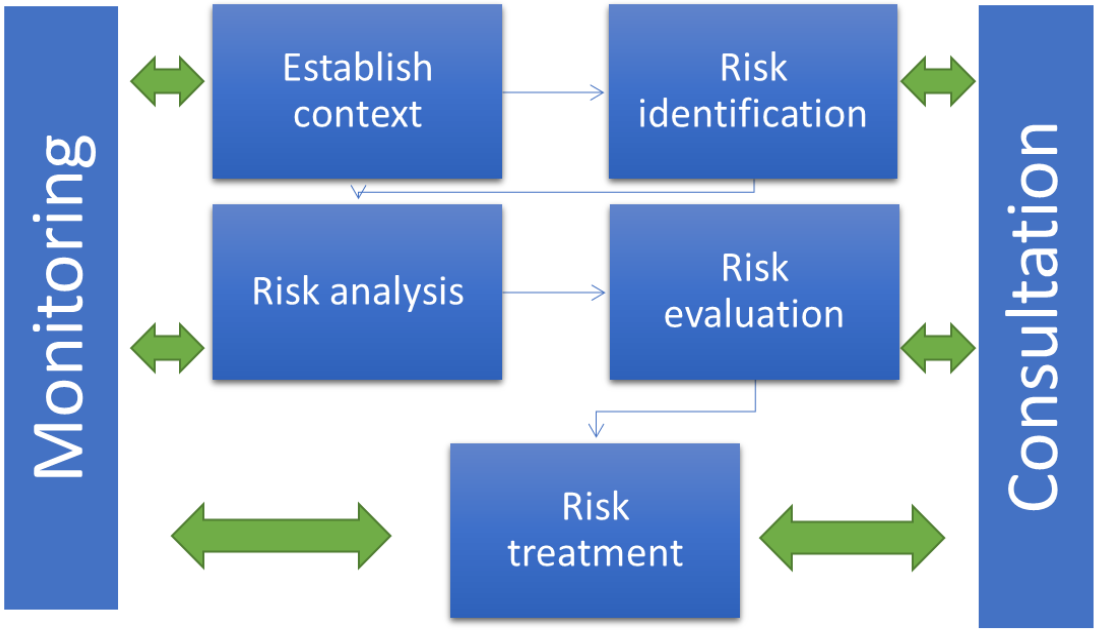

Figure 3: ISO 31000 Risk Management Standard

3 Methodology

The primary method of data collection was qualitative, using desk research. As stated by Taylor, Bogdan and DeVault (2016, 7-8), a qualitative approach is particularly concerned with how humans actually act and behave in real life, as pure statistical data often ignores the human element. It also acts as a good starting point for the cyber resilience matrix by Linkov et al. (2013) explained later in this report.

Desk research, also known as secondary research, uses already existing information from various sources for analysis. This contrasts with creating entirely new data, which is the domain of primary research (Heaton 2008, 506). This is also a necessary, since elements of the system have to be discussed separately and much of the information must be taken from confidential sources and from books, articles or websites that go through related topics, but are not directly linked to the project itself. There is no entirely grounded terminology regarding the system, so they had to be defined where appropriate.

3.1 Literature review

The work will be done in the form a literature review, in which existing literature on the topic will be discussed and the various aspects of the knowledge gained will be brought forward (Hart 2018, 31). This was chosen due to the relatively “soft” elements of the sociological implications of the topic discussed, contrasted with the “hard” elements of technical engineering or cyber systems knowledge. Specifically, this will be done closer to the

interventionist style of literature review (as opposed to scholastic), due to the practical need of the work involved.

An interventionist literature review is primarily designed with a practical purpose in mind, whether it is for managers or other stakeholders to whom the information fulfils a need to improve policy. According to Hart (2018, 93-94), an interventionist review is primarily created to find information and help the stakeholders move in the right direction, the right way. It does not offer any definitive solutions to a problem merely suggestions for improvement in policy or operations.

3.2 Document analysis

To allow for proper document analysis, it was necessary to identify both the type work this was to be (a literature review) and what methods could be used in said analysis in relation to the nature of the work.

Ridley (2012, 98-99) would describe the process by which a literature review works as cyclical, moving between three phases of reading, writing, searching. These phases have no clearly delineated end which would lead to another but are constantly active. In essence then, document analysis and the resulting product, which is the literature review, would therefore be subject to the same principles throughout the process. This process also allows the integration of literature along the way, as new information is discovered.

3.3 Information security analysis

Since the system will rely on cyber infrastructure to function, its resilience will need to be assessed with the proper framework. This will be done using the resilience matrix framework suggested by Linkov et al. (2013) which categorises the various parts of system resilience into physical, information, cognitive and social dimensions.

As mentioned earlier, the work will not be going into the physical and information domains. As described by Linkov et al. (2013), the physical aspects of the system such as its physical architecture and systems design, and the information aspect that makes such systems work through software and its program design. While the technical details of these systems are outside the scope of this work, acknowledging their existence is needed to define the two most relevant domains and their functions.

Cognitive functions are characterised by the making of decisions using both physical and information systems. In terms of the CBE, this would mean the way the system presents itself

to the user, who then acts upon the given choices and events (Linkov et al. 2013). In other words, what a person thinks and does.

The social domain describes the organization that affects the communication and the above described cognitive functions (Linkov et al. 2013). For the CBE this would mean its nature as a form of network of organizations and industries, which would in turn influence the way the different stakeholders interact with each other and the system. These two main domains both rely on direct human experience, making them particularly suited for a qualitative analysis (Taylor, Bogdan, DeVault 2016, 7-8).

All the above domains can also produce their own risks that need to be prepared for and considered. Linkov et al. (2013) suggests a four-stage method for the management of possible events, split into preparation, absorption, recovery and adapting.

- Preparation is the planning of methods to deal with possible disruption.
- Absorption is the ability to keep critical functions ongoing while maintenance or other activities are taking place to restore the functionality of the system.
- Recovery is to restore full functionality to the system and assets.
- Adapting is taking the lessons learnt and using them to prepare for the next event.

The process will then cycle back to its first phase, starting it all over again, although with added resilience thanks to the experience. By keeping the restrictions in mind for this work, the phases give a good idea of how an organisational resilience can be built even in “soft” areas like human behaviour.

3.4 Corporate Security Management Analysis

While the actual methodology of risk management will be by the standard explained later, it would be useful to go through certain aspects of corporate security management to understand the function and complexities of any role engaged in such activities. According to Bamfield (2014, 791) there has been very little research or literature created that entirely encapsulates what the purpose and objectives of security *management* is, as opposed security at large, such as policing. The field has moved on from the focus of guarding and low-level crime, to a whole new management specialty responsible of the smooth and safe running of the organization and along with positions such human resources management or operations management, forming a key aspect and competitive edge for any company.

In the same vein, security management is often reactive, spending its time responding to problems and those developing, rather than strategic planning or preparedness. This is quite

normal for managerial work, where the planning has to be integrated into the daily operational demands. This leads to dealing with issues on a case by case basis (Bamfield 2014, 791-792).

Bamfield (2014, 793) split the main objectives of security management into three categories:

- Protecting assets (physical equipment, buildings etc.)
- Protecting people (employees, visitors etc.)
- Protecting the reputation of the organization or its brands

A security department is often a relatively small and specialized group and is reliant on the information it gets from other actors, be it the IT-department or law enforcement authorities. This creates a multifaceted environment a security manager must deal with on a regular basis. Each organization is different, so the actual make-up of the department is also a variable, be it in terms of size or specialty, such as physical or IT-security. Regardless, the core activities outlined above remain largely the same in any corporation, due to the inherent nature of the tasks performed by the department.

3.5 Security system design

Technical information and engineering while not a part of this work, does provide a systems approach that allows us to glimpse the principles a security system should operate on. Brooks and Smith (2014, 107) would argue that security systems are designed to deter, detect, delay and allow for a response in any kind of security event by "integrating people, procedures, and equipment for the protection of assets or facilities". This is used to support the company objectives and support any relevant legislation, through consistent and measurable actions. As stated earlier, management is often reactive, systems being installed after the fact, leading to a possible disconnect between it and the larger organization.

4 Research and analysis

As stated earlier, the model suggested by Linkov et al. (2013) and other concepts introduced earlier in Chapter 3 will be used in the analysis. The ISO 31000 concept of uncertainty can be used as a way of guiding the process of analysis allowing for the mapping and identification of various parts producing uncertainty.

From Linkov et al. (2013), this work will specifically use the cognitive and social domains, as explained earlier. The cycling of the phases can give an understanding on how it would be possible to develop resilience in a particular area. By keeping these factors in mind, we will analyse each concern on its own by identifying the specific factors that produce uncertainty.

4.1 Data access

One of the major concerns of information security is the handling of the data access. Who can access it, where they can do so and even when they can do so. One of the major uncertainties is therefore the reliability of the stakeholders and those who have access to the system. A completely open system would be easy to use, while a completely secure system won't let anyone through (Whitman & Mattord 2011, 19).

If the access is spread to too many actors, possible malicious intent will be hard to control if such occurs. However, if the system is too narrow to accommodate various actors, it will inevitably fall flat and fail to become an industry standard, failing to justify its existence. A solution would have to find the "middle way" of security, where security and practicality meet, designed from the perspective of human behaviour and proper user experience. If a person does not understand or finds a function too hard, they will not use it (Morrow 2018). One of the ways this can be handled is using a blockchain explained earlier, in which each step of a process must be completed before the next one begins. This is indeed the proposed method of securing the system.

Compartmentalisation like this is a paramount for the CBE to function, once again increasing trust that is required for it to work in the first place. A further layer of security is the already planned method of users only knowing what they need to know. This would depend on what form of information they need i.e. which part of the supply chain they are responsible for (Collaxion 2018).

4.2 National and organisational differences

As already described in the discussion on legal and contractual concepts, one of the major problems of a large network with multiple stakeholders are the differences in procedure and the possibility that foreign or otherwise outside organisations may get involved through regular business processes. While initiatives like the GDPR allow for evermore standardised and unified approaches to information security, national laws differ regarding the specifics. Retention of data, its ownership and the way these are managed are therefore a risk in by itself, in the context of national differences. The uncertainty is in the exact handling of the data, as a nation might not have the same standards of security as others (Roche 2014, 1-6). This varied heavily even within the EU, until the arrival of the GDPR in 2018. Regardless, encryption is suggested whenever data has to be stored outside of direct control (Gray 2014).

Initiatives such as the GDPR are therefore important for the functioning of various issues such as information security across numerous states. Companies will now be forced to consider information security where possible, but it will also aid further in the development of cross-industrial data platforms across the world. With the international standards included in the

system (including various management systems), this also gives a powerful tool when competing abroad.

4.3 Human factors

It is often stated that the weakest link in any security system is the human (Vishwanath 2016), be it intentionally or by pure accident. As digitalization progresses, the digital will have an ever more profound effect on the physical world, meaning that even crimes that could have limited itself before in to one realm or another, could now affect both. These can be divided firstly into internal and external categories, followed by a division into accidental or malicious (intentionally harming) activities (Santa 2018). This split is certainly not new as we can see from Loch and Werkantin (1992, 176), but useful nonetheless.

Accidental cases are often caused by ignorance of security protocols or ambivalence towards them. These security risks can include various forms in which information systems are compromised such as clicking a suspicious link, inserting an unknown USB drive into a computer among other vectors. These are called internal accidents due to originating inside the system (Santa 2018).

External accidents are also a factor. These include events such as blackouts which affect various parts of society, but in the case of this work's concern, will put the entire information economy the system relies upon on halt. Disturbances can reverberate down the entire supply chain and critical data might be lost, if systems maintaining it are affected (Santa 2018).

Then of course is the presence of malicious behavior, both internal and external. Employees might be tempted to sell or otherwise engage in unauthorized activities with the data. While the nature of the system is such that one compromised section is not spread to the others, it can throw the entire system under a bad light, eroding the trust that is needed for it to function. Parties to the system may also cause damage and can potentially cause far more harm as they are in a key position in the system (Santa 2018).

External malicious behavior is any threat that is caused by factors outside the system or the companies involved in it. An example of this form of activity could be any form of sabotage conducted by another actor who wishes to gain an advantage due to the caused disruption. On the reverse side of accidents on behalf of an employee, is the very purposeful creation of malicious software meant to harm the systems they infect (Santa 2018).

There is a method of exploiting that targets the human element, used by criminals to access secure assets and by security professionals attempting to test an organization's security. This exploit is mainly known as social engineering, which is explored in more detail in the next segment.

4.4 Social engineering

Social engineering is a complex subject, which includes various methods by which an intruder attempts bypass security through the use of human psychology. A more specific description can be found in the Social Engineering Framework created by Social-Engineer LLC (2018) defining the act as “any act that influences a person to take an action that may or may not be in their best interest”. The framework also splits social engineering in to three top methods:

- Phishing
- Vishing
- Impersonation

Phishing is a classic scam (e.g. the Nigerian prince scam), in which an attacker sends out multiple emails, sometimes numbering in thousands, containing a link that when clicked will either download malicious software or trick a person to hand out personal information. There are also various forms of phishing that exist, such as spearphishing which is designed to exploit a particular individual instead of sending out masses of regular phishing messages. Phishing is by far the most common method of social engineering (Social-Engineer 2018).

Vishing (voice phishing) is by goal effectively the same as phishing, but by using a telephone. The attacker will mask themselves or use other methods to trick a person to reveal confidential information. This can also be a part of impersonation, explained below.

Impersonation is exactly what the word implies, in which an intruder disguises themselves to gain access to sensitive areas, assets or people. This can also apply on the internet in various ways like fake social media accounts and other such measures. An example of this could be what’s called a honeypot, someone who approaches a victim with the pretext of developing a relationship in the guise of an attractive personage or political ally (Watts 2018, 85). While there are many other methods that might compromise the system, the above gives a good idea of the wide range of possible vulnerabilities of an organization, both physically, socially and digitally.

5 Development suggestions

Human behavior is difficult to predict, therefore forming a significant risk factor. Clear directives should be made regarding information security and the handling any form of IT-system. There should be oversight regarding the actual dissemination of information in the organization, making sure that the principles of information security are understood, and people are aware of their role in the organization’s security culture. With more individualized training to identify phishing messages and the like, it will be possible to build defenses within people and

change their habits improving the cybersecurity of an organization. This method will also make the organization far more resilient towards social engineering attacks (Vishwanath 2016).

Physical access to the IT-systems must be carefully monitored. This includes the entire spectrum of physical security solutions from proper access control, to the design of physical obstructions such as doors. One method of testing their effectiveness is physical penetration testing or pentesting, which can reveal various security faults in the organization (Red Team Secure 2019).

Due to the relative recency of blockchain's arrival on the tech scene, threats are hard to predict for it specifically. New developments in their vulnerabilities must be monitored. While threats like the mentioned "51% attacks" are at the current moment mostly a theoretical possibility, the development of such new technologies can possibly bring out unexpected developments in the form of glitches creating accidental harm or exploits utilized by nefarious actors. These would be the technological equivalent of black swans, an unexpected development that is extremely hard to predict.

The contractual and legal issues create a practical problem for the system, namely in the form of trust. The large data requirement makes bilateral (or multilateral) contracts untenable as any kind of agreed upon contract cannot take into account future needs (changes, additions etc.). This necessitates the ability of a content creator to control what information is displayed and to whom depending on their role and in terms of the individual user. These issues culminate in the operator of the system itself and their access to the information they oversee. Social media sites such as Facebook or services like Discord allow for the relative control of information by excluding specific groups from seeing certain parts of published content, although they do not solve the operator problem. Especially Facebook has been found to have handled user data poorly, and whether through negligence or otherwise, has managed to spread the data to places it does not belong (Eidelson & Frier 2019).

6 Conclusions

The system that is going to become the CBE is a work in progress, therefore any kind of research done at this stage will have to be reviewed and updated as time goes by. The inherent nature of the Internet as insecure (Cavelty 2016, 401), will also create questions about the future and what kind of form the system will be taking in time. While none of the risks faced by the CBE are unique as far as digital systems go, they could morph into something different.

Social engineering is very unlikely to go away as it exploits fundamental weaknesses of human behavior. Habits and other forms of ineffectual cognitive processing have been identified as

the main driver of individual victimization (Vishwanath, Harrison & Ng 2016,1). Whether this vulnerability can be fully eliminated is still an open question.

The emergence of blockchain has opened various opportunities in both the realm of security and its reverse, insecurity. As stated before, many of these threats are emerging and therefore unknown. However, the more common the adoption of the technology is, the more it needs to be brought into focus in organizations planning to utilize it.

More research will be required to create a more comprehensive picture of the vulnerabilities of the system, especially concerning the limitations of this work. This includes the actual risks inherent in the used software and hardware. With the revelations of such happenings as the alleged hardware hacking of Apple and Amazon (Robertson & Riley 2018), the threats involved are evolving.

The CBE has significant competitive potential as stated earlier in chapters 1 and 2, opening a flexible and secure way of transmitting information from one member of the network to the other. Multilateral contracts are complicated and hard to manage, so a system with the flexibility of control as suggested earlier can both justify its cost and existence. Especially if a larger investor can see themselves gaining competitive edge in the digital age.

7 Self-reflection

For the writer, this thesis has been a challenge in more than one way. A major issue was learning new things about emerging IT-systems, which in their technical specifications would have required a different skillset entirely, focused heavily on software and hardware. However, this also allowed exploration into the “softer” area of information security, which is social and cognitive dimensions mentioned earlier in this thesis. It was also somewhat surprising to find how deeply ingrained certain automatic actions are in the human brain, to allow for bypassing general critical thinking.

Another area of learning was the challenge of fitting together with a larger network of stakeholders and finding common ground. As Chapter 5 and 6 discussed, at a certain point the complexity of a contract is so high that alternate means of cooperation must be found. While standards are helpful in this regard, rights of stakeholders become paramount necessitating a degree of innovation.

Finally, while internal documentation helped clarify the idea of the system in concrete terms, this thesis had to work in the abstract as well. It has been a challenge to piece together various threads of inquiry to create something that would be helpful for the purposes of the client. In this regard, despite the limitations created by the scope of this thesis and the other challenges already mentioned, the writer found that it is possible through keeping in mind the needs of the client.

References

Printed sources

Bamfield, J. 2014. Security and Risk Management. The Handbook of Security, 2nd Edition. London. Palgrave Macmillan UK.

Brooks, D. & Smith, C.L. 2014. Engineering principles in the Protection of Assets. The Handbook of Security, 2nd Edition. London. Palgrave Macmillan UK.

Cavelty, M. 2016. Cyber-security. In: Contemporary Security Studies, 4th Edition. Oxford. Oxford University Press.

Hart, Chris. 2018. Doing a literature review: Releasing the research imagination. Sage Publications Ltd.

Heaton, J. 2008. Secondary Analysis of Qualitative Data. The SAGE Handbook of Social Research Methods. Sage Publications Ltd.

Ridley, D. 2012. The literature review: A step-by-step guide for students. Sage Publications Ltd.

Taylor, S., Bogdan, R. & DeVault, M. 2016. Introduction to Qualitative Research Methods: A Guidebook and Resource. New Jersey. John Wiley & Sons, Inc.

Watts, C. 2018. Messing With the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News. New York. HarperCollins Publishers.

Electronic sources

Ahokangas, P., Lehtimäki, T., Helaakoski, H. & Peltomaa, I. Collaborative Business Networks of the Future. 4.5.2015. Accessed 15.10.2018. https://www.researchgate.net/publication/275524666_Collaborative_business_networks_of_the_future

Altman, I. How Blockchain Will Change Business and the Law. 29.6.2018. Accessed 25.9.2018. https://www.forbes.com/sites/ianaltman/2018/06/29/blockchain-changes-business-law/#3e8004cc5cb9

European Union. General Data Protection Regulation. Accessed 20.10.2018. https://gdpr-info.eu/art-37-gdpr/

Chima, R. Cloud Security – Who Owns the Data?. 19.9.2016. Accessed 28.2.2018. https://www.bbconsult.co.uk/blog/cloud-security-who-owns-the-data

Frier, S., Day, M. & Eidelson, J. Millions of Facebook Records Found on Amazon Cloud Servers. Accessed 22.04.2019. https://www.bloomberg.com/news/articles/2019-04-03/millions-of-facebook-records-found-on-amazon-cloud-servers

Gray, D. Data Ownership in the Cloud. 14.3.2014. Accessed 28.2.2018. http://datacon-omy.com/2014/03/data-ownership-in-the-cloud/

International Organization for Standardization. 2018. ISO 31000:2018. Accessed 5.5.2018. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Ismail, N. Why 'data hoarding' increases cyber security risk. 30.3.2017. Accessed 15.10.2018. https://www.information-age.com/businesses-still-taking-risks-back-123465440/

Linkov, I, Eisenberg, D., Plourde, K., Seager, T., Allen, J. & Kott, A. 2013. Resilience metrics for cyber systems. Accessed 5.5.2019. https://www.researchgate.net/publication/263176904_Resilience_metrics_for_cyber_systems.

Loch, K. D., & Warkentin, M. E. 1992. Threats to Information Systems: Today's Reality, Yesterday's Understanding. Accessed 24.10.2018. http://home.business.utah.edu/actme/7410/ME%204_15_02/Loch%20Carr%20Warkentin%20MISQ%201992.pdf

Miles, C. Blockchain Security: What keeps your transaction data safe?. Accessed 28.8.2018. https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

Morrow, S. 2018. Security vs usability a conundrum in modern identity management?. 3.7.2018. Accessed 10.2.2019. https://www.csoonline.com/article/3286609/identity-management/security-versus-usability-a-conundrum-in-modern-identity-management.html

Woods, L. Data Retention and National Law. 21.12.2016. Accessed 28.2.2018. http://eulawanalysis.blogspot.fi/2016/12/data-retention-and-national-law-ecj.html

Statista. Bitcoin blockchain from 2010-2018. Accessed 28.8.2018. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Van Wirdrum, Aaron. Bitcoin Unlimited Miners Maybe Readying a 51% Attack on Bitcoin. 29.3.2017. Accessed 28.8.2018. https://bitcoinmagazine.com/articles/bitcoin-unlimited-miners-may-be-preparing-51-attack-bitcoin/

Red Team Secure. Physical Penetration Testing. Accessed 14.02.2019. https://www.redteamsecure.com/physical-penetration-testing/

Robertson, J & Riley, M. The Big Hack: How China Used a Tiny Chip to Infiltrate America's Top Companies. 4.10.2018. Accessed 15.10.2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Roche, J. Cloud Computing: Legal Issues. 12.4.2016. Accessed 26.9.2018. https://www.researchgate.net/publication/301222790_Cloud_Computing_Legal_Issues

Santa, M. Differences Between Internal and External Threats to an IT Database. Accessed 5.5.2018. http://smallbusiness.chron.com/difference-between-internal-external-threats-database-74165.html

Social-Engineer LLC. Accessed 15.10.2018. https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Statista. Bitcoin blockchain from 2010-2018. Accessed 28.8.2018. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Turner, M. The Human Element of Cybersecurity. 26.5.2015. Accessed 26.9.2018. https://www.securitymagazine.com/articles/86387-the-human-element-of-cybersecurity

Vishwanath, A. Cybersecurity's weakest link: humans. 5.5.2016. Accessed 24.10.2018. https://theconversation.com/cybersecuritys-weakest-link-humans-57455

Vishwanath, A., Harrison, B. & Ng, Y. Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. 10.2.2016. Accessed 24.10.2018. https://www.researchgate.net/profile/Brynne_Harrison/publication/278676335_Suspicion_Cognition_Automaticity_Model_SCAM_of_Phishing_Susceptibility

Whitman, Michael E., & Herbert J. Mattord. 2011. Principles of information security. Accessed 24.10.2018. https://books.google.fi/books?id=L3LtJAxcsmMC&pg=PA1&hl=fi&source=gbs_toc_r&cad=4#v=onepage&q&f=false

Unpublished sources

Collaxion PowerPoint

Collaxion Internal Communication

Figures