# Inforation Security: Panacea becoming Malady

## Abstract

According to Gartner, information security spending is estimated to reach $2.77 trillion for the year of 2016. The spenditures are going higher every year, as public and private organisations face increasing amount of threats. New security concern arise as technological innovations drive society further. Internet of Things, Digitalisation of services developments in the mobile field, just to new few, are molding modern society. Information security is called to protect the previous; some would like to argue they enable them. Previously, research has usually taken a singular approach, dividing information security field into social (or user-centered) and technical (hardware, software, networking) sides. A small portion of research has been devoted to things that are not operational, or the information security making. Such topics include standards, regulations and laws, economic and so forth. We argue that information security cannot be fully understood, unless a serious attempt to look at it as an entity is undertaken. Acts of users have an impact on technical security controls, security awareness training (perhaps deriving from regulations) affect users, technology affects users and so forth. In fact, research molds all of these, as new knowledge propagates into every corner of information security making. Our research views information security as a practice in flux, changed by outside forces. Therefore, we argue it is vital to understand the entirety of how information security is done, so we can analyse it. We reviewed several different topics and their research and came to a conclusion that lots of the underlying cornerstones go unchallenged. Our aim is to give it a new reading, analysis and further research based on those analyses.

In this research, we want to question information security with multi-disciplinary lenses; we will analyse the social impacts, what information security does to its users, and tie it to the more traditional information security, or technical part. We argue, that information security should be looked from the view of what it does – which has largely gone unnoticed – and the way increasing complexity might, under certain circumstances, make systems, or data, less secure. This is our main theme we will examine with all our individual studies and we seek to show that once we understand the underlying complexities, we then understand that by adding more complexity does not necessarily equal better security. Essentially, if the target system is complex enough, it is difficult to defend against unauthorized users.

We will take the concept of anomaly, and use it as analogous to the term abnormal (lisää liite) from social psychology. In the process of sense-making, we are tempted to categorise, which in essence is a method of exclusion. Exclusion is done when we can find something that is normal and abnormal. Scientific literature and knowledge will provide us the tools for proper categorisation, or exclusion, for example in the case of mental illness (liitteet, tästä lisää omassa kappaleessa, kantaa läpi väitöskirjan). Logically, then, we can analyse information security via anomalies as well. What does normal network traffic look like. Is this machine behaving normally? Is it affected with a piece of malicious code, making it behave strangely? Code, and users can act in malicious ways, based on their actual states and intent. We are not going to dwelve deep into the world of signs and language used in information security, but the concept of normal/abnormal is a key concept.

Our concept has far reaching ramifications; we are excluding users, code, hardware from the space of normalcy, so the power of information security research is far reaching. With the new knowledge reached, the state of normal is created. Throughout this research, we consider all parts of information security as mere actors, or components of a larger machine that does security.

Starting from simple detection of anomalies, we can analyse the entirety of information security in a new way, that leads us away from the frameworks and closer to practices as well. Detecting a possible attacked, what is going on in that situation? In human interaction (in the case of social engineering) or human-machine interaction, where the analyst is trying to sort through data from controls to decide whether an attack has taken place. However, to get here, we must first take apart information security, conceptualise and give it a new reading.

Previously, information security research has been conducted under principles that have been taken *as is* – CIA triad (Confidentiality, Integrity, Availability) of information. We do not seek to argue against the goal, however, we intend to show its means of achieving the goal to be often paradoxical, and often causing completely new problems that escape, as practitioners and researchers alike seek to create a more secure digital world.

We will take snapshots from three different aspects and analyse them rigorously, with each having their own contribution to the field of information security research. We will start with our own analysis of social engineering, as it is the starting point of our narrative. ”User is the weakest link” is one of the most popular opinions there is in the field. We see this as a good starting point, as it seems to be a popular topic, and yet we know very little about it. Starting from ”the human factor” also provides us an opportunity to contribute to the body of knowledge, which is not large at the moment. If social engineering is the biggest problem in information security, then understanding the phenomenon is very valuable, as the field leans on more technoloy-based solutions. Second, we will conceptualise information security, so we can better understand the relations between users and technology. Third, we will seek to find paradoxes in security, based on findings before. We argue, that adding more information security does not necessarily result into a more secure environment.

If we trivialise information security and reduce it to mean technology, we are left with a group of controls, cryptographical algorithms and detection and monitoring tools. But, attackers evade controls, dupe users, and simply take advantage of an opportunity, it follows that we need to include people as well. We simply cannot trivialise security to mean users, either. To have a better understanding, we need to seek a more overarching way of look at what it does, and what it is becoming. As the world is constantly changing, so is information security, in constant flux, where everything is connected to something. Fourth, we will seek to understand the technology itself; is more security technology always better? In order to detect a possible intrusion in a network, is it conceivable to go with a single solution for singular view? Or is it better to stack up and have a variety of views. This will be our fourth research, which will finish the research.

## The Human factor: (published)

Social engineering (SE) relates to cons and frauds taking place in both the digital and analogue worlds simultaneously. In the example above [**in the original paper**], the digital account is intruded upon in part through a conversation over the telephone. Mitnick *et al.* (2003) have argued that SE uses the weak human element to bypass technical protection. Even if SE mixes the social and the technical in interesting ways, we are still lacking a critical analysis of SE. Instead, what we seem to have is a cloud of myths which linger over it. From time to time, SE is seen as a magical event in which indi- viduals suddenly find themselves to be mere puppets of the attacker. For example, descriptions of SE techniques such as neuro-linguistic programming (NLP) (Barrett 2003,

Hadnagy 2011), manipulation (Gragg 2003, Manske 2000, Allen 2006), and flirting (Schifreen 2006) contribute to per- ceptions of the mystery and trickery behind SE. Mitnick *et al.* (2003) reinforce the mystery of SE by entitling their book on the subject *The Art of Deception* (cf. also Thorn- burgh 2004).

In a sense, SE is presented as the shadowy art of mastering the secrets of manipulation. Furthermore, there is also another side to the issue as it is claimed to be a common occurrence (Power and Forte 2006). In addition, the consequences of any given SE incident are clear, as SE causes evident damage to companies – though again, the exact value of the damage caused may often be difficult to evaluate. Moreover, companies possess an insufficient understanding of countermeasures, having little or no effec- tive defence against SE (Power and Forte 2006). All in all, this forms a peculiar equation combining fascinating elements – manipulation, deception, information systems, everyday life, and considerable damage – and it all takes place in the realm of the global business world.

With the above in mind, we took as the starting point for this article the question of what is known about SE: what has been studied, how the events are depicted, what techniques of intrusion – as described in the literature – social engineers use, and in what ways the success of SE – i.e. why victims fall for it – is explained in terms of theory. In order to find previous studies on SE, we reviewed a body of literature we found on the topic, including, journal articles, conference papers, and white papers, in the timeframe 1996–2008. In addition, we examined some of the more current texts to see if they seemed to provide anything new to the corpus. As a result, 40 SE articles and texts were found and analysed as data.

All in all, this article has three goals. First, it seeks to create an analytical and critical concept of SE and its socio- material connections on the basis of what is said about SE. The second goal is to gather all the individual acts – imag- ined and real – that are mentioned in the literature to describe the methods – the techniques of intrusion – used by the attacker. We seek to analyse these techniques of intrusion so that we can grasp the different aspects of SE. In order to understand the multiplicity of SE, we need to identify the functional dimensions which the techniques can manifest. The third goal is to discover how SE has been studied; we are particularly interested in the empirical evidence in SE stud- ies and the studies’ theoretical underpinnings. Moreover, we seek to analyse the difficulties and significant pitfalls previ- ous research has faced, and how it has failed to capture SE in its entirety in the current design of its research and explana- tion. Instead of discussing SE in terms of mere individual techniques, an approach adopted by many other authors, we need to acknowledge that each technique can carry out different functions. It is these dimensional functions that matter in explaining various kinds of attacks through differ- ent theories. The functional dimensions – not the individual techniques – require their own theoretical approaches in order to be analysed and understood.

We will start with a conceptualisation of SE. This will allow us to describe the stage at which SE takes place, and some features of SE. We will then go deeper into the actual techniques of SE – what the intruder’s toolkit looks like – and construct the dimensions of these techniques. In Section 4, we will analyse theories and evidence used in previous research in the light of our conceptualisation, which is based on these dimensions. We will discuss problems relating to the areas on which the emphasis has been placed previ- ously and point out what is lacking in the current literature. Finally, we will discuss the implications that our framework has for SE research and propose future research paths.

We concluded, that in the SE literature, SE has hitherto been presented in a disorganised manner: the phenomenon has been described through a number of individual cases and techniques which – without any overarching analysis – have then been placed under the fuzzy concept of SE. In this article, we have sought to bring order to the concept, and so enable research to be improved.

We have found that individual techniques were mislead- ing as an attempt to grasp the diversity of SE in its entirety. By analysing the SE literature, we have been able to extrap- olate three dimensions – persuasion, fabrication, and data gathering – from the individual techniques. Each dimension performs a different function, and this could not have been perceived if attention was paid solely to a single technique.

In terms of theory, the advantage of a multidimensional approach is also demonstrated when SE studies are reviewed. The research tends to overemphasise the dupe’s role and ends up explaining the success of SE in terms of the psychological features of the dupe. This type of explanation covers, at best, the dimension of persuasion, but not fabrication or data gathering as these two dimensions have very little to do with the dupe’s psychological traits. The studies we reviewed which included empirical evidence explained the success of SE attacks through personal traits, but these attacks should have been analysed from a multidimensional viewpoint rather than treated as merely one-dimensional attacks (using the dimension of persuasion). In this manner, our multidimensional approach provides an opportunity to reconsider and a chance to elaborate on the explanations of the studies.

However, even at this stage, they have proven to be useful as the frame analysis has encouraged us to pay attention to the dupe’s interpretation of the situation and actor-network theory has led us to think of actors beyond the intruder and dupe. Evidently, these theories need to be explored more closely in terms of SE research. Still, they have already shown themselves to be useful.

Furthermore, in future research, the variety of SE should be recognised: attention should be paid to all the dimen- sions and all the phases in the attack as a whole, or these should at least all be acknowledged. In addition, future research could, for example, study how an organisation can develop better work flows and technology that allows the user to comply with the security policy without, for example, having to compromise the organisation’s focus on customer service. Any form of SE analysis which uses our multidimensional approach and understands that the event usually involves more than a mere intruder–persuasion– dupe framework will then provide more insight than one in which the dupe is seen as the weakest link.

## Capturing information security as an actor: (published)

In this paper, we develop a philosophy of information security, a manner of approach that discusses the ontology of information security. More specifically, we delineate the ontology of information security to provide a point of view from which new research subjects can be suggested. Most of the existing research literature on information security is driven by practical aspirations. Scholars have focused on questions of improvement; for example, on how to develop information systems so that they are more secure, or on how to prevent the abuse of the systems (Baskerville, 1993; Dhillon & Backhouse, 2001). In these undertakings, the concepts of confidentiality, integrity, and availability (CIA) have played a major role because scholars have viewed these as the chief objectives of information security (e.g., Dhillon, 2007; Stanton & Stam, 2006). Nonetheless, despite those studies that focus on CIA as the objective of information security and on how they are achieved in practice, information security in and of itself – the question of what it is ontologically – has remained largely unexamined (cf. Pieters, 2011). In this paper, we examine the ontology of information security to depict what information security is and what it does or, rather, to depict what it is through what it does. That is to say, we commence from the idea that information security is not a neutral entity; that is, it is not additional to or parallel with information systems but is in itself active and productive.

Information security has become a part of everyday life. Organizations use significant quantities of resources to build up a sturdy information security system. Users in organizations and at home invest time in carrying out practices related to information security; for example, entering passwords and pin codes, updating software with the latest security patches, and dealing with suspected phishing emails. Moreover, as new technology is introduced, new security issues arise (e.g., viruses, mobile phone theft). Thus, information security is a transformative and pervasive entity.

Due to the ways in which information security territorializes different spaces (from homes to large organizations), interrupts threats (e.g., to keep information available only to authorized users), and connects users (e.g., a user connecting to an email account through information security), we believe that utilizing Deleuze and Guattari’s concept of the machine and territory in order to grasp some ontological features of information security is productive. The ontological approach – that is, the description of information security’s material and conceptual functions – questions whether information security is a mere protector of information. In other words, we argue that information security goes beyond its role of providing CIA because through its activity it increases the complexity of the system in which it is implemented. An ontological analysis reveals these additional roles. For example, information security can be problematic when it comes between a user and information, when it requires constant updating, or when those who use it require constant education. Moreover, by employing the concept of the machine and analyzing territorial, spatiotemporal features of information security, we develop new concepts and connections that reveal different aspects of information security and provide help with the future analysis of information security as a productive actor. This conceptualization provides a possibility for a new research problematization in which information security in itself is seen as a problematic actor as it comes between a user and a system. Through this problematization and through the future research that can be generated by it, we can improve our understanding of information security.

We introduce the concept of the machine, and explore machines in information security and how everything that becomes connected to information security also becomes subjected to it. Moreover, we claim that individuals become modified by this subjection.

we analyze the territorial nature of information security in spatial and temporal terms. Information security never exists in a void but always requires a material medium (data territory) and agents to achieve the order that it seeks. The agents, who organize safe zones in which data territories are situated, also exist in space and time. We also look at how another spatial category, the perimeters between the inside and the outside, connect or entangle with each other in information security.

In conclusion, we argue that information security is, ontologically, an order-preserving and producing socio-techno- material machine that is a multiple, connective, territorial, subjecting, and transforming interrupter and producer. The security machine harnesses and subjects agents so that the combination created is able to carry out its task of interrupting chaos. Information security is an order-maintaining rhythm machine. Its main goals are to maintain the order of information written on a medium, and to maintain the order of surrounding territories – the safe zones. The constant becoming – the emerging connections and disconnections of the machine and its targets – makes the entire constellation transformative, which may send this precious order back to chaos.

In the task of creating an order inside the system, information security interrupts the agents inside. However, the security machine is not a mere interrupter but a mediator. It makes the outside and chaos relevant to the order of information. Through passwords and user names, the security machine produces a relation between the system and its users. The security machine is all about the purification of the outside and the organization of the inside. The aim is for chaos to be left outside and the elements brought inside to be purified. However, there is always noise: while information can theoretically be pure at the level of order, it can never be pure when it is written on a medium because the noisy material medium becomes part of the information. An inside cannot be completely purified because it is built out of elements of the outside; the only difference between the elements lies in their order and organization. Information security is an order itself, but it is not without impurities. Chaos gets in. In fact, chaos is invited in by the security machine, which itself comes from the outside as an addition to the information system. As information security is an active entity, we propose that its effects on other agents inside the system should be studied. In this paper, we introduce concepts that could be used in such research.

## Information security as a paradox: (published)

We approach information security from a novel perspective as we examine its unintended ramifications and its paradoxes. Information security and cybersecurity are necessities of modern societies. Simply put, services which are based on information and communication technologies would not function without information security. Thus, information security can easily tend to be thought of in only positive terms, as it ensures and facilitates our way of life. Furthermore, people rarely complain of information security being *too* sturdy. So the case between Apple and the FBI, in which the FBI finds the robustness of security in the iPhone software problematic, is an uncommon case. It is much more common for problems pertaining to information security to be related to vulnerabilities and weaknesses in information security.

However, there are many paradoxes that come with information security. Fundamentally we argue that information security seeks to exclude interruptions to the system it protects, yet it  
is in fact itself an interrupter that makes the system different. First we describe information security in general, along with its significance in terms of the functioning of society. In other words, we go through the positive side of information security. Then we discuss information security in a slightly more theoretical manner. Our purpose is to discover what in fact information security is by looking into what it does. Then we start to go through its paradoxes.

Security is often often taken solely as means to protect data. To assure proper information security, even this manner is not so trivial; Security is based on relations and ownership. It is a question of who the authorized user is, who has ownership of certain information and what the authorized user desires to do with it. Because security is connected to users’ desires, it means that there is no way of knowing, for example, whether the structure and status of certain files is secure or not merely by examining the files themselves. In other words, by looking at the registry, files, and processes of a computer, you cannot say whether the computer is secure or not. In order to assess how secure something is, you need to know what the owner of that computer wants, what he or she desires.

Let us clarify this through an example. Think of a text file that you have written and saved on a mass storage device. Later, the file is erased and the text is gone. The question is: is this a good or a bad thing? Did deleting the file serve information security? There is no way of telling whether the action is benign or malicious without knowing what the owner of the file wants. Again, this assessment cannot be based on the mere status of the file (deleted, not deleted); the user’s desire (and/or organizational information security policy) has to be included. However, and importantly, the external desire is not an absolute in the sense of always being the same. Of course, users usually resemble each other, which makes users’ desires sometimes look as though they are absolute and universal. For example, most email users do not want to receive spam. However, conceptually, desire is always open. Despite the relativity of security, we can define information security by what it does; namely, it protects the order of relations Thus, in our example above, information security seeks to protect the relation between the user’s desire and the file. In the larger context of a modern society dependent on information systems, this means that there is a desire to ensure that information systems function smoothly (which is one objective of information security).

Let us move to the actual paradoxes. As we have discussed, information security seeks to prevent systems being interrupted. For example, information security makes sure that monetary transactions are not interrupted. However, paradoxically, information security itself works through interruptions. As it prevents external interruptions, distortion and distraction, it in fact generates them. For example, one such interruption generated by information security is the request for a password and user name Use a web-based service and you are asked for credentials. In simple terms, this enquiry is a stoppage, an interruption. The user is cut off from their normal flow of action. The same applies to security updates which require a restart of the system. Interruptions due to a restart occur on a frequent basis.

Of course, it can be argued that the system can be made to remember passwords. The fingerprint scanner can be deactivated. The entire system can be configured in such a way that no passwords are required. However, as the energy drain is avoided, the level of security is also lowered. Alternatively, the interruption has changed its form. If a program that remembers the passwords and hides them behind a master password is used, then interruption comes in the form of the installation of that program. In addition, this program then consumes some of the device’s resources.

Information security is based on analysis and control. However, every analysis is an interruption in itself. The interruption of information security is not pointless or random but overarching: interruption concerns all the entities that come into contact with the system that is under protection. Every entity is analyzed and interrupted. It makes no difference whether you are a legitimate user or a malicious hacker. Both are analyzed. Equality is generated in a strange way. The difference comes after the analysis. Then, the user is either authorized (allowed use of the system) or rejected (denied access).

Information security functions as a maintainer of order. However, paradoxically, in order to keep the existing order of the system, the order is altered by information security For example, a security program installed on a system reorganizes processes and reroutes the flows of information within the system that it protects. In order to monitor network traffic, an additional loop is required. In order to keep viruses excluded, a virus scanner is installed. However, these all drain energy – processing cycles – from the actual system. Information security seeks to protect an order, yet it changes that order. In order for network traffic to be analysed, encrypted packages have to be decrypted first, darining resources, creating a possibility of serious security flaws in case of faulty implementation of such techniques. In fact, it is a paradox in itself to make plaintext out of once secure information. In other words, to provide security in the terms previously understood; once we look at it from the security machine perspective of interruptions – it follows that adding more security can actually lower the level of security – at least in terms of controls evading encryption, and creating new anomalies for analysts trying to sort through the network traffic.

To put it slightly differently, information security is a reorganizer, an additional element that adds complexity to the system. In order to protect information and information systems from distractive and interruptive entities, information security establishes an order that is always distractive and interruptive in terms of the main functioning of the system. Usually the interest has been in how malware, for example, slows down computers. In the modern age, malware has also taken a more insiduos developments, as they are being used to infiltrate target systems for corporate and nation state espionage to criminal gangs around the world. Increasing coplexity in the world of malware puts new challengers for information security needs.

A simple example illustrates the situation from the paradox point of view; one of the constantly problematic applications, such as adobe reader, is statistically a hotbed of vulnerabilities , it still has to function with its own formats. In other words, it parses one format. Whereas anti-virus has to understand all formats, or dismiss the ones it cannot parse. So, logically put, anti-virus products are bound to be unreliable and also vulnerable for the unseeable future, unless the logic changes altogether.

Another simple example, that is very complex when it has to be dealt in real life; security controls are often based on some sort of protocols, such as TCP/IP (documented in RFC 791). The infamous Ping of death exploits the fact that a correctly sized packet has been pre-determined and the controls that handle network traffic were also designed to follow those rules. However, attackers can misuse weaknesses found laid out in protocols and cause havoc. Therefore, protocols have to be secure, whereas they are not often designed for all the future attacks in mind, that a clever and malicious attacker hatches in his or her own mind.

Fixing these issues for firewalls and other vastly and globally deployed devices is not a small undertaking. The paradox in here is that the very controls that were supposed to protect become targets, and might eventually render the original intent of operation unavailable. The previous examples imply that the preconditions (perfect protocols, hardware, software and deployment and usage of them) to predict future is unrealistic and there is a real possibility that in the design and incorrect deployment of information security devices, a great risk exists, and not in the least with the feeling of security.

There is also the world of resources. For instance, absolute and overarching network monitoring would require much more massive machinery than the machinery that runs networks. A great example can be found in the analysis of the EINSTEIN project. The EINSTEIN project was a piece of US government research to see how agency-wide or multi-agency-wide IDS-based (Intrusion Detection System) monitoring could be implemented. The idea of an IDS is that it inspects network traffic and tries to seek for anomalies or known signatures (of, for example, malware). IDS is therefore just a passive snooper in the networks. “The purpose of the 2004 EINSTEIN was to do real-time, or near real-time automatic collection, correlation, and analysis of computer intrusion information. IDSs were to be located at federal agency access points to the Internet.”

The study quickly reached the conclusion that monitoring all traffic is a must if the goal is to detect all anomalies in the traffic. In other words, if one monitors only some of the network traffic, then it would be reasonable to deduce that some anomalous traffic would get through undetected. However, monitoring is very labor-intensive. It consumes resources beyond a reasonable cost. It was discovered that wide-scale IDS-based monitoring would be extremely labor-intensive, unscalable, and would create new security problems. If deployed, it would, indeed, be paradoxical.

Paradoxically, information security hardware and software increase the complexity of a system and in fact interrupt the system and users which information security is supposed to protect. As the systems are initially complex enough, information security can actually make the system so complicated that no one can control it perfectly. Counterintuitively, the tools of control make systems uncontrollable. The paradox is that although security measures increase complexity we cannot live without information security. The problem is that too much security cripples productivity, throughput, and steals valuable processing cycles. Thus, successful information security is about balance, how to achieve a required level of security without losing too much energy.

We do not argue that these controls are bad, or have no place. We argue that it is so complex, that in certain conditions, they can do more harm than good. Essentially, they are the automated tools in the process of helping raising a flag when something seems abnormal. Then, it follows, that such tools, though vital, can also be used against the defenders. In the more severe cases, where attacker resources as seemingly unlimited, it would be reasonable to assume that as those components of control are brought in from the outside, that they might be already doing bidding for others, and functioning in the desire for the attacker, not the defender.

Even less sophisticated attackers can snoop on what defenders are looking for, for example by providing samples to public virus or other services, an attacker can find if his or her code has been detected and if it has a signature. In this example, we want to illustrate that the user’s desire plays a key role, and that it is important to understand, as it has ramifications from defensive point of view as well – informations security controls can be used against their owners, as nothing is truly ever clean.

## Security controls as obfuscators for detection (work in progress, help needed!)

As we have shown previously, information security is an ever inreasing field with multiple lines of direction, foldings, ripple effects, paradoxes and unintended consequences less understood. In the core of information security making as a practice lies the specialist who is in charge of detecting anomalies, the unwanted behaviour of systems. We have established that it is vital to understand information security through its complexity, rather than any singular mode, as it neglects the effects actors have on each other (be it users, hardware, software, processes, regulations, etc.). Therefore, we find it useful to use the security machine, as conceptualised earlier, instead of the traditional frameworks.

We intend to study how adding a new security control to a network affects detecting anomalies in it. To put is simply; we want to seek the conditions where adding a network device will bring more problems than it solves. We will not actually determine what is solving a problem, or what those problems are. Instead, we will add different types of network devices (such as IDS/IPS) to a network and have incident responders analyse situations. We seek to investigate how adding a new component will affect the detection capabilities of an incident responder, familiar with the environment. The outcome of this study will prove the conditions in which a particular control is actually increasing capabilities, and the conditions in which it starts to lose its usefulness.

Our assumptions for this study includes:

1. there is a point when adding a new device will provide better detection capabilities
2. there is a point when adding a new device will decrease the capabilities
3. Every node included in the network will increase complexity

Our third assumption is given, and mathematically (ehkä jotain tähän), we find this to be self-evident.

However, we want to cover the incident responders opinion as well; it is entirely reasonable to assume that a responder is more happier with what is, mathematically more complex – we cannot assume for the person doing the monitoring that it must be more difficult. Instead, we will develop a script for this experiment, that will simulate what is going on in the network, so we can have a steady baseline of activities under control, and monitor the incident responder at his or her work.

Our method of gathering empirical evidence will be interviews after simulated situations. Interviews will be individual, where each added device is asked about. The interview is semi-structured as it allows more questions to be asked, as well as more relaxed environment for personal remarks of the responders.

The experiment will be held in a large Finnish financial institution, with dedicated responders. The devices and scripts will be deployed in the test network, which is close to the actual production network.

Our study will provide unique insight, as well as an unknown outcome that might be counterintuitive. Adding more security does not necessarily mean more security.

So far we have shown that the opposite is the case, and our understanding of information security is compartmentalised and limited. Our technical part of the collection of studies will tie the narrative and prove that

1. information security has very limited chances of success. We show why that is, and the preconditions for better security
2. information security as a field can be understood from a much more simple concept of normal/abnormal and the practice of exclusion, and the problems with that
3. Information security is a paradox in itself
4. The underlying issue is the increasing complexity
5. The solution for better security is going to more simple, as it allows more understandable design (things are allowed to behave in fewer ways), so the control of them is easier (as human cognition is limited).

Our last part of the study will strengthen all the previous studies for this thesis work and provide the research for the fourth and fifth point.