Universiteit Leiden

ICT in Business and the Public Sector

Toward an alignment model for security requirements for medical information processing organizations that are dependent on third parties

Name: Jurre Pieter Sturris

Student-no: S2135744

Date: August 3, 2020

Version: Thesis V1.7.Docx

1st supervisor: Werner Heijstek

2nd supervisor: Mohamed Atef Ibrahim

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University

Niels Bohrweg 1

2333 CA Leiden

The Netherlands

Preface

This thesis is the final step towards obtaining my Master of Science degree in ICT in Business and the Public Sector at Leiden University. This thesis is the product of an endeavor which sometimes never seemed to end.

The last two years I have been focusing more and more on security. Not only within my study at Leiden, but also with different events. The additional summer schools of the JSCU and the NCS3 showed how far an organization can go in securing their information. Therefore, it is especially important to keep a balance between the likely risk and the possible mitigation measures.

Conducting my research was not possible without the help of BDO, therefore I would like to thank them a lot. Although it seems strange, but especially when the pandemic hit, it was good to know that there was a good team with enthusiastic people that I would join in September.

I also want to thank my supervisors from Leiden University, Werner Heijstek and Mohamed Atef Ibrahim, for their feedback based on their own experiences from their respective fields.

And of course, Sebstiaan van Rijn. Without your feedback, our weekly calls, your experience in the healthcare field, and your wisdom in the IT audit field in general, my thesis and future career path would have probably looked completely different. Thank you for helping me!

Jurre Pieter Sturris

Amsterdam

August 3, 2020

Abstract

This research investigates the awareness of general practitioners about the cybersecurity of their websites, which are intended to be used by their patients. This is an important issue as cybersecurity incidents occur more often and at the same time, more personally identifiable information is being shared via these websites.

This research is conducted through a survey distributed among more than five hundredth general practitioners of which 51 responded. A vulnerability scan was performed on 377 websites, the overlapping ones were linked so an analysis could be performed. Afterward, interviews were held to support the conclusion better.

The data suggest that general practitioners do think about the importance of cybersecurity due to the sensitivity of the information. However, the results from the vulnerability scan do not reflect this, i.e. they were substandard.

The conclusion of this study is that to create a secure digital environment, it is important to connect the two worlds of general practitioners well with the world of Application Service Provider. This is best done by making sure both parties have a shared understanding but are not lost in the details.

Table of Contents

List of Figures and Tables

1. Introduction

With the increasing digitization of enterprises, new risks are introduced. When these risks manifest into actions, cybersecurity incidents happen. This will not only have consequences for the company involved, but it will also have a direct consequence for society as a whole (Wetenschappelijke Raad voor het Regeringsbeleid, 2019).

The healthcare sector is also susceptible to these incidents, as shown by the following examples of incidents and the resulting public discussions. Specific attention is given to the small health care institutions of general practitioners as they are prone to dealing with ICT and with their patients on a very daily basis – with the subsequent risks involved.

In two reports by Deloitte, the cybersecurity of Dutch hospitals was examined (Deloitte, 2015; Deloitte, 2016). The findings were that these hospitals were vulnerable, and some systems, not only information technology but also operational technology, were infected with malware. Written questions were asked by members of the Dutch House of Representatives about the seriousness and significance of the matter (Verhoeven & Dijkstra, 2016). The minister of Health, Wellbeing and Sport responded that there were no known cases where medical devices were compromised (Schippers, 2016). In a subsequent inquiry by Women in Cybersecurity (Van Teeffelen, 2017), it was shown that 25 of the 97 hospital-websites had no secure connection.

In November 2018, the Dutch newspaper *de Volkskrant* published that hackers obtained very personally identifiable information (2018). This information came from the website *PratenOnline.nl*, a chat forum where people can talk with professionals about their psychological issues. The data that was obtained included 16,631 chats between patients and psychologists. The site's target audience age was between 12 and 23 years old, who had symptoms of anxiety and depression. The site has been taken offline since the incident.

In April 2019, the *Elkerliek Hospital* admitted that it was successfully attacked in December 2018. A phishing campaign was used to gain access to the mail servers of the hospital. Although the organization cannot exclude completely that the attackers did not look into the patient files on the compromised email accounts, the hospital presumes that this is not the case because of the assumed intent of the hackers (Raad van Bestuur Elkerliek Ziekenhuis, 2019).

Also, in April 2019, the Dutch news organization *RTL Nieuws* published an article based on two whistleblowers (2019). These whistleblowers provided documents by which they wanted to show the irresponsibility of the healthcare sector. These documents came from the child protection agency of Utrecht, named *SAVE*. Due to the discontinuation of an old domain name, the whistleblowers were able to attain this domain. All emails that were still sent, out of habit, to addresses ending with this domain, were confiscated. *RTL Nieuws* counted 3,278 dossiers of 2,702 children of which two-thirds were younger than 18 years old. The records showed complete names and date-of-births, which makes it easy to identify the victims. Among the cases were reports of sexual abuse, domestic violence, psychological issues, and addictions with gaming, drugs, and porn. Because the names were printed on the dossiers, patients could be directly linked to these problems. When leaked, this would have dramatic consequences for the already vulnerable group. Immediately, SAVE improved their processes and systems, and requested Fox-IT to write an independent report to cover the breach and the aftermath (SAVE: Samen Veilig, 2019).

Following the data breach of the child protection agency, a public debate was held. During the debate of the Dutch House of Representatives, a motion was submitted to require the government to penetration test healthcare organizations (Hijink & Raemakers, 2019). This motion has been accepted with a majority of the votes. Minister De Jonge of Health, Welfare and Sport said that he agreed with the motion, but that he was not a proponent of penetration testing all child protection agencies. Because testing over 6,000 organizations would mean too cumbersome of a task for the monitoring agencies.

Besides the external parties that are limited in resources, also the organizations themselves are restricted. Smaller organizations are more often constrained compared to larger ones. This is often because of a lack of awareness, knowledge, or resources (Paulsen, 2016; Kabanda, Tanner, & Kent, 2018). Another key issue is that SMEs do not take cyber risks seriously, as shown by Nycz, Martin, & Polkowski (2015). This absence of attention and a prime focus on their core activities make SMEs an interesting target for cybercriminals. This is also confirmed by the data showing that more and more organizations have to cope with cyberattacks. In 2017, 43% of the healthcare and wellbeing organizations, as defined by the Dutch national institute of statistics (CBS), with 10 to 50 employees have had incidents (Centraal Bureau voor de Statistiek, 2018).

The CBS also shows that only 4% of small-scale healthcare organizations, i.e. 10 to 50 employees, have hired or want to hire IT personnel, compared to 37% at large scale healthcare centers, i.e. more than 250 employees.

Table 1: ICT usage, business sector, -size, 2018

Organization size, number of employees	Anti-virus software (%)	Governance for strong passwords (%)	Authentication by soft- or hard token (%)	Encryption for storing data (%)	Enctryption for sending data (%)	Data in physical different location (%)	Network access control (%)	VPN when logging in from outside (%)	VPN when logging in from outside (%)	Methods for evaluating IT security (%)	Risk assessment (%)	Other measures (%)
10 to 50	97	78	45	38	51	88	46	46	49	40	47	23
50 to 250	100	87	63	47	57	87	52	70	81	57	64	38
250 and more	99	91	88	67	81	93	59	83	91	77	79	63

As shown in Table 1, smaller Dutch healthcare organizations are more prone to not using good basic cybersecurity hygiene measures.

Another issue with cybersecurity is that is has been shown that only the larger incidents have the focus of the media (Gafni & Pavel, 2019) and the Dutch Data Protection Authority (Authoriteit Persoonsgegevens, 2019). Gafni and Pavel found that the information needed for SMEs is not easily found; not in the general media, not on technological and professional cybersecurity sites, and not in academic papers. This is a requirement for good awareness and a better preparedness of SMEs. Reasons Gafni & Pavel give is a deficiency of knowledge at the SME level, a lack of reporting when they do know they have been hacked, no interest by the media, or a lack of public attention due to information overload.

The *Autoriteit Persoonsgegevens* has publicly announced that for now, it will only go after large-scale data processors like hospitals, general practice centers, and care groups with more than 10,000 patients instead of the smaller, often first-line, healthcare providers (2018).

Besides the increase of risk and the lack of required control, general practitioners tend to use more and more information technology to interact with their patients. In a report, 64% of the general practitioners in the Netherlands think online written communication is a good addition to the existing face-to-face contact or contact by telephone (Nictiz & NIVEL, 2017). This has been manifested in part by the implementation of

appointment-planning portals on GPs their websites. In 2017 44% of the websites had this, compared to only 14% in 2013 (Nictiz & NIVEL, 2017). The same kind of increases are seen with the application of electronic consultation, refill prescriptions, and medical information, both about the patient itself and about medication.

The Dutch College of General Practitioners has provided guidelines for their dossier on eHealth (2019). The three points it focusses on, are online services, support for self-management by patients themselves, support for the general practitioner information system. These instructions help general practitioners handle the current trend.

The current trend will even get a bigger boost when the upcoming legislation about patient rights with electronic processing of data will come into effect on the first of July 2020. This legislation requires, among others, that the first line healthcare providers in the Netherlands open up their patient data for the patient itself. This is all supported by government-funded programs called OPEN.

2. Objectives

2.1. Problem identification

As seen in the introduction, there are risks involved when using digital information systems. There is no organization yet that has completely mitigated these so far, while the digitization is still being encouraged. In the Dutch healthcare sector, this encouragement has the form of government-funded programs, while the private sector supports this with innovations like Microsoft's HealthVault and Google's Health. Also, the front-end of the information-exchange with the patients themselves, has the undivided attention of this development, with the introduction of websites, web portals, and apps. Considering the continuous implementation of this kind of web platforms, and the corresponding risks, the controls for information security should be high on the agenda for all healthcare organizations.

As shown in the previous chapter, bigger healthcare organizations have trouble managing this, so the question is how smaller organizations organize this, and especially the general practitioner. The research will be on whether they have specific risks concerning their web sites, and if they are aware of this. And if these organizations are not aware, what is the best way to increase this realization. So, the problem that is depicted here is that there is a discrepancy between what the general practitioner expects and the actual security of the GP-websites to establish a secure environment. This is mainly due to the misalignment of the general practitioner who is accountable, and the application service provider (ASP) who is responsible for implementing, maintaining, and administering the web application.

2.2. Scientific gap

For the potential scientific value, a validated conceptual framework will be created. This framework will be specific for the medical sector. This will be the title of the research: *toward an alignment model for security requirements for medical information processing organizations that are dependent on third parties*. This framework is the main scientific objective of this research.

The additional aim for this research, is to understand the current status of the cybersecurity of general practitioners, and their business & IT alignment maturity. Besides this, another aim is to give general practitioners practical guidelines to improve their alignment, as well as their application service providers.

3. Research Question

Following the previous chapters, a research question and its sub-questions have been formulated.

3.1. Main Question

What is the most fit conceptual framework for creating Business IT alignment within a general practitioner's office in the Netherlands with regard to their website while keeping cybersecurity in mind?

3.2. Sub Question

To answer the main question, multiple sub-questions have to be answered first. The sub-questions are:

1) What is the current cybersecurity status of websites of Dutch general practitioners?
2) How is the general business & IT alignment maturity of Dutch GPs and their ASP currently?
3) How should business & IT alignment maturity generally look like between the GP and their ASP to maintain a secure website

In the next chapter, the literature review will be conducted.

4. Literature Review

In this chapter, the related concepts, theories, and ideas relating to cybersecurity in general, cybersecurity at small organizations, cybersecurity for websites, and risks and vulnerabilities for general practitioners' websites will be examined.

First, the concepts will be discussed and explained which definition will be used for this research. Secondly, the most influential papers will be named. Following this, the relevant theories and models from these articles will be explained, and it will be explained how these can help answer the research questions.

4.1. Concepts

This paragraph will explain the key terms that are being used: Application service provider, Information security, Cybersecurity, Healthcare information security, Web applications, Vulnerabilities, Risks, Threat, and Awareness.

4.1.1. Application service provider

Gartner defines an application service provider as an enterprise that delivers application functionality and additional services to different clients (Application Service Provider (ASP), 2019). For the general practitioners, ASPs provide the design, assist with the governance, and host web applications.

4.1.2. Information security

Information security is defined as "the risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or a system" by the National Institute of Standards and Technology (2012). Von Solms and Van Niekerk describe information security as the aim to safeguard business continuity and lessen business damage by mitigating the effect of security incidents (2013).

4.1.3. Cybersecurity

Cybersecurity is about more than just information security, it is also about protecting those that are acting inside the cyberspace, and their (physical) assets that can be reached via cyberspace (Von Solms & Van Niekerk, 2013).

Another description given by the NIST is "the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems." (2015). The International Telecommunication Union explains it as all the measures that can be taken to protect any cyber asset (2008).

4.1.4. Healthcare information security

The Healthcare sector processes very sensitive information and therefore, information security is even more important for this sector (Magnusson, 2004). Magnusson also provides a historic perspective from a hard copy file to a shared electronic dossier, making it more important than ever to focus on information security due to the scale on which a data breach can occur.

4.1.5. Web applications

Web applications offer end-users from their client-side access to functionality provided on a server through the end-users' web-browser (Erlingsson, Livshits, & Xie, 2007). The Dutch Nationaal Cyber Security Centrum defines it as an application that is accessible by a web browser or another client, which supports the HyperText Transfer Protocol, or its secure version (2015) . While the possibilities are endless, the used techniques are always based on the http-standards as defined in the Request for Comments.

4.1.6. Vulnerabilities

A vulnerability is defined by the Dutch *National Cyber Security Centrum* as a property of a system, that can be abused for unwanted activities (2013). The NIST defines it as *"a weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy."* (2001).

4.1.7. Risks

Risk is defined by the National Cyber Security Centrum as the product of the probability that a undesired events occurs and the damage due to this undesired event (2012).

In information security, it is generally assumed that there are three major objectives to strive for:

4.1.7.1. Confidentiality

"The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit." (National Institute of Standards and Technology, 2001). The United States Code defines it as the preservation of authorized restrictions on retrieval of information (2011).

4.1.7.2. Integrity

"The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation)" (National Institute of Standards and Technology, 2001). Another definition is that it is the need to make sure that information has not been altered and that it is correct and complete (SANS Institute, n.d.).

4.1.7.3. Availability

"The security objective that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data." (National Institute of Standards and Technology, 2001). The SANS Institute defines it as the need to ensure that the functionality of the system can be met and is accessible to whomever need to use it, while the United States Code defines is as "the timely and reliable access to and use of information" (2011).

4.1.8. Threat

The definition of a threat is an unwanted event that could happen due to the use of a vulnerability. When a threat is put into action, it will result in damage to property and/or a disturbance in processes (Nationaal Cyber Security Centrum, 2013). The NIST defines it as the potential for an actor to intentionally exploit or accidentally trigger a specific vulnerability (2001).

4.1.9. Awareness

The realization that what an actor does, can impact the security of the organization's assets (Cyberveilig Nederland, 2019). When this realization is formed, this will influence the behavior of the actor. A study done by Mitchell, Marcella and Baxter showed that a lack of awareness among employees was one of the major information security risks (1999).

4.2. Background

In this section the landscape will be discussed, as well as the data exchange within this landscape.

4.2.1. Industry Landscape

In this section, the Dutch healthcare sector will be introduced and explained. The focus will be on the general practitioner and the interaction he/she has with other parties.

The healthcare sector in the Netherlands accounts for 9.9% of the gross national product in 2018, which resulted in €76.9 billion (Centraal Bureau voor de Statistiek, 2019). With this capital, care is provided to the 17.18 million inhabitants of the Netherlands (Centraal Bureau voor de Statistiek, 2019). This is offered by 343,714 registered healthcare professionals (Centraal Informatiepunt Beroepen Gezondheidszorg, 2019).

4.2.1.1. General practitioner - huisarts

The general practitioners in the Netherlands are part of the so-called first-line healthcare. The first line is the care where patients can go to themselves without a referral (Independer, 2015). Especially the general practitioner has a pivotal role as everybody in the Netherlands has to register themself with a first-line doctor of their own choice. A general practitioner is allowed to establish a diagnosis, to prescribe drugs or to perform surgical treatments, is responsible for adequate record-keeping of the complete medical history and is necessary to endorse referrals to medical specialists. Other first-line healthcare organizations are dentists, physiotherapists, pharmacies, home care professionals, social workers, and psychologists.
If a patient has decided that it requires a professional opinion, he has multiple options. If there is an emergency, he can call *112* for an ambulance, he can call the emergency number of his general practitioner, or he can go straight to the *Spoed Eisende Hulp*. With the first two options, a triage process is done by phone.

When it is less urgent, he can call his GP's office, where he will be connected to a doctor's assistant. The assistant will do a triage process to decide whether the patient needs an urgent visit from the GP, a normal planned visit, a planned consult within office hours, or a consult by phone.
All the medical aid a general practitioner gives is free of charge for the patient, i.e. it is covered in full by the mandatory basic insurance. If an examination or treatment is needed that the doctor himself cannot perform, the patient will be forwarded to a medical specialist; most often connected to a hospital.

General practitioners are normally available at their practice between 8:00 and 17:00. Outside these hours, the *Huisartsenpost* takes over for urgent medical issues, as explained in subsubsection 4.2.1.2.
In the Netherlands, there are 9,798 regular established general practitioners, with 5,028 practices (Nivel, 2017).
There are multiple forms of practices that general practitioners have formed. Most common, 43%, are the duo practices, where two general practitioners work together in a partnership. Solo practices account for 35%, while group practices account for 22% (Nivel, 2017).
The group practices are growing and working with multiple general practitioners has the advantage of sharing responsibilities, being more flexible, and sharing knowledge (Van der Pluijm, 2017).
Although the general practitioner is the axis between the patient and the healthcare, it accounts for €2.999 billion, e.g. 3.9% of the total healthcare budget (Tweede Kamer, 2017).

4.2.1.2. General practitioners center - huisartsenpost

Outside of office hours, the general practitioners work together in 119 regional centers where they can provide care that cannot wait until the next day (InEen, 2016). As discussed in the same report, they provide roughly the same care for patients and will redirect patients directly when urgent care is needed. It is more expensive than general practitioner's care, but less expensive compared to emergency department. The financial benefit for the patient is that it is completely covered by their insurance, while if they go to the emergency department, they may have to pay back part of the cost to their insurance.
Before 2002, general practitioners had a small partnership with around 5 to 8 neighboring practices. This partnership provided emergent care for the whole area during out-of-office hours on a rotating basis. But this was deemed unprofessional and gave an overload of shifts. So, the general practitioners professionalized this partnership and formed clusters of around a hundred general practitioners. With this gathering of resources, the number of shifts a general practitioner needed to do went down, while the expertise and the range of facilities went up (Nederlands Huisartsen Genootschap, 2019).

4.2.1.3. Pharmacy - apotheek

The pharmacist is the professional in the Netherlands who is allowed to give out prescription drugs to patients. Only doctors, and dentists and obstetricians for special drugs, are allowed to prescribe medicines. This separation of tasks is created so the doctors can be as independent as possible from the pharmaceutical industry.

In 2018 there were 1,989 pharmacies in the Netherlands (Stichting Farmaceutische Kengetallen, 2018). In some cases, general practitioners are allowed to have a pharmacy. This is particularly the case in rural areas, where it is not profitable to run a pharmacy for a small population. But when a pharmacy settles within acceptable reach for the patients, the general practitioner has to restrict himself to only prescribe drugs.

The cost for medicines in the Netherlands for 2018 was €4.969 billion, i.e. €289 per citizen.

4.2.1.4. Emergency department - spoed eisende hulp

An emergency department is a specialized unit within 87 Dutch hospitals (Nederlandse Vereniging van Spoedeisende Hulp Artsen, 2019). At these units, no prior appointment is required, and people can be brought in by ambulance, being referred by a general practitioner, or walking in themselves.

The emergency department is one of the most expensive sub-branches of healthcare in the Netherlands. This is because of multiple reasons. First of all, this unit provides a full range of care, with an occupancy of specialized medical staff around the clock. Secondly, missing an indication of a disease is deemed not an option. So extra tests and scans are more common, compared to the general practitioners' center where a more wait-and-see attitude is customary. Besides this, the ambulance, in which patients are transported, cost €611 million for 2018 (Tweede Kamer, 2017). The usage of the four helicopters of the Mobile Medical Team that are on standby 24-hours a day is not included in these costs.

Visiting an emergency department is discouraged by the government because of its cost. So, patients do lose their deductible when they decide to visit the emergency department instead of the general practitioner or the general practitioner center.

4.2.1.5. Hospitals - ziekenhuis

Ziekenhuizen are part of second-line healthcare. Patients can only get an appointment with a specialized doctor once they have a referral from a general practitioner or the *spoed eisende hulp*. This referral principle limits unnecessary visits from patients and reduces the waiting time for other patients and suppresses the cost.

There are 71 hospital-organizations in the Netherlands, with 120 locations. Eight of those hospitals have partnerships with Dutch universities and are called academic hospitals. They also provide specialist third line care (Volksgezondheidenzorg.info, 2018). The price of maintaining this specialized care is €21.660 billion.

4.2.1.6. Home care – thuiszorg

The home care in the Netherlands is set up to support the elderly and care for the diseased at their own home. The municipality is responsible for organizing this, as described in the law *Maatschappelijke Ondersteuning 2015* (Rijksoverheid, 2014). The patient in need can choose their services and products with a personal budget: *persoonsgebonden budget*. This makes sure that there are still some market mechanisms in place.

The nurses that visit the recovering patients, help them with basic care like, washing, clothing, feeding, reminding to get their medicines, and treating injuries (Rijksoverheid, n.d.).

4.2.1.7. Chain care organizations - ketenzorginstellingen

For patients with a certain disease, such as diabetes, respiratory diseases, or cardiovascular diseases, so-called *ketenzorginstellingen* are created in recent years. These organizations provide integrated health care to keep the patient in an optimal condition. A pivotal role again is played by the practice of a general practitioner, where a specially trained assistant is responsible for the continuous management of patients with these chronic diseases.

These organizations support the patient throughout the whole process of disease recognition, intervention, and recovery. Because of the cost-effectiveness of different healthcare providers, the patient is moved to the most inexpensive place for that step in the process. This is called transmural healthcare. To disturb the patient as little as possible, and to streamline the process of handovers between the different organizations, the *ketenzorginstelling* vertically integrates all these steps.

The introduction of chain care organizations has made it of vital importance that information is not being kept in silos anymore. It should be easily accessible and updated in one central place. Since the general practitioner has been the dossier holder, it is being kept this way.

The general practitioner will receive all the status-updates of the patient and will only share the relevant information with the next link of the chain where he sees fit. The general practitioner will not only get feedback from the home care organization (one of the links in the chain care) about the recovery status of patients but also about the psychological state of patients. This is because the doctor can make a better impression of the independence and resilience of elderly patients.

4.2.1.8. Child protection - jeugdzorg

The early years of child development are monitored at specified moments at the pediatric consultation clinic. At these voluntary visits, the neonatal heel prick, hearing test, and Dutch national immunization program are the main points of attention (Rijksinstituut voor Volksgezondheid en Milieu, 2019). This bureau focusses mainly on physiological development.

The other responsibility of the child protection agency is youth protection and youth aid. These are the tasks that support children with staying on the right side of the law and providing a safe environment. When mishaps do occur, children can be placed out of home into a temporary or permanent foster family or a (closed) youth institution. This task focusses more on the support of the psychology of preadolescents and adolescents. In 2018 12.2% of the youth in the Netherlands received some form of support from *jeugdzorg* (Jeugdzorg Nederland, 2019).

The child protection agencies keep a file on all the children they handle. As with home care, the agency keeps the general practitioner up to date. The doctor, however, shares only the minimal required information due to patient-doctor privilege.

4.2.1.9. Public health - gemeentelijke gezondheidsdienst

The public health services in the Netherlands are divided into 25 regions; the same as the regional medical emergency preparedness and planning teams. The main goal of the *GGD* is to protect, control, and promote the health of the Dutch citizens (GGD GHOR Nederland, 2019).

They attain this by performing the task of child health care, environmental healthcare, socio-medical advice, periodic sanitary inspections, epidemiology, health education, and community mental health.

4.2.1.10. Insurers - verzekeraars

In 2006 a new insurance law was set in place by the Dutch government. All Dutch citizens have an insurance obligation, i.e. they have to buy the compulsory basic insurance, *basispakket*, with the option to buy additional insurance, *aanvullende verzekering*. On the other hand, all the insurers have an acceptance obligation for the compulsory basic insurance.

Three cashflows are being paid by the citizens and employers. Those are 1). compulsory basic & optional additional insurance, 2). own risk/deductible, and 3). income dependent contribution.

The fee for the compulsory basic insurance, *zorgpremie*, is around €100.00 per month. Additional insurance can increase this amount to around €250.00 per month to include dental care, physiotherapy, and optician. This fee is decided by the insurers themselves, but they have to guarantee a certain cash reserve, so they will have enough accounting liquidity.

The own risk/deductible, *eigen risico,* is set by the Dutch government and is to prevent unnecessary visits to expensive medical experts. For 2020, this is set at €385.00 (Tweede Kamer, 2019). For a visit to a general practitioner, patients will not lose any of their own risk.

The income-dependent contribution, *Inkomensafhankelijke bijdrage (IAB)*, are the taxes that the government withholds from the salaries of employees. In 2019, 6.95% of an income will be taxed up to a maximum of €55,927.

The insurers get financed in two ways. The first method is by getting paid by the individual citizens as described in the previous paragraph in the form of *zorgpremie*. The second method is by being subsidized by the healthcare insures fund. This fund functions as a risk equalizer, *risicoverevening*. If an insurer has a disproportioned number of high-risk insureds, the insurer will get subsidized by this fund. If an insurer has a disproportioned number of low-risk insureds, the insurer has to contribute to this fund. This fund also receives the income-dependent contribution and an additional government grant: *Rijksbijdrage*.

Citizens with a low income, or no income at all, will get a healthcare benefit: *zorgtoeslag*. For individuals with an income up to €20,500, it is €99.00 per month. This amount decreases gradually and is only €2.00 per for an income between €29,000 and €29,500 (Belastingdienst, n.d.)

The healthcare providers, *zorgaanbieders*, are compensated in two ways. First, in the form of an availability remuneration, *beschikbaarheidsbijdrage,* from the *healthcare insures fund*. This is done because the Dutch government thinks it is necessary to subsidize particular care centers, even if they are running at a financial loss. This is the case with the trauma helicopters, academic care, and burn centers. The second way of reimbursing the care providers is to pay them directly for their services.

Figure 1 shows major institutions of the Dutch healthcare system, and how it is financed by different kind of cash flows.

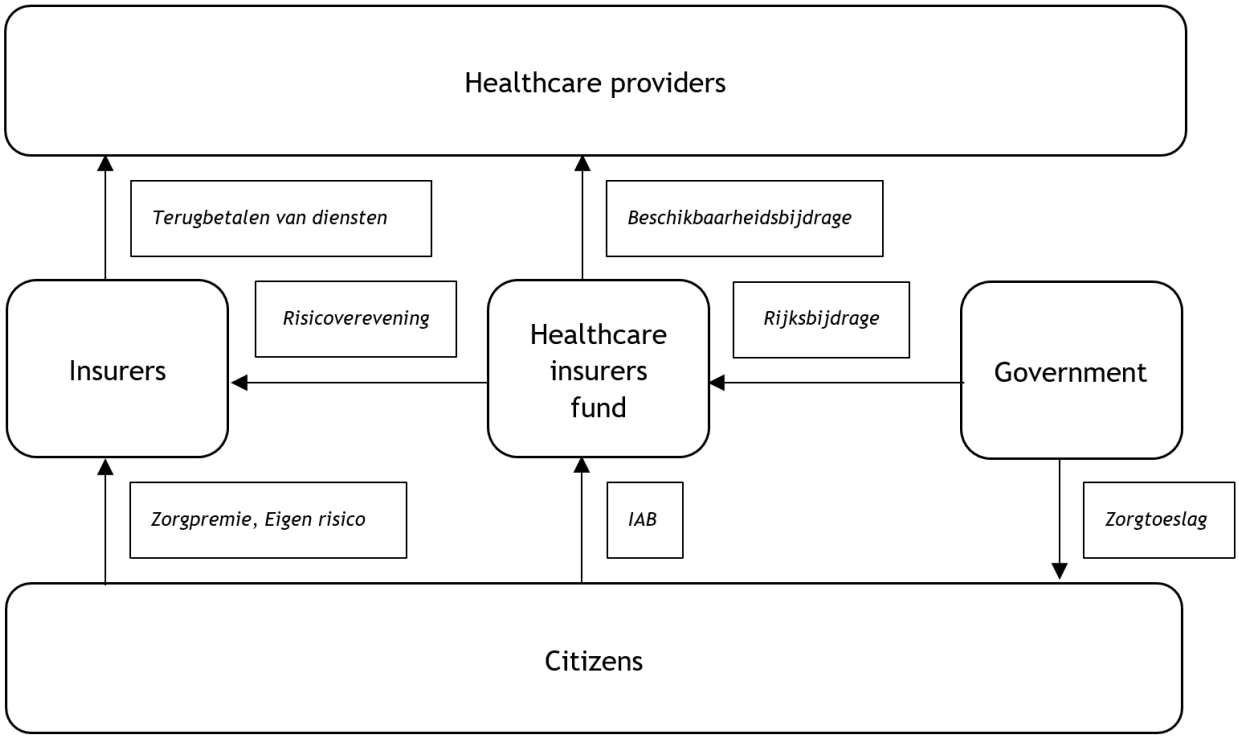


Figure 1: Financing the Dutch healthcare system

Because the general practitioner is covered in full by the *basispakket*, his services will be paid for by the insurers. For this reason, a well-administrated list of performed procedures has to be kept and handed over as proof to the insurer for the declared expenses, and to prevent fraud. These documents contain the patients' name, date of birth, Dutch social security number, received treatments, and obtained medication. It is assured by law that the insurer is not allowed to use this information for anything other than to reimburse the general practitioner, i.e. an insurer is not allowed to use this information to deny a life insurance.

4.2.1.11. Government - overheid

The Dutch government has two important tasks within the healthcare landscape. The first one is to decide what the *basic insurance* has to cover. This decision is based on the advice of the National Health Care Institute. To be included in the basic coverage, the institute checks if the treatment passes the criteria of *necessity*, *effectiveness*, *cost-effectiveness*, and *feasibility* (Zorginstituut Nederland, n.d.). Two committees with external experts are consulted: the Scientific Advisory Committee and the Insured Package Advisory Committee. The first committee's task is to measure its cost-effectiveness, the second one looks for the impact on society (Zorginstituut Nederland, 2017).

With the new budget plans of the Dutch government, the minister of Health, Wellbeing and Sport presents which treatments will be covered, every year in September. At this moment the price of the own risk/deductible and the healthcare benefit is also decided.

The second task of the government is to provide the right legislation. Four main acts support the majority of the current healthcare system in the Netherlands. These are the Health Insurance Act (Zorgverzekeringswet, Zvw), the Long-Term Care Act (Wet langdurige zorg, Wlz), the Social Support Act (Wet maatschappelijke ondersteuning, Wmo), and the Youth Act (Jeugdwet) (Zorginstituut Nederland, 2019).
The Health Insurance Act has come into effect on January 1, 2006. The other three have replaced their preceding laws on January 1, 2015.

4.2.1.12. Dutch National Association of General Practitioners - Landelijke Huisartsen Vereniging

The LHV is an organization that looks after the interest of its 12,000 members (Landelijke Huisartsen Vereniging, 2019). Its main interests are the positioning of the general practitioner in the health landscape, the conditions that give GP-care added value in the healthcare, and to make it attractive for GP's to work.

4.2.1.13. Dutch College of General Practitioners - Nederlands Huisartsen Genootschap

This organization is the scientific society of Dutch general practitioners and has as main objective to promote a scientific grounded general practitioner practice. Over 95% of the Dutch GPs are a member of this organization. It is funded by its members, and the umbrella organization of the Dutch health insurers (Nederlands Huisartsen Genootschap, 2019).

4.2.2. Data

Special attention has to be given to the data, how it is recorded, and how it flows throughout the healthcare sector. The data this sector has is personal identifying information. This data, because it will contain health-related data, but it could also contain genetic or biometric data or data concerning a person's sex life or sexual orientation, is considered sensitive by the European GDPR. In the next sections, the history, as well as the current situation and the future is outlined.

4.2.2.1. History

In 1958, the *NHG* introduces as standard the *NHG-Werkkaart*. This is a green A5-format folder for the general practitioner. On the outside of the folder, there was room to write down the medical records of their patients, while inside there was room to save results from other organizations.
In 1991, the first general practitioner's information system is launched in the Netherlands for Windows (Nederlands Huisartsen Genootschap, 2019). The *LHV* and the *NHG* founded the Council for Computerization and Automation in 1997, to support general practitioners with their transition from analog files to digital workstations. In the early years of 2000, the NHG published multiple guidelines for digital information exchange between the general practitioners and other general practitioners, general practitioners center, and pharmacies, which they updated regularly. In the year 2009, they also publish guidelines about information security.

On November 1, 2008, the national unified Electronic Patient Dossier started, although there was no parliamentary approval yet. A government-funded information campaign was set up to inform citizens of the effects, and the possibilities to appeal being included into the system.
In April of 2011, the legislation was unanimous appealed by the Dutch Senate due to questions about the privacy of the patients and the security of the data. A coalition of five healthcare providers tried to sustain the project. After critical questions in the Dutch House of Representatives, Minister Schippers of Health, Wellbeing and Sport terminated the project in its entirety.

The need for better information exchange was still imminent. Instead of unifying the database itself, another approach was applied. The National Switching Point, *Landelijk Schakel Punt*, was introduced. Healthcare providers were not required by law to use it. It was only made so it could be used.
Another issue with the *EPD* was that patients had to opt-out if they did not agree with the terms. This was tackled by the *LSP* with an opt-in method, e.g. patients had to agree which kind of organizations were allowed to share their files. This created some issues with medical professions, e.g. doctors thought they knew all the medicine a patient had, but he had hidden the organizations that he was embarrassed for.

4.2.2.2. Methods

Within the office of a general practitioner, different kinds of devices and programs are used to communicate and share information with other healthcare professionals. In subsubsection 4.2.2.3 to 4.2.2.9 the current applications are discussed. In subsubsection 4.2.2.10 to 4.2.2.12 the future is outlined.

4.2.2.3. Fax

Although an old device, the fax is still relatively common in the Dutch healthcare system. It provides an easy way for doctors to send results and prescriptions with their signature to the relevant partners.
Because it is point-to-point communication, the medical profession presumes it is a relatively safe way to send sensitive information. Besides this, it also provides an automatic physical reminder to take action.

4.2.2.4. Telephone

The most important equipment for direct communication. It provides instantaneous a clear background of the patient. It is also an important tool because it provides immediate feedback. This is needed if a general practitioner sends a patient to a hospital with a referral letter. A quick call can make sure that this patient will be seen promptly, e.g. with an email the general practitioner is not sure if the recipient reads it at that exact moment.

4.2.2.5. Email

The general practitioners use email to communicate with other professionals. It has been discouraged by the *NHG* to use this method to send personal identifying information due to security concerns. Since the GDPR came into force, the *Autoriteit Persoonsgegevens* has been giving advice to businesses. The advice for the medical sector regarding email is to use it accordingly with the NEN7510 and NTA 7516 norms (Autoriteit Persoonsgegevens, 2019). These norms prescribe that certain technical measures must be put in place because the original email protocols are inherently unsafe (NEN, 2019).

4.2.2.6. Website

With the introduction of the internet, general practitioners also started to publish information on websites. Nictiz, the center of expertise for eHealth, published a report in 2017 about the current state of eHealth. Since 2013, an increase has been seen in all the functionalities. The number of general practitioners that offer the possibilities to create an appointment, to get a prescription, to get a referral, or to have an electronic consult have increased. Although the doctors do think it is a useful addition to their regular care, it has been shown that the patients do not always know that the possibility is there, and even fewer patients actually use the options (Nictiz, 2017).

Besides the more medical-related functions, also administrative issues like change a of address can be communicated from the patient to the general practitioners through a medium like this. In an email conversation, the LHV estimated in January 2020 that nearly all general practitioner's offices had a website that provided functionalities for the general practitioner's patients.

4.2.2.7. Instant messaging

For quick communication between specialists, instant-messaging apps are being used. Because WhatsApp does not comply with the requirements standards, other apps are introduced. These apps focus on the Dutch healthcare market to provide a tool for quick collaboration to discuss challenging cases. The *LHV* has posted guidelines on what to do when conversing with other professionals and sharing images. It has discouraged the use of WhatsApp in favor of other apps like Siilo and AlterDesk.

4.2.2.8. General Practitioners Information System - HIS

Every general practitioner in the Netherlands currently works with a *HuisartsenInformatieSysteem (HIS)*. Here the complete patient history is stored, appointments can be created, and medicines can be prescribed. Also, the financial administration for the general practitioner himself happens in this system.

Hosting a *HIS* can be done in multiple ways. The first one is by hosting the HIS on an own internal server, the second one is by hosting the application on an external server, and the third one is having a hybrid version with having some parts internally and other parts externally.
The benefits of internal hosting are that general practitioners have the feeling that they are more in control, that there are only initial upfront costs, and even when the internet is down, they can continue to operate. The drawback of this is that when the server is off, no one can log into the *HIS*. This makes sharing patients' files with other GPs, when the GP is on holiday, for example, harder. Another point is that off-site backups and redundancy are harder to maintain.

The potential benefits of hosting it externally are that there are redundancy measures in place and good cybersecurity practices and sharing of information is easier. The disadvantage of hosting it externally is that a monthly fee is charged, and a reliably fast internet connection is required.

A general practitioner, interviewed for the healthcare landscape, had a hybrid solution. The general practitioner mentioned that his practice stored its HIS in the cloud, while the referral letters and other correspondence where saved on their own server.

The *LHV* has researched 9 *HISs* in 2018 and sees an improvement of functionality compared to their last study in 2016 (ICT&health, 2018). Mr. Van der Tang describes the market as fragmented, but he also sees rapid developments (2014).

Because there are multiple different developers of *HISs*, and no open standards are being used yet, interoperability is lacking, and often problematic (Nederlandse Vereniging van Doktersassistenten, 2017). This, in combination with the fact that there are only a few big vendors, makes it also harder for new entrants to enter the market with a new product (Eikelenboom, 2019).
This has also a direct effect on patients when they move to another place and switch general practitioners. The administrative process is causing manual transactions, increases the workload, and adds potential risks of copying information incorrectly.

4.2.2.9. National Switching Point - LSP

To exchange some information from the *HIS* with other parties, the *Landelijk SchakelPunt (LSP)* has been created. The *LSP* is the successor of the *EPD*, with improvements.

To connect to the *LSP*, healthcare providers have three requirements. First, they need a good governed information system. Secondly, they are required to have a well-governed healthcare network for reliable and secure communications between their information system and the *LSP*.
Finally, the authentication measures need to be in place so that it complies with the unique healthcare professional identification number legislation. This is a system that works with server certificates, identification cards, and pin codes to authenticate the professional. On the card itself, it is stored which information the professional is allowed to see (Vereniging van Zorgaanbieders Voor Zorgcommunicatie, 2019).

General practitioners are allowed to share a professional summary. This summary contains the open episodes, the journal, prescribed medicine of the last four months, results of the patient, contra-

medication, and actual handover data. Pharmacists can share the medication of the last 6 months, and data about allergies, drug intolerances, and contraindications.

Only professionals with an active treatment-relationship with the patient can request to see the data. These include pharmacists, locum tenentes, specialists in hospitals and other institutes. Before this can happen, the general practitioner and pharmacist have to ask formal permission of the patient to share their data on the *LSP*.

The major difference with the intended *EPD* is that data is not stored centrally in one national database, but it is dispersed between al healthcare providers' different information systems.

4.2.2.10. Future

In the future, the idea of the government is that more and more data must be disclosed between healthcare providers. Secondly, it is also required that the patients themselves have more control over their files, i.e. they can access it, and they can decide who can look their data up. To achieve this, multiple state-sponsored programs have been funded.

4.2.2.11. Personal Health Environment - PGO

The *Persoonlijke GezondheidsOmgeving*, or personal health environment, are a collection of websites and applications that provides patients access to their own data, by complying to interoperability standards. All of the patient's data, from different healthcare providers, is shown in one place. It is mandatory that patients can access their data free of charge in July 2020 (Landelijke Huisartsen Vereniging, 2019). The environment will be secured by the government managed authentication method *DigiD*.

It is also possible for the patient to indicate which (categories of) healthcare providers are allowed to see the patients' data. This creates a finer control mechanism for the patient compared to the current situation with the *LSP* (Patiëntenfederatie Nederland, 2019). This has been criticized by healthcare professionals, because they are not able to guarantee that they have the full patient file on hand, e.g. patients could have blacked out current medication or previous treatments they are ashamed of. This could even lead to unnecessary deceases (Adviescollege toetsing regeldruk, 2019).

The technical agreements for interoperability between the *PGO* and the healthcare providers are supported by the *MedMij* initiative. This is a coalition of the Dutch patient federation, *Nictiz*, *LHV*, healthcare insurers, other healthcare providing umbrella organizations, and the Ministry of Health, Wellbeing and Sport (MedMij, 2019).

4.2.2.12. Disclosure Patient-data First Line - OPEN

To support general practitioners with disclosing their patient data to the *PGO* specifically, *Ontsluiting Patientgegevens uit de Eerstelijnszorg in Nederland (OPEN)* has been founded (Landelijke Huisartsen Vereniging, 2019). This program is led by *LHV*, *NHG*, and *InEen*, an interest group for the first line. It has been characterized by the Dutch government as one of the programs that support the VIPP program: information exchange between patient and professional.

This initiative provides financing for the general practitioners, a roadmap on how to best reach the objective, a regional network to share best practices, and ways to unburden the general practitioners (Nederlands Huisartsen Genootschap, 2019).

4.2.3. Conclusion

General practitioners are a central hub of the Dutch healthcare landscape. They have a lot of personally identifiable information. This is highly sensitive patient data. However, they have to open this up for the patients themselves but also to third parties. For now, their website is the main portal for how patients can access their information. Here are security risks involved and it is not yet known what the current security status of their website is.

4.3. Theoretical Frameworks

In this section, the theoretical frameworks found in literature will be discussed.

First, the theories about perceptions will be discussed. These are the Technology Threat Acceptance Theory, the Selective Organizational Information Privacy and Security Violations Model, and the three Technology Acceptance Models. Following the perceptions, the behavioral theories will be examined: Policy Awareness on Employee's Cybersecurity Behavior and Understanding Security Behaviors in Personal Computer Users.

The sixth subsection about Strategic Alignment Model will outline the alignment between business and IT, with the different perspectives and the maturity model.

Finally, the effects of IT alignment on the business results are discussed in Factors Impacting IT-Business Strategic Alignment and Model Strategic Alignment & Benefits Management Leading to Outsourcing Success.

4.3.1. Technology Threat Acceptance Theory

In research by Liang and Xue, the Technology Threat Acceptance Theory was proposed (2009). This theory was developed by synthesizing multiple theories and applicable literature. This literature came from the subjects of information systems, psychology, management, marketing, health psychology, and finance.

The authors proposed 12 propositions, which they motivate by literature.

As Figure 2 shows (Liang & Xue, 2009), the model takes into account the threat appraisal of an actor, i.e. how he perceives the threat and his coping appraisal, i.e. the process of finding an appropriate way to circumvent the risk. These factors will influence the final coping behavior of the actor, which can have different forms: *problem-focused coping* or *emotion-focused coping*.

The perceived threat is defined by Liang and Xue as the discrepancy between the users' current state and the undesired end state. This is formed by two preconditions: the actor's subjective probability that malicious IT will negatively impact him, and the actor's subjective idea of how severe the consequences will be.

For coping appraisal, the definition of *perceived avoidability* is the actor's subjective assessment of the probability that he will be able to avoid malicious IT by using specific protection measures. This perception is formed by three subsequent factors. *Perceived effectiveness* is the belief that a specific action will lead to a specific outcome. The *perceived costs* not only reflect monetary value, but also the needed efforts like time and inconvenience. These costs create a barrier to the desired behavior. *Self-efficacy* is the actor's confidence in taking security measures.

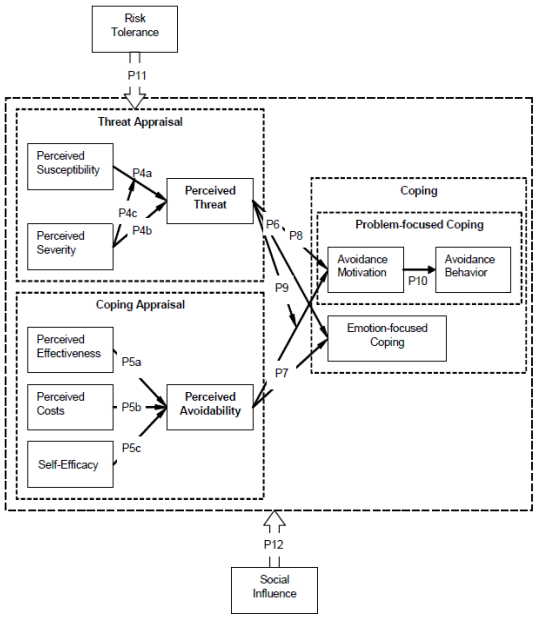


Figure 2: Technology Threat Avoidance Model

4.3.2. Selective Organizational Information Privacy and Security Violations Model

In a study done by Wall, Lowry, and Barlow, they proposed a model for the influence of Contextual and Rule & Regulatory Conditions on the perceived risk of violating a privacy or security rule with the moderator factor of strain, as shown in Figure 3 (2016).

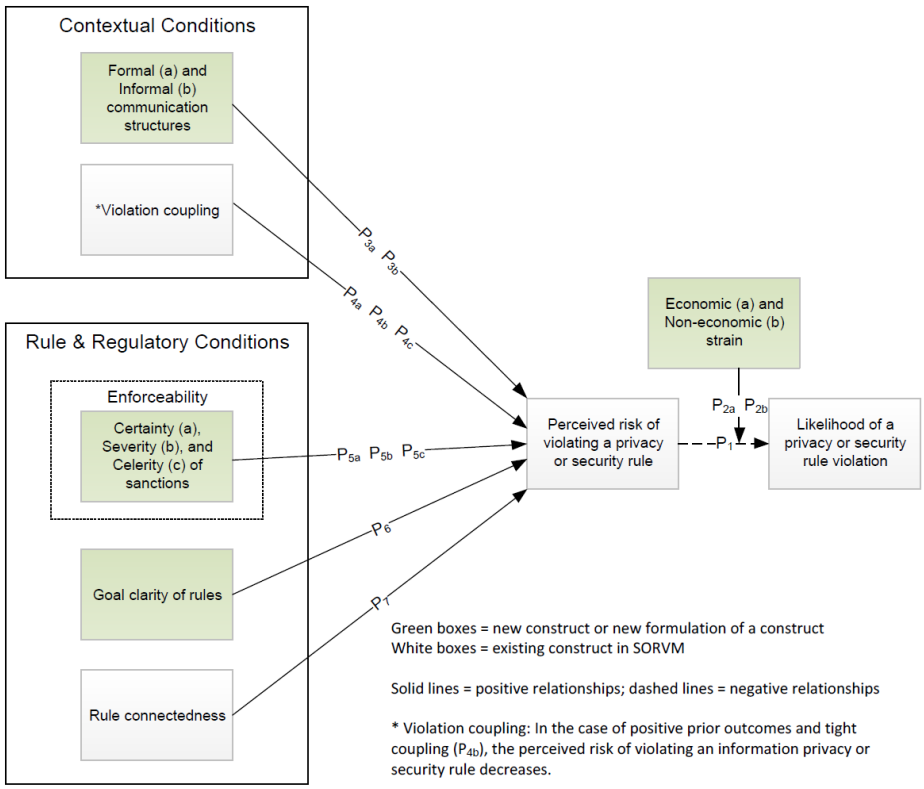


Figure 3: Selective Organizational Information Privacy and Security Violations Model

The model tries to address the reason why organizations violate current privacy regulations. This is done by creating a model based on literature. Within this model, seven propositions were proposed. These were supported by a case relating to unauthorized computer system intrusion at TJX Companies.

The contextual conditions comprise of two parts. The formal and informal communication structures, that develop the organization vertically and laterally respectively. And the coupling of privacy and security violations with the impact of its result. This means that the offender is relative sure that a violation will lead to a presumed outcome, either negative or positive.

The Rule & Regulatory Conditions include three parts. The first part is the enforceability, which includes the certainty a sanction is enforced. The severity is the perceived impact a sanction has for an intended act. The celerity refers to the time between the act and the final punishment. The second part is the goal clarity, which encompasses the concept that the procedures are in line with the desired outcome and is clear and understandable for those expected to follow them. The last part comprises of the connectedness of the privacy and security rules with other kinds of rules concerning risk and compliance.

The strains that moderate the correlation of the perceived risk and likelihood of a violation, is twofold. First, when there is an economic strain, organizations are becoming more risk tolerant. However, when organizations are reaching near-bankruptcy, they become more risk averse. On the other side of the spectrum, when there is an abundance of resources, organizations are also more likely to engage in dangerous behavior (Singh, 1986). The non-economic strains are the factors that deter the motivation of individuals to reach their goals through legitimate ways. Examples of non-economic strains are a failure to attain goals, a discrepancy between expectations and successes, elimination of positive stimuli, and the construction of negative stimuli (Agnew, 2001).

The perceived risk of violating a rule was defined as the perception managers had within an organization to the likelihood and impact of negative consequences due to infringements. The likelihood of an actual violation was measured by asking employees how likely they would be in certain situation of transgressing.

The study showed that all the proposed propositions were supported by the research done on their case study. The contextual and rule & regulatory conditions had a positive relationship with the perceived risk, while the perceived risk had a negative relationship with the likelihood of rule violations. The strain of economic and non-economic resources had a positive moderator effect on the organization's risk perception.

4.3.3. Technology Acceptance Model

The technology acceptance model was proposed by Davis in his thesis for his Ph.D. in management (1985) and validated again in a case study done by Davis, Bagozzi, and Warshaw (1989). The goal of the research was to develop a theoretical model "of the effect of system characteristics on user acceptance of computer-based information systems".

Davis builds upon the theory of reasoned action, proposed by Fishbein and Ajzen (1975). The model constitutes out of motivational mediator variables: perceived ease of use, perceived usefulness, and attitude toward using. Taken together, these variables intervene between how the system is designed and intended to use, and the actual behavior the user performs on the system, as shown in Figure 4.

The system is defined as the design features that affect the variables perceived usefulness and perceived ease of use.

The perceived usefulness is defined by Davis as "the degree to which an individual believes that using a particular system would enhance his or her job performance", while the perceived ease of use is defined as the level to which an individual thinks that using a specific system would be with minimal effort. These two perceptions have a relationship with the *attitude towards using*. This attitude refers to the level of evaluation an individual has with using a specific system.

The actual system use is determined as the behavioral response that follows from the users' motivation.

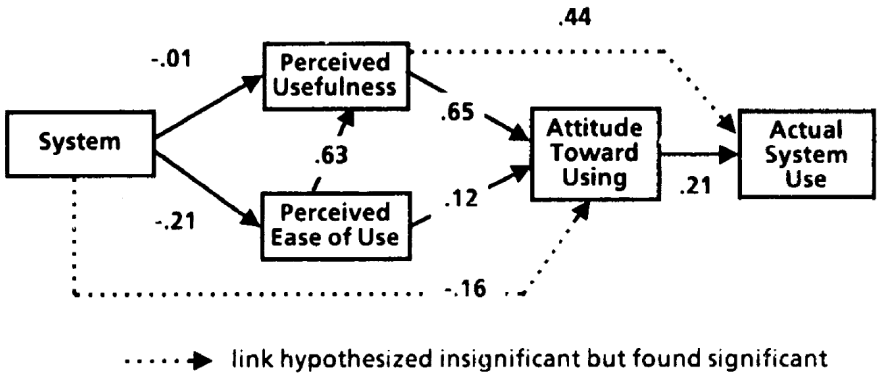


Figure 4: Technology Acceptance Model 1

In the early and late 2000s, the technology acceptance model was improved twice (2000; 2008). In the first iteration, the additional variables *subjective norm*, *image*, *experience*, *voluntariness*, *job relevance*, *output quality*, and *result demonstrability* were added by Davis and Viswanath (2000). As can be seen in Figure 5, the tested correlations were all validated.

For the second model, four longitudinal field studies were performed to validate the *Technology Acceptance Model 2*, as shown in Figure 5. For twelve proposed hypotheses, nine were confirmed in all of the four

studies. Two hypotheses were confirmed in three studies, while one hypothesis was supported in two case studies.

Additionally, to the model described above, the second model has the variables *subjective norm, image, job relevance, output quality, result demonstrability, experience, and voluntariness*. These variables are used as the design features from the first model.

The subjective norm is the typical norm that someone perceives to do or not to do some particular behavior, while the image is defined as the degree to which someone can enhance one's status. The job relevance is the applicability of a system to help an individual with their job. Output quality is the consideration people take on how good a system performs the tasks. Although systems can help users with their tasks, it is needed that this relationship is understood by the user. Therefore, result demonstrability is defined as the tangibility of the effects of using the tool. Experience is a moderator variable. The conceptualizes the hands-on understanding a user has with a system. Another moderator is voluntariness and is expressed in the requirement to use a system.

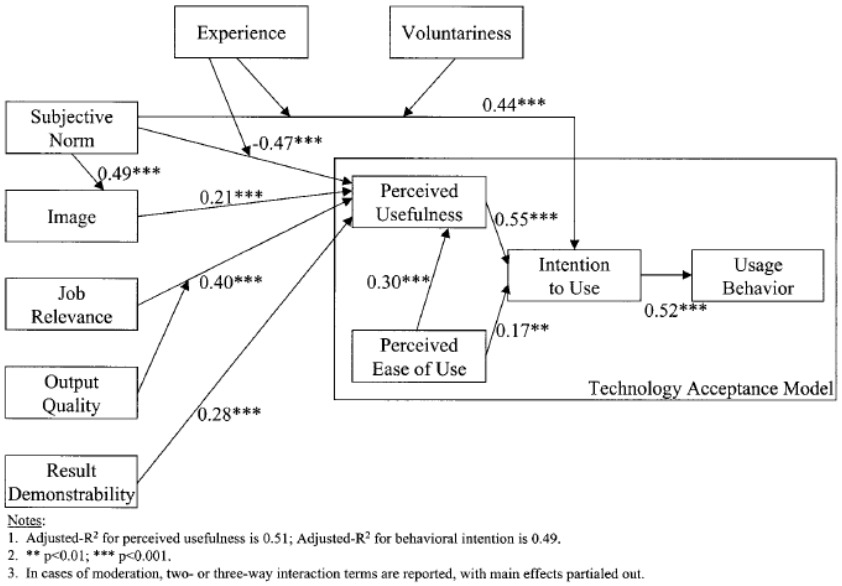


Figure 5: Technology Acceptance Model 2

In the last iteration, the model was extended with the determinants of the perceived ease of use (Venkatesh & Bala, 2008). Next to these 6 determinants and their relationships as shown in Figure 6, an addition 3 relationships were suggested and empirically tested which are indicated by the thick lines. This was done with a longitudinal field study across four sites over a 5-month period with four points of measurements. These four organizations are from different industries with different complexities

The six determinants for the perceived ease of use are grouped together in two separate areas. These are anchoring and adjustment. The area of anchoring exists out of computer self-efficacy, perceptions of external control, computer anxiety, and computer playfulness.

The authors define self-efficacy as the individual's believe in having control believes in regard to their ability to use a system. Perception of external control is related to the support an individual thinks he will get from the organization in the form of support and resources to facilitate the use of the system. The degree of an individual's fear when using a system is the definition of computer anxiety, while computer playfulness relates to the intrinsic motivation a user has when using a new system.

The *adjustment* area exists out of *perceived enjoyment* and *objective usability*. The first determinant is defined as the perceived enjoyment a user has without taking into consideration any performance related issues. The second determinant has the definition of the "comparison of systems based on the actual level (rather than perceptions) of effort required to completing specific tasks" (2000).

As explained above, there were three additional relationships suggested and empirically validated. Experience had a positive moderating effect on the relationship between computer anxiety and perceived ease of use. Experience also had a positive effect on the moderating relationship between perceived ease of use and behavioral intention. Experience had a negative moderating effect on the relationship between the perceived ease of use and the perceived usefulness of IT. This would mean that if an individual would gain experience, his fear of using the system would diminish, as would his idea of the usefulness of the system. His perceived ease of use on the other hand would increase. Due to this two-sided property of experience, it is an important factor to note in organizations.

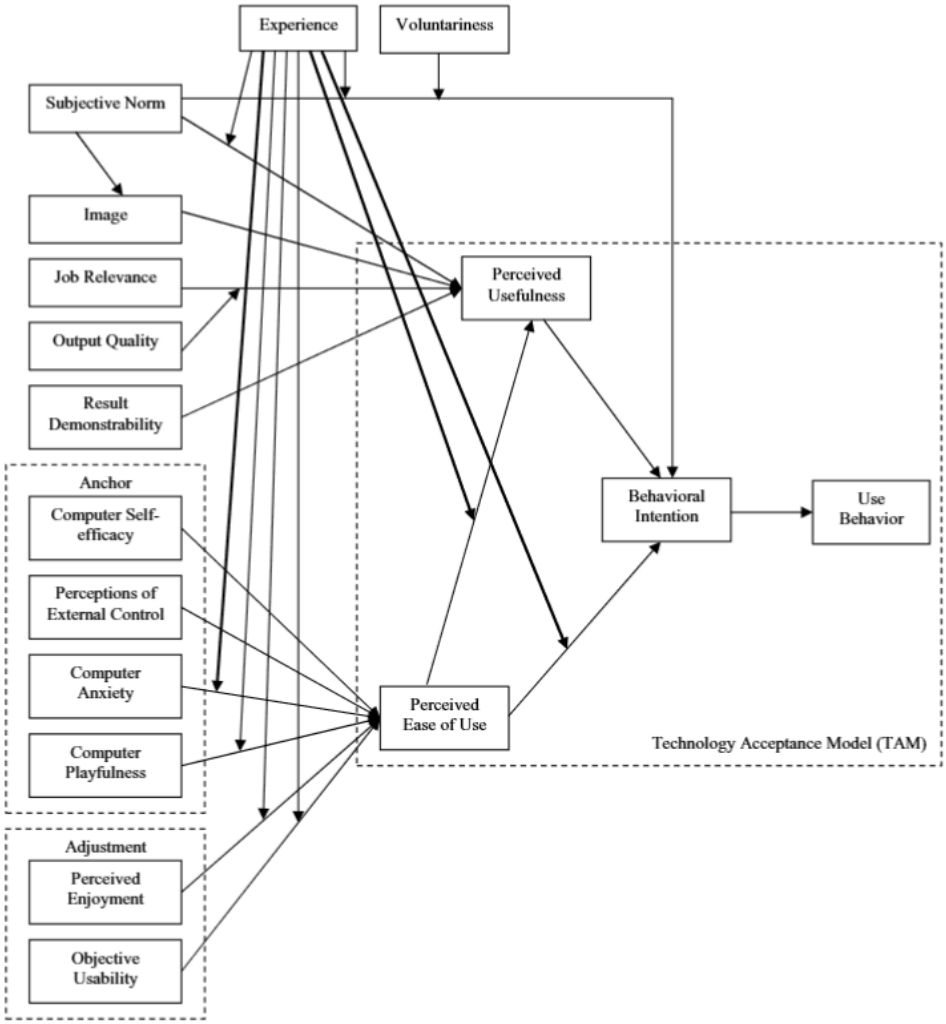


Figure 6: Technology Acceptance Model 3

The added value of this third model, is that it shows that there is a unique role for each determinant of perceived usefulness and perceived ease of use. The properties that make them unique, is that the determinants of perceived usefulness do not influence perceived ease of use and vice versa. These determinants are standing on its own.

4.3.4. Policy Awareness on Employee's Cybersecurity Behavior

In an article by Li et al. t, the effect of cybersecurity policy awareness on employees' cybersecurity behavior was explored. As Figure 7 shows, it has similarities with the Technology Threat Acceptance Theory of Liang and Xue. This is because both models build upon the protection motivation theory of Rogers (1975).

The proposed theory includes the organizational environment of the actor as well. This environment includes *peer behavior*, i.e. if an actor sees that his peers regularly follow cybersecurity guidelines, he is more likely to behave this way in fear of being left out if he does not. *Cue to Action* is the trigger for certain protective

behavior. These cues can be internal, e.g. actor's computer infected with malware, or external, e.g. media coverage of a data breach. And finally, the prior experience an actor has with information security practices. The threat appraisal is defined in this model as the assessment the actors make about the danger a threatening cyber-crime poses to them, while the coping appraisal refers to how they assess their abilities to minimize potential damage.

In their paper, they have proposed 12 hypotheses, 11 of these were supported. As shown in their paper, peer behavior had a positive effect on the cues, and the cues had a positive effect on the actor's prior experience with information security.

This experience with security practices is an important variable for all of the factors of the protection motivation theory. The perceived severity, perceived vulnerability, response-efficacy, and self-efficacy were all positively affected by a higher prior experience with information security practices. The perceived barriers were negatively impacted, i.e. the higher the prior experience was, the lower the perceived barrier. The final five proposed hypotheses influenced the cybersecurity protection behavior (CPB) and four of these were validated. The response-efficacy and self-efficacy had a positive effect on CPB, while the perceived barriers negatively influenced CPB. The hypothesis that perceived severity would positively impact CPB was not supported by the data.

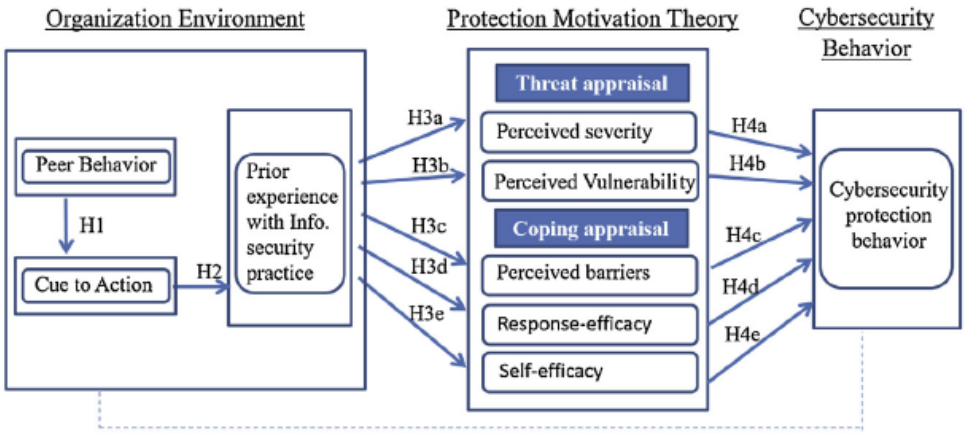


Figure 7: Policy Awareness on Employee's Cybersecurity Behavior

4.3.5. Understanding Security Behaviors in Personal Computer Users

In a study done by Liang and Xue, they built upon their model they proposed earlier as shown in section Technology Threat Acceptance Theory (2009; 2010). In the first model, Liang and Xue proposed twelve propositions and validated these with literature. In the research article of 2010, the researchers proposed nine hypotheses.

The research was done by surveying 152 personal computer users, and the analysis of the data revealed several correlations. The concepts from the previous model were used for this model as well. As can be seen in Figure 8, all but one of the proposed hypotheses provided adequate support.

The perceived severity and the perceived susceptibility had both a positive impact on the perceived threat. The interaction between the perceived severity and the perceived susceptibility, however, could not be validated by the data. The perceived threat, safeguard effectiveness and self-efficacy had a positive effect on the avoidance motivation, while the combination of perceived threat and safeguard effectiveness, and safeguard cost had a negative impact. The avoidance behavior was positively correlated with the avoidance motivation.

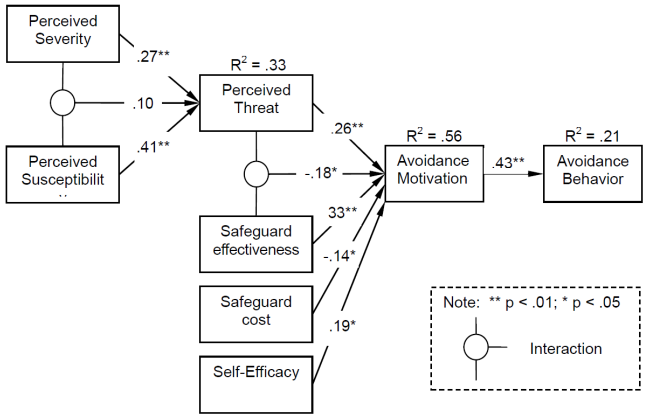


Figure 8: Threat Avoidance Model

4.3.6. Strategic Alignment Model & Perspectives & Maturity

Alignment between the business and IT is composed of two dimensions, as shown by Henderson and Venkatraman (1990; 1993). The two dimensions are the strategic fit and functional integration.

As shown in Figure 9, there can be a strategic fit between the external strategies of the business and IT, and the internal infrastructure & processes of the organization and IT. It has to be noted that if there is a strategic fit between the business strategy and the organizational infrastructure & processes, there is not necessarily a strategic fit between the IT strategy and the IT infrastructure & processes. In a study done by Yayla and Hu, it was empirically validated that having a strategic alignment is of importance for organizations (2009).

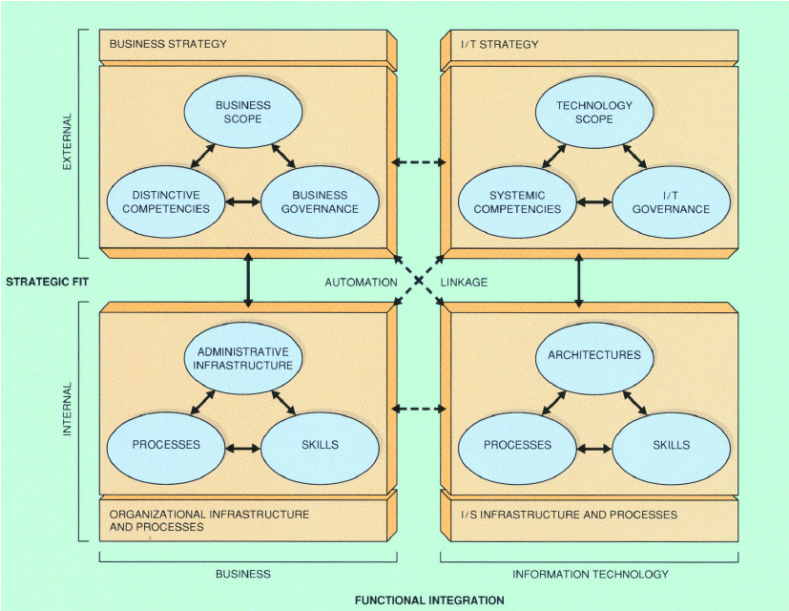


Figure 9: Strategic Alignment Model

Secondly, there can be functional integration between the left, the business side of the organization, and the right, the IT side of the organization.

The business strategy comprises the business scope, distinctive competences and the business governance. Henderson and Venkatraman define these respectively, as which products and services an organization delivers, the key attributes of strategy, and developing new ways of governance.

The I/T Strategy is the combination of technology scope, systemic competencies, and I/T governance. The technology scope is defined as the specific IT that support current or new business strategies and the systemic competencies are the attributes of the IT strategy that positively support the construction of new

business opportunities. The I/T governance is the "selection and use of mechanisms for obtaining the required I/T competencies" (Henderson & Venkatraman, 1993).

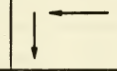
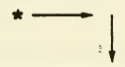
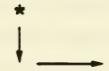
The internal domains for the business as well for the I/T addresses three components. For the business strategy these are processes, skills and the administrative infrastructure, while for the I/T strategy these are processes, skills, and architectures.

For the business side these are defined as the designing organizational processes that support the ability to execute its strategy, the skills required to execute its business strategy, and the roles, responsibilities and task structures respectively.

For the IT side, the following definitions are used. For processes, definition is the decisions that are made in regard to the operations of the infrastructure such as development, maintenance and monitoring. Skills deals with the acquisition, retention, and development of individuals with knowledge of the infrastructure, while the architecture defines which choices are made to define the soft- and hardware landscape of the organization.

Four dominant perspectives are proposed by Henderson and Venkatraman on how to align your business within the four sub-domains. These four perspectives are shown in Table 2 (Henderson & Venkatraman, 1993). From the Domain Anchor, marked with an *, the succeeding domains are aligned to the starting point. In the IT Planning Method Example Henderson and Venkatraman show which theories support their perspective.

Table 2: Four Dominant Perspectives on IT Planning

Label	Cross-Domain Perspective	Common Domain Anchor	I/T Planning Method Example
(1) Technology Exploitation		Technology Strategy	Opportunity Identification (Sharpe 1989) Value Chain Analysis (Cash)
(2) Technology Leverage		Business Strategy	G/CUE (Gartner Group 1989)
(3) Strategy Implementaion		Business Strategy	CSF (Rockart 1979) Enterprise Modeling (Martin 1982)
(4) Technology Implementation		Technology Strategy	Service-level Contracting (Leitheiser & Wetherbe 1986)

* Domain Anchor

For the first alignment method, *Technology Exploitation*, the start domain is the Technology Strategy, i.e. IT and external. From this domain, the Business Strategy is modified to benefit optimal from the competitive role of IT, and sequentially the internal business will be adopted to support this strategy with the fitting governance and capabilities.

The idea is that all the views are used together, to optimize the business. So, not only one perspective should be used, but they should be used all together.

To measure how aligned an organization is, a strategic alignment maturity model has been created by Luftman. This model has six criteria areas as shown in Figure 10.

The process to measure maturity is as follows. A team of business and IT experts determine at which level all the separate areas are on a scale from 1 to 5. The discussion that leads to the determination of this level, is useful to understand the current state of the business. It is also necessary to understand how the organization can best progress to a better maturity level. After this separate grading, the overall level is determined. The next higher rank of maturity is the goal to which the organization works towards (2000).

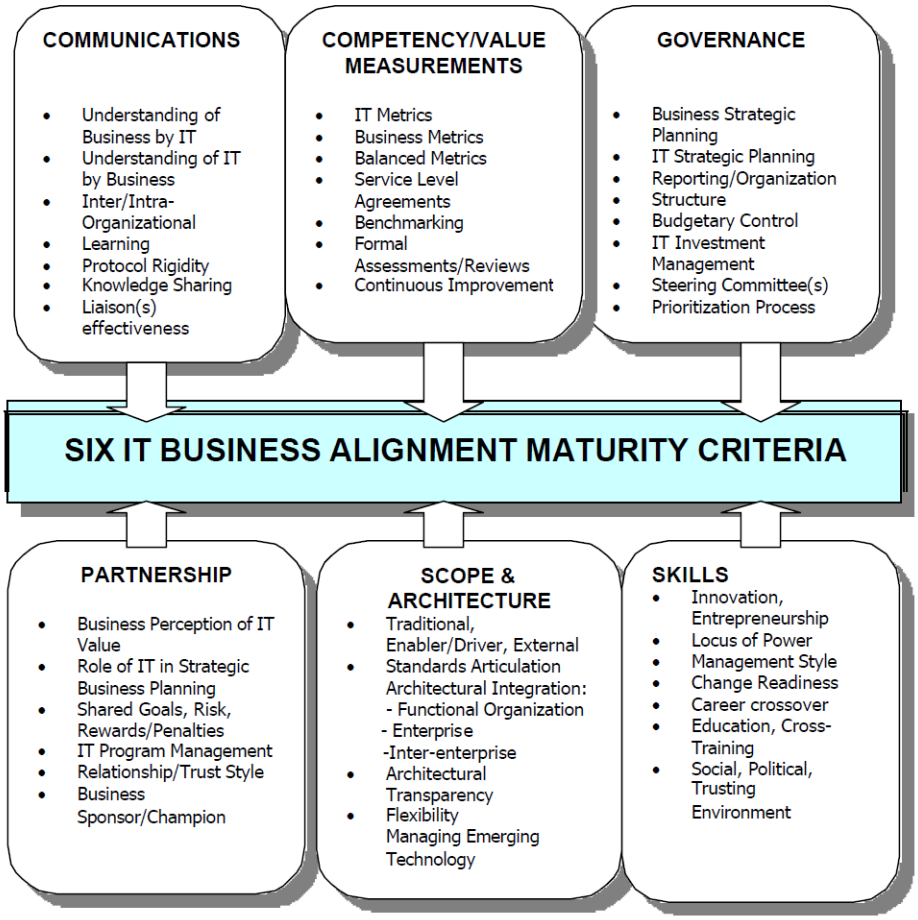


Figure 10: Alignment Maturity Criteria

Luftman has also created a strategic alignment maturity summary, as shown in Figure 11. The six levels are summarized as follows. Within the first level of strategic alignment maturity, i.e. the lowest level, it is unlikely that the domains are aligned in any way. This means that any investment an organization does in its information technology, will not create a significant business impact. For the second level,

departmentalized solutions are being created, but no overall goal is set yet. Any alignment at the departmental level is not augmented to the whole enterprise, but the potential is being understood. At the third level, the understanding of the business by IT is present, but vice versa not yet completely. The strategic alignment maturity can be described as focused, i.e. governance, processes, and communications are fixated towards business goals. At the fourth stage, IT is seen as a value center and as a competitive advantage from the business perspective. At the final level, the understanding of both the business and IT is at both sides pervasive. The governance process considers both the IT strategy and the business strategy at once to mutually and optimally align them.

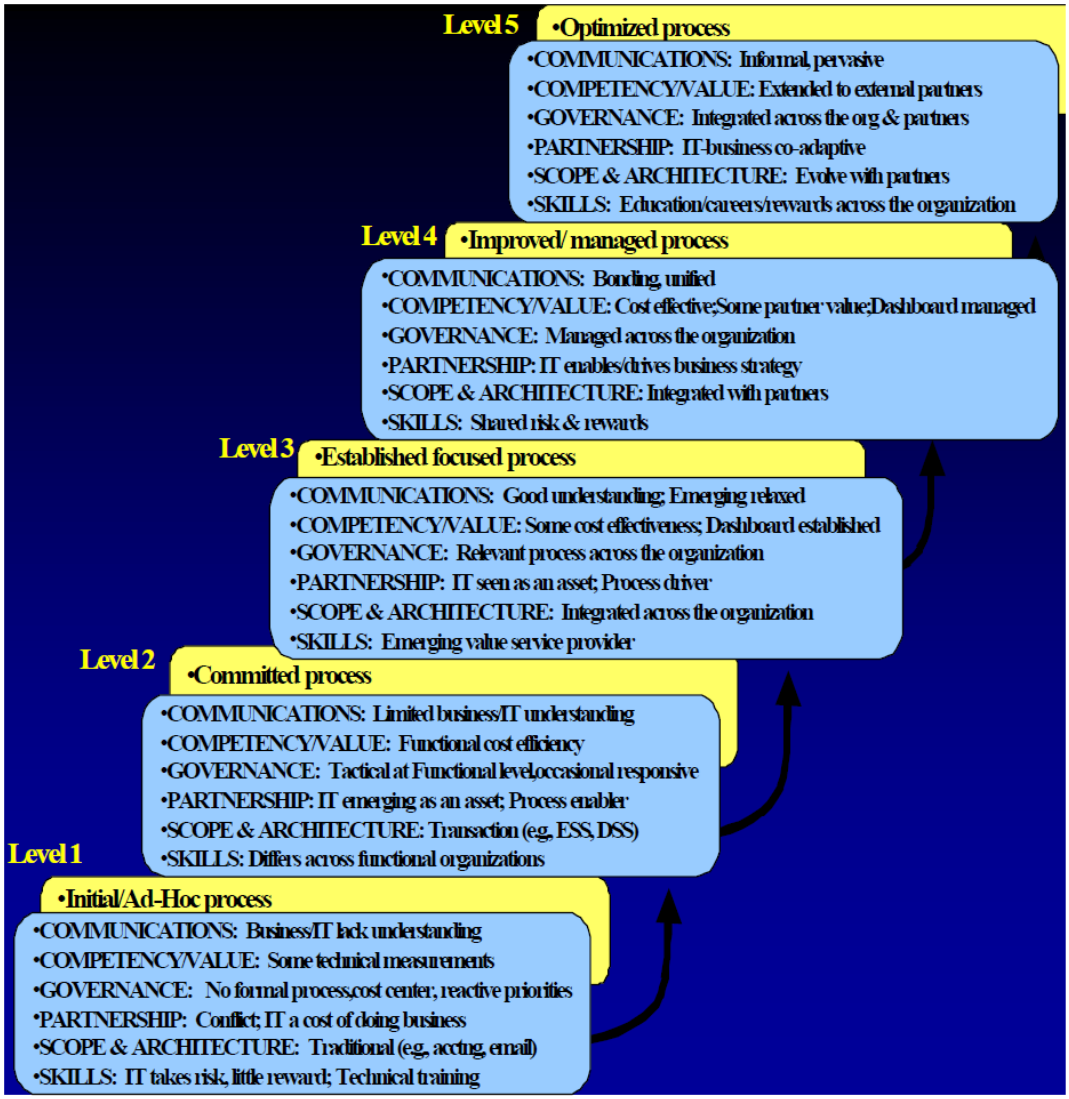


Figure 11: Strategic Alignment Maturity Levels

The maturity model has been validated (Luftman & Brier, 1999). This study was based on survey data that represented over 500 firms from the Fortune 1000 from 15 different industries.

4.3.7. Factors Impacting IT-Business Strategic Alignment

S. Jorfi and H. Jorfi have examined the role of IT flexibility, capability and communications effectiveness on strategic alignment in the Agricultural Bank of Iran with Strategic Information Systems Planning serving as a moderator variable (2011). As the researchers have shown with their conceptual framework as shown in Figure 12, there is a correlation between the three independent variables *IT flexibility*, *IT capability*, and *Communications Effectiveness* and the dependent variable IT-business strategic alignment.

IT flexibility is defined by Duncan and Byrd and Turner as the combination of four constructs: software modularity, hardware compatibility, network connectivity, and IT skills adaptability (Duncan, 1995; Byrd & Turner, 2000). Jorfi and Jorfi uses this definition without the IT skills adaptability.

The definition for IT capability used in the article was the ability an organization had so that it could support the actions and work procedures in the organization by ordering and connecting other resources that are crucial.

Communication effectiveness is described as the understanding between the sender and the receiver, whereby a high degree of similarities supports a high level of communication effectiveness. Subfactors of communication effectiveness are skill, motivation, and knowledge of both the sender and the receiver.

These three independent variables, according to the validated model, have a significant relationship with *IT-business strategic alignment* (Jorfi & Jorfi, 2011). The factor of *strategic information systems planning*, is the moderating variable. This variable is identified as the activities of identifying a set of software applications that will support an organization in executing and realizing its business plans and attaining its business goals.

From the 12 proposed hypotheses, 7 were significantly validated by their data from 82 questionnaires that were filled out by managers. The outcome of the study was that there is a relationship between the skill of communication, as well as the motivation and knowledge and the IT-business strategic alignment. For the factors of IT flexibility and for IT capability, there was also a positive correlation with IT-business strategic alignment.

The strategic information systems planning had no moderator effect on any of the three aspects and the final alignment.

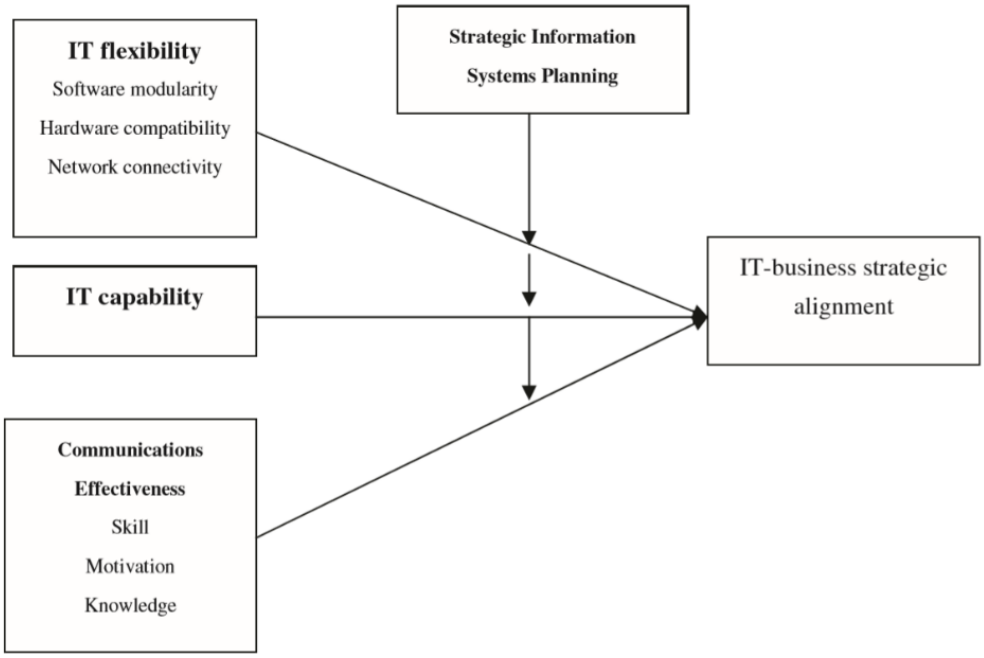


Figure 12: Factors Impacting IT-Business Strategic Alignment

4.3.8. Model Strategic Alignment & Benefits Management Leading to Outsourcing Success

Van Lier and Dohmen researched the relationship between strategic alignment and outsourcing success in a multiple case study (2007). They made the proposition that strategic alignment influences the IT outsourcing success. In the cases that were part of the study, it showed that there was an outsourcing success as a function of the strategic alignment of these organizations.

The variable of strategic alignment was defined by the maturity model of Luftman (2000). In this maturity framework, as shown above in section 4.3.6 there are six criteria that are scored on 39 different statements. Van Lier and Dohmen scored these case studies according to the Luftman maturity model, while the outsourcing success was defined as the perception managers had of the project, as well as the percentage attained of the potential benefits. The researchers found that there is a link between strategic alignment and both perceived and calculated success of these outsourcing projects.

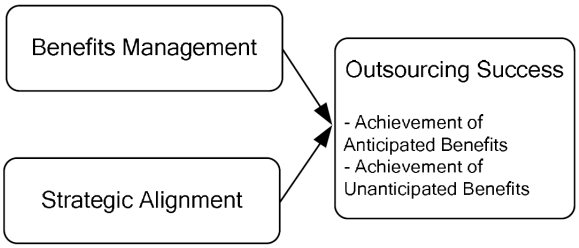


Figure 13: Benefits Management and Strategic Alignment in an IT Outsourcing Context

4.3.9. Comparative Analysis of Theoretical Frameworks

Table 3 shows an overview of the different theoretical frameworks as discussed in the previous sections. The covered subjects from each article are shown, as well as the subjects not covered, and so the overall gap is provided.

Table 3: Comparative Analysis of Theoretical Frameworks

Related works	IT Business Alignment	Perceived Threat	Perceived susceptibility	Motivation	Avoidance behavior	Coping appraisal	Cybersecurity	Service Application	Capabilities
Technology Threat Acceptance Theory		✓	✓	✓	✓	✓			
Selective Organizational Information Privacy and Security Violations Model		✓	✓		✓	✓			
Technology Acceptance Model				✓	✓				
Policy Awareness on Employee's Cybersecurity Behavior		✓	✓			✓	✓		
Understanding Security Behaviors in Personal Computer Users		✓	✓	✓	✓	✓			
Strategic Alignment Model & Perspectives & Maturity	✓								✓
Factors Impacting IT-Business Strategic Alignment	✓								✓
Model Strategic Alignment & Benefits Management Leading to Outsourcing Success	✓						✓	✓	

4.4. Proposed Conceptual Framework

Based on the frameworks discussed above, a conceptual framework is proposed that covers all the subjects as shown in the comparative analysis. The concepts used for the proposed framework will be explained first, then the relationship between them, followed by eight proposed hypotheses.

4.4.1. Concepts

The concept that will be used are a combination of the definitions discussed in Concepts as well in Theoretical Frameworks

The first independent group of variables is the concept of threat appraisal. As seen in paragraph 4.3.1 and 4.3.4, this concept consists out of the perceived severity and the perceived susceptibility of the risk.

4.4.1.1. Perceived Severity

The concept of perceived severity in the proposed framework is the perception a general practitioner has about the consequences a risk will have on their practice.

4.4.1.2. Perceived susceptibility

The concept for the perceived susceptibility that will be used is: *the perception a general practitioner has* on the probability damage will occur.

These two concepts combined will form the threat appraisal of the general practitioner. The threat appraisal is the concept of *the evaluation by the general practitioner of the potential undesirable consequences of being attacked by malicious actors*.

The second group of independent variables is the coping appraisal group. This group consist out of the perceived costs, skills, knowledge and self-efficacy of the general practitioners.

4.4.1.3. Perceived costs

The definition of the perceived is the financial and non-financial barriers a copping solution would create, as seen in subsection 4.3.2.

4.4.1.4. Skills

The concept of skills is the idea a general practitioner has about his own and his practice's ability to perform coping actions and behavior that would diminish the threat.

4.4.1.5. Knowledge

The concept of knowledge is about the understanding a general practitioner has about the possible threats and countermeasures its practice can take to mitigate the risks.

4.4.1.6. Self-efficacy

Self-efficacy is someone's trust in his own capabilities to perform a task well.

4.4.1.7. ASP capabilities

The moderator variable of ASP capabilities comes from the theory presented in subsection 4.3.7. In the theory of the Strategic Alignment Model, and the following maturity model of Luftman, the Six IT Business Alignment Maturity Criteria are presented. The definition of the ASP capabilities used here will be similar to the one used by Jorfi & Jorfi: the ability the application service provider has that can support the organization of the general practitioner's office by arranging and bringing together IT resources that are important (2011).

4.4.1.8. Alignment related behavior

The alignment related behavior is the mediator variables. This behavior is related to the avoidance behavior in subsection 4.3.1, 4.3.4, and 4.3.5. In these sections, the connection between threat and coping appraisal have been made to come up with an avoidance motivation which would result in certain desired behavior.
In the proposed model, the avoidance behavior which will be the result of the intersection of the threat appraisal and the coping appraisal is the alignment related behavior. This alignment related behavior comes with the six criteria that are presented by Luftman. The kinds of behavior of the general practitioner that will be the focus of the research are *partnership*, *communication*, *continuous learning*, and *locus of control*. The four areas are defined as the following. The partnership is about the searching for, or having an, active partnership.

Communication is about how and how often the general practitioners interacts with his ASP to transfer his knowledge as well as his requirements. Continuous learning is about the desire, behavior and outcome of keeping up to date with new insights.

The locus of control is the concept where the general practitioner has the feeling that he has control over the outcome of events within his practice.

4.4.1.9. Cybersecurity of web applications

Finally, the dependent variable is the result that will follow from the web scanner.

4.4.2. Conceptual Framework

When all the concepts and variables are combined, the following conceptual framework presents itself.

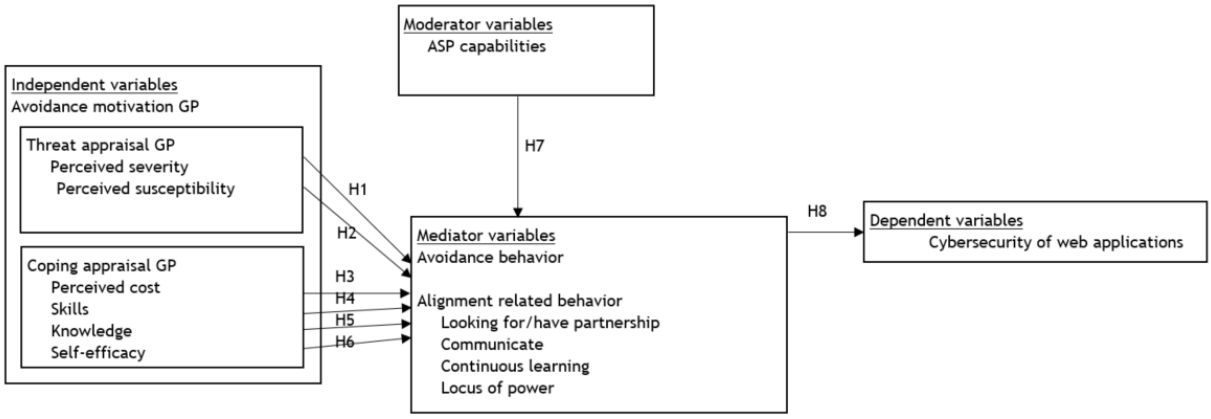


Figure 14: Conceptual Framework

4.4.3. Proposed Hypotheses

To answer the research questions correctly, multiple hypotheses are formulated. These are derived from the conceptual model as proposed in section 4.4.2. To come up with significant relationships between the concepts, assumptions are made.

The feeling a general practitioner has about the impact of a cybersecurity incident, will have a positive influence if he will perform alignment related behavior. This is because he will actively look for ways to diminish his risks by looking for a partnership or keep on learning. Therefore, the following hypothesis is formulated:

H1: Perceived severity positively affects alignment related behavior

---

If an individual has the feeling that he is more likely to be the victim of a cybersecurity incident, he is more likely to actively seek for methods to prevent these incidents. This attitude will affect the alignment related behavior because he will look for ways to improve his ways to mitigate his risks. Consequently, the next hypothesis is stated:

H2: Perceived susceptibility positively affects alignment related behavior

---

When barriers come up when trying to decrease risks, individuals will think twice about implementing these mitigation methods. These are not only financial costs, but also the obstacles which impedes reaching your goal. Therefore, the next hypothesis is stated:

H3: Perceived costs negatively affect alignment related behavior

---

The skills an individual has, will have an effect on their behavior. If a professional thinks he has the skills to form a good partnership, he will more likely also perform this behavior. This results in the next hypothesis:

H4: Skills positively affect alignment related behavior

If a general practitioner has more factual knowledge about the nature of the risks, he will try to do something about it. Resulting in the following hypothesis:

H5: Knowledge positively affects alignment related behavior

The confidence an actor has in himself to handle a situation correctly, will help him to ask for help and form correct partnerships. Because it is important for the general practitioner's practice to acquire knowledge and skills from outside his organization, this behavior will lead to alignment related behavior. Therefore, the next hypothesis is formed:

H6: Self-efficacy positively affects alignment related behavior

---

Adequate capabilities of the ASP to help and support the general practitioner with his needs, is of utmost importance to create a good partnership. Open communications, a fair balance of control, and a customer-focused approach will help align the business with the IT. This leads to the following hypothesis:

H7: ASP capabilities positively affect alignment related behavior

If a general practitioner performs more alignment related behavior, like he communicates his requirements, and he is looking for continuous learning, the outcome of the alignment would have a positive effect. Resulting in the following hypothesis:

H8: Alignment related behavior positively affects cybersecurity of web applications

5. Method

In this chapter the chosen methods will be explained.

Different methods of data gathering will be chosen because each approach supports different sub questions, as can be seen in Table 4.

Table 4: Link between research question and method

Research Question	Method
1. *What is the current cybersecurity status of websites of Dutch general practitioners?*	Scanner
2. *How is the general business & IT alignment maturity of Dutch GPs and their ASP currently?*	Input survey and interviews
3. *How should business & IT alignment maturity generally look like between the GP and their ASP to maintain a secure website?*	Interviews

In this section the method will be outlined how this problem will be researched and how the goal will be reached.

First, general practitioners will be contacted to answer a survey. The survey will ask questions about their awareness of cybersecurity risks, vulnerabilities, governance, and compliance. No technical questions will be asked.

In parallel, an automatic tool will be used to scan websites of all of the general practitioners on vulnerabilities. This tool will also assign a score to the web applications ranging from one, i.e. less vulnerable, to five, i.e. more vulnerable.

The results of the surveys will be linked to the result of the web scan by the web address to carry out the analysis. In the end, general practitioners will be interviewed as well for a better supported conclusion.

5.1. Literature review

To research the concepts regarding the current state of information security within healthcare and commonly used theoretical frameworks, first the literature will be used for descriptive research.

For these concepts descriptive research will be done by searching for specific definitions by significant organizations and definitions used in peer-reviewed papers.

Terms will be:

- Application service provider
- Information security
- Cybersecurity
- Healthcare information security
- Web applications
- Vulnerabilities
- Risk
- Threat
- Awareness

For researching existing theoretical frameworks, this will be done by looking into the secondary literature first. After common frameworks have been found, the original papers will be looked for and examined. From these original papers, the subsequent influential papers will be looked for at Google Scholar, the catalogue of Leiden University, and ResearchGate by examining their citation impact.

5.2. Survey

A survey is a quick and easy way to gather much data from multiple respondents. Because of its "one size fits all" property, it is good to get an overall idea of what the population has to offer. To get more detail of the practices, follow-up interviews will be held with a selection of the general practitioners that have filled in the questionnaire.

5.2.1. Advantages and disadvantages of surveys

Performing a survey for research purposes has multiple advantages, but also some significant disadvantages that should not be overlooked.

The benefits of a survey are that it is easy to reach a larger audience while keeping the cost down. A survey is also very flexible in the sense that multiple topics can be asked with the same form. Another important advantage is that surveys are easy to compare with each other and to do statistical analysis on when Likert-scales are being used.

The negative side of surveys is that it is a "one size fits all" solution. It is an inflexible method for respondents to fill in their answers. Another undesired property of a questionnaire is that it is artificially: respondents give answers based on what they think and feel, not how they behave. Respondents sometimes only start thinking about the subject at the moment the question is being asked while not having an opinion about it beforehand.

The general opinion about surveys is that it is a method that "is generally weak on validity and strong on reliability" but it can be a valuable method when combined within a multiple-methods research design (Babbie, 2007; Saunders, Lewis, & Thornhill, 2010).

5.2.2. Formulation of the questions

Performing a survey can be difficult, because of different factors (Babbie, 2007). These factors are mainly about that the questions should be formulated unambiguously. Terms should be formulated clearly, and no assumptions should be made about what a definition means. When closed-end questions are being asked, it is important that they are exhaustive, i.e. they should cover all the possible responses, and the options are mutually exclusive.

Another factor is that statements should be formulated as short as possible, as well as without any double-barreled questions. This means that a question should not contain the grammatical conjunction *"and"*, e.g. *"Should the government spend less on education and more on defense?"*. A different way that is often misinterpreted and it has been shown that it affected the outcome of a survey a lot, is a statement with a negation. An example of such a statement is "*Should the government not spend less on education?"*. The last factor that has to do with the formulation of the questions, is that a question should not include bias or a leading answer (Krosnick & Presser, 2010).

A different issue is the selection of the correct respondents. These have to be competent to answer the questions, i.e. knowing a valid answer, as well as willing to answer these.

Because every researcher can fall in the trap of unclear questionnaires (Polivka & Rothgeb, 1993), the questionnaire is first pretested on two general practitioners.

5.2.3. Survey concepts

The two properties that determine the overall quality of the survey are, as with all data collection methods, validity and reliability. Validity is the property that the collection method measures what it intends to measure, and reliability is the property that it gets the same result over and over again.

Although a high validity is hard to achieve with a survey due to its passive medium, there are sub-properties of validity which can be a helpful tool to steer on. There are three sub-properties: criterion validity, content validity, and construct validity.

Criterion validity, as mentioned by Babbie, is the "*degree to which a measure relates to some external criterion*". An example would be the validity of an admission test to predict future college success. This is often proven by statistical analysis (Saunders, Lewis, & Thornhill, 2010).

Content validity is defined as the extent to which the data collection method provides appropriate coverage for the concept being researched. A good way to reach this is through literature review and to have a preceding discussion with others (Babbie, 2007). In this research, the literature has been studied beforehand, as well as discussions with subject experts.

The last validity, construct validity, is based on the logical relationship between the different variables. This is best judged based on the continuous process of academic rigor, i.e. the cumulative work of other similar research projects (Peter, 1981).

Reliability, on the other hand, is when a measurement method provides the same outcome every time, all else being equal. There are three common approaches to examine this: test re-test, alternative form, and internal consistency (Mitchell V. , 1996).

With *test-retest* reliability, two sets of test scores are compared. These scores were acquired by keeping the testing conditions the same, i.e. the experimental tools, observer, measuring instruments, location, objectives, and the subjects did not change. Then some form of correlation, most often the Pearson correlation coefficient, is computed to show that the respondents answer the same way at both tests. The general rule is that it should have a confidence level of 0.95.

Alternative form relates to asking the same intended question with the same response, but with different wording. The drawback is that respondents will get annoyed to answer the alternatively formulated question again.

Internal consistency is the concept that the responses to each question within a survey, or part of it, correlates with other responses and their underlying construct. This is often done by Cronbach's alpha. Although there is no clear rule of thumb, the alpha should be above 0.6 to be considered acceptable (Nunnally & Bernstein, 1994).

When the results came back, the Cronbach alpha has been calculated, as shown in Table 5, for the different constructs. This shows that there is an acceptable internal validity.

Table 5: Constructs' Cronbach's Alpha

Construct	Survey Questions	Cronbach's alpha
Perceived severity	Q3.2, Q3.3, Q3.4, Q3.7	.766
Perceived susceptibility	Q3.5, Q3.8	.771
Perceived costs	Q4.4, Q4.5	.833
Alignment related behavior	Q4.3, Q4.8, Q4.9, Q5.7	.792

5.2.4. Pretesting of surveys

As described by Presser and Blair, the pretesting of a survey is an indispensable stage in the development of a good research method (1994). Therefore, the survey that will be sent out to the general practitioners will be first tested among some general practitioners and application service providers.

The following, as mentioned by Bell, will be measured: the time it took to complete the questionnaire, how clear the instructions were, which questions were unclear or ambiguous, which questions the respondents felt uncomfortable about answering, whether topics were missing, whether the layout was clear and attractive, and any other comments the pilot group has (Bell, 2005).

5.2.5. Creation of the Survey

The creation of the survey is based on the conceptual framework that has to be tested. Therefore, all the variables, as described in paragraph 4.4.1, with relation to the general practitioner, will have questions where this variable is tested. In Appendix 1: Survey questions with variable, the survey questions are linked with the corresponding variable from the conceptual framework, while in **Error! Reference source not found.**, the complete Dutch survey is shown. In the following appendix, the translation into English has been shown.

It is important to create a safe environment where the respondents have the feeling that there are no repercussions to what they answer. This is often done by anonymizing the survey. Unfortunately, due to the nature of the research, it is impossible to completely anonymize the survey because the web address of the general practitioner's practice has to be filled in. The general practitioners are notified however that this data will only be used for the analysis, and not in any other way.

The type of questionnaire will be a computerized self-administered questionnaire (CSAQ). The reason for choosing this option instead of *survey interviewing*, *telephone surveying*, *computer-assisted self-interviewing*, *touchtone data* entry, or *voice recognition*, is that CSAQ is more efficient, less time consuming for the researchers, as well as the possibility for participants to fill in the survey in parallel (Nicholls, Baker, & Martin, 1996). Although in the early years of the internet, a valid objection was that online surveys could not be a meaningful representative population, nowadays these concerns are greatly reduced (Babbie, 2007).

5.2.6. Population size

To make sure that the research is done properly, and the research can be repeated with the same outcome, it is important to have a high level of confidence and a low margin of error.

A minimal 95% level of confidence is considered the norm within research, as well as a maximum margin of error of 5%. As seen in section *4.2.1.1. General practitioner - huisarts*, there are 9,798 regular established general practitioners and 5,028 general practitioners with a practice. The *LHV* sent a mail writing that they presumed that nearly all general practitioners' practices had a website in January 2020. It is unknown how many websites there are exactly because multiple practices can have the same domain name.

As can be seen in *Table 6: Required Sample Size*, the required total response should exceed 357 when considering the general practitioners with a practice if a confidence level of 95% and a margin of error of 5% is anticipated.

Table 6: Required Sample Size

		Confidence level (%)		
		90%	95%	99%
Margin of error (%)	1%	2893	3301	3862
	2%	1272	1626	2277
	3%	658	881	1353
	4%	393	537	862
	5%	259	357	588
	6%	183	254	424
	7%	136	189	319
	8%	105	146	248
	9%	83	116	198
	10%	68	95	162
	20%	17	24	42
	25%	11	16	27

5.2.7. Distribution

The distribution of the questionnaire was done in multiple steps. First, the questionnaire was delivered to 477 email addresses of general practitioners having a website. The acquisition of these email addresses was done by using three different search engines to acquire a representable sample: Google, Qwant, and DuckDuckGo. Dutch search terms used on these search engines were: *"@huisarts*"*, *@huisarts*, *"huisarts" & "info@"*, *apotheekhoudend huisarts*, *huisartsen email*, *huisartsen mail*, and *www.huisarts*. The emails were delivered in batches in the period of January 24th, 2020 until February 3rd, 2020. A reminder was sent out in batches again in the period of February 6th, 2020 until February 11th, 2020.

Another delivery method was used as well. On HAweb.nl, a network for Dutch general practitioners, a post was published on January 26th, 2020 to the 114 general practitioners in West-Friesland asking the general practitioners in that geographic area to participate.

A third delivery method was done by contacting Lizeke de Clerck, manager of the LinkedIn group *Huisartsen*, and Mike Blok, manager of the LinkedIn group *Huisarts & ICT*. De Clerck did respond and said she would post my request in the LinkedIn group. This message has been posted on January 27th, 2020.

The academic training institutions for general practitioners at the Dutch university hospitals would not cooperate due to the number of requests they receive and the perceived lack of urgency of this subject.

5.2.8. Monitoring Returns

When the surveys are being sent out and the answers come back in, it is important to timestamp these. This is the case when an impactful event, like a data breach at a colleague's practice, changes the attitude of the general practitioners, which could result in a different response before and after the event. Beside timestamping, it is important to have a visualization of the rate of return. This can be shown in the number of surveys returned each day, as well as the cumulative percentage of returns (Babbie, 2007).

Because of the low response rate after the reminder, 40 general practitioners were selected at random to ask for feedback for why they had not responded. The practices were called on February the 28th, and the receptionist answered. Therefore, this is a proxy, and not a direct means of measuring the intent of the general practitioner himself.

The most common answers given were that the assistant thought that a) the general practitioner never filled in surveys, b) that the general practitioner was too busy in general, or c) that the general practitioner were

too busy because of the COVID-19 disease caused by the SARS-CoV-2 virus (the virus was diagnosed for the first time in the Netherlands on February the 27th).

The email was found by the assistants while on the phone, which is an indicator that there was no issue with the mails sent being labeled as spam.

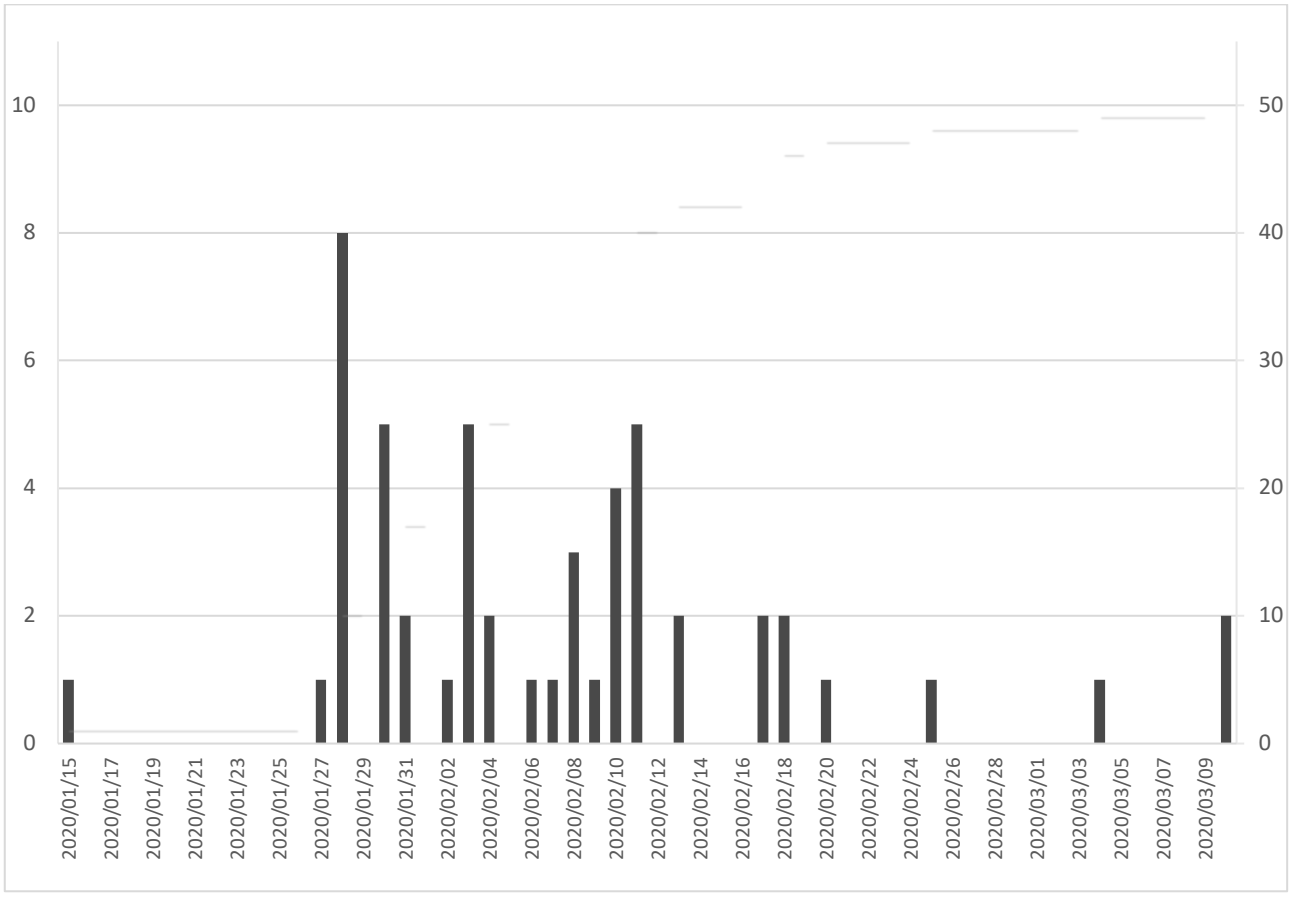


Figure 15: Response Rate

5.2.9. Selecting surveys

On March the 10th, 2020, there were 51 responses filled-in into the Qualtrics Survey Software. From this, an export has been made into an SPSS file, where a selection has been made.

To filter out incomplete surveys which would influence the results, a selection has been made based on two criteria. First, question 2.8 had to be filled in. With this criteria, 5 responses were removed from the data: #16, #32, #33, #41, #42, #44. The second criterium was that the set of questions ranging from 3.2 to 3.4 had to be answered. This selection criteria removed two other responses: #19 and #50. The resulting 43 responses were used for analysis.

5.3. Web scan

To test the variable for the security of the websites will be tested by an automated web crawler. This tool looked at multiple properties divided among four categories on which a score is calculated. There will be 377 web domains scanned on vulnerabilities.

Table 7: Web scan properties

Category	Property	Cut off value
Connection	HTTPS	A check will be performed if the website is accessible through HTTPS, if the SSL configuration contains vulnerabilities and if SSL v2 or v3 is being used.
	TLS	A check will be performed if TLS is being used and which version. The configuration will be checked for vulnerabilities. Older versions of TLS contain known vulnerabilities.
	Certification validity	The used SSL certificate will be validated and there will be checked if it is using a self-signed or a CA certificate.
	Wildcard certificate	A check will be performed if a wildcard SSL certificate is being used. A wildcard certificate can not only be used for the main-domain but also sub-domains
Management	SSH	A check will be performed if the server has accessible services for remote access purposes.
	Telnet	A check will be performed if the server has accessible services for remote access purposes.
	File sharing	A check will be performed if the server has an accessible file sharing service running. (E.g. Samba)
	Remote desktop	A check will be performed if the server has accessible services for remote desktop purposes. (E.g. RDP, VNC)
	Management interfaces	A check will be performed if (database) management interfaces are accessible. (e.g. /admin, /wp-admin, /phpmyadmin)
Configuration	Directory listings	A check will be performed if the webserver is vulnerable

		for directory listings.
	Unnecessary files	A check will be performed if the webserver contains any unnecessary files (e.g. readme.html, back-up.zip).
	HTTP Headers	A check will be performed if any insecure HTTP headers are being used (e.g. Strict-Transport-Security, X-Frame-Options)
Security	Domain name security	A check will be performed if the domain names make use of modern security (DNSSEC).
	Blacklisting	A check will be performed if the domain is blacklisted (in e.g. spam filters).

These variables are based on the Top Ten of the Open Web Application Security Project. This is a list of the ten most common critical vulnerabilities that web applications have (OWASP). These are used by BDO to create a comprehensive test, consisting out of numerous checks, on your webserver and the underlying infrastructure. This test tells the current security state of the website.

6. Results

In this chapter the results from the surveys and the web scans will be presented.

In this section the self-administered scores from the general practitioners will be shown. First, the general background of the participants is shown. After that, the computed variables from the conceptual framework will be revealed and explained.

6.1. Background

To understand the population of the survey, additional questions have been asked relating to the characteristics of their office. These background questions will be shown first.

In Figure 16, the distribution of the responding general practitioners is shown. This figure shows that a wide range of general practitioners in respect to their years of experience have responded.

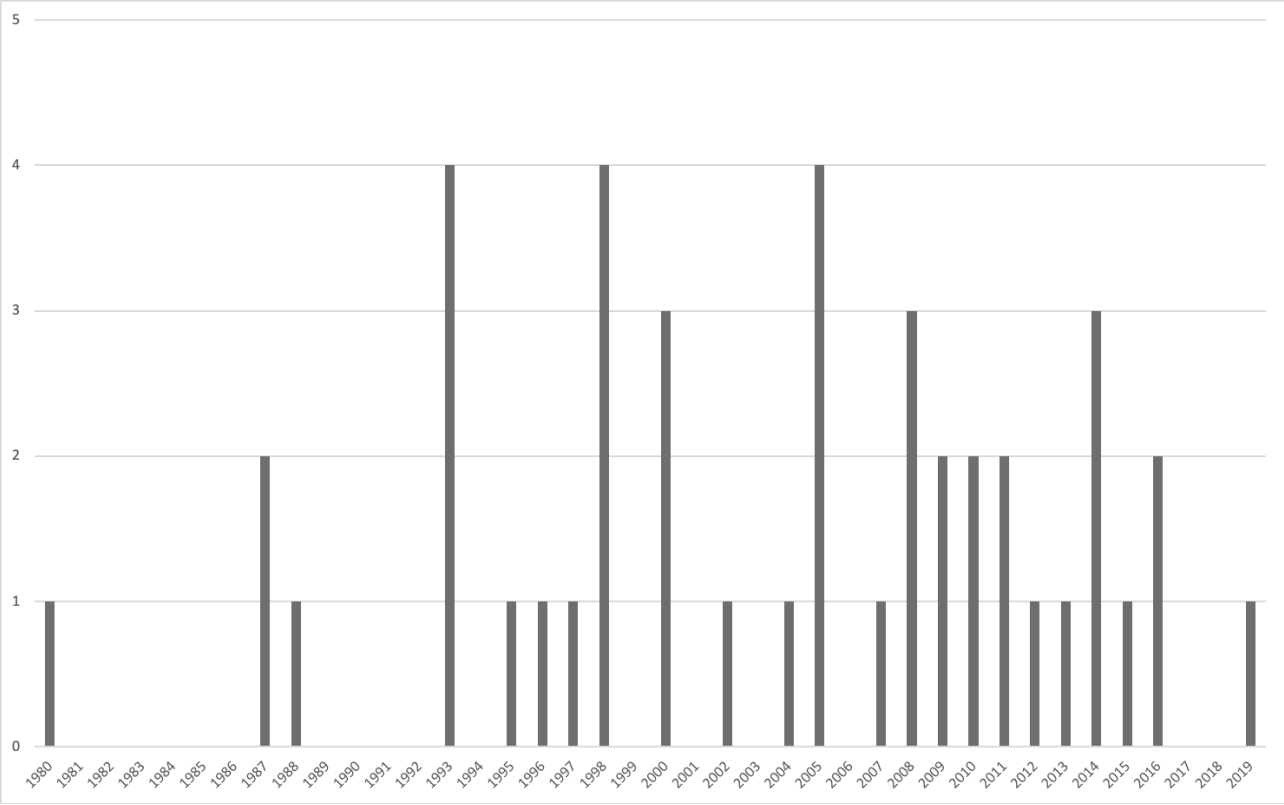


Figure 16: Starting year as a general practitioner

According to the general practitioners themselves, the majority said there was no or just a little attention during their studies for information systems. The distribution is shown in Table 8.

Table 8: Attention to Information Systems

Too much	0	0%
A lot	0	0%
Some	6	14.0%
Little	18	41.9%
None	19	44.2%

According to one general practitioner, it was quite self-evident for the institution that the general practitioner in training would learn about the information system when he/she would start at a practice.

According to filled in surveys, the majority of the general practitioners revealed that there was no or just a little attention during their studies for security. The distribution is shown in Table 9.

Table 9: Attention to Security

Too much	0	0%
A lot	1	4.2%
Some	2	8.3%
Little	12	50%
None	9	37.5%

An interviewee mentioned that there was an appeal done on their morality at their studies that general practitioners had the responsibility to handle patient information securely.

In Table 10 the distribution is shown of the different actors that should be held responsible for the security of the patient website, according to the general practitioners.

Table 10: Responsibility

Technical management or Application Service Provider	30	69.8%
General practitioner/myself	7	16.3%
General practitioner organization (NHG, LHV)	1	2.3%
Other	5	11.6%

In the comment section for the option Others, one general practitioner stated that “as a general practitioner you are responsible in the end, but if you give an assignment to do it according to the LHV-guidelines, you can make the ASP liable”.

In Table 11 the percentage of general practitioners that thought their website had these functions is shown.

Table 11: Functionality Website

	The patient can:	Yes	No	I do not know
1	Request refill prescription	74.4%	25.6%	0.0%
2	Make appointments	67.4%	32.6%	0.0%
3	Get a link to another medical-related website	90.7%	7.0%%	2.3%
4	Get an electronic consult	67.4%	30.2%	2.3%
5	Change their contact data	32.6%	55.8%	11.6%
6	Unregister from the practice	18.6%	76.7%	4.7%
7	Register at the practice	67.4%	32.6%	0.0%
8	Get a referral letter to other medical professionals	23.3%	74.4%	2.3%
9	Examine prescribed medication	39.5%	58.1%	2.3%
10	Examine diagnoses that have been made	11.6%	86.1%	2.3%
11	View test and laboratory results	16.3%	81.4%	2.3%
12	Add self-measurements and remarks to his own dossier	7.0%	90.7%	2.3%

These results are in line with the numbers of the eHealth-monitor 2017 by Nictiz. Here it was shown what the status was of general practitioners their patient-website. 77% of the general practitioners indicated in that report that patients could request refill prescription, 44% could make appointments, 62% could get an electronic consult and 38% could get referred to other medical professionals via their website.

For the roles of maintaining the website two questions were asked. The roles were related to the content management and to the technical administration, which are shown in the Table 12.

Table 12: Website Roles

	Content manager		Technical administrator	
Someone within the practice	32	76.2%	4	9.5%
A professional third party	10	23.8%	35	83.3%

I have no idea	0	0.0%	0	0.0%
Other	0	0.0%	1	2.4%

Most general practitioners do the content managing themselves, although there is a substantial part that uses a third party for this end.

6.2. Variables

In the next section, the results from the respective variables will be clarified.

6.2.1. Perceived severity

Perceived severity is the concept of the perception a general practitioner has about the impact a cyber related risk can have on their practice. The score of perceived severity is based on question 3.2, 3.3, 3.4, and 3.7. For example, question 3.2 asked if the general practitioner was aware of the possible risks concerning the patient web application.

The score is calculated by assigning scores to the respective answers, i.e. +2 for *completely agree*, +1 for *agree*, 0 for *neutral*, -1 for *disagree*, -2 for *completely disagree*. These scores are then accumulated, divided by four to calculate the mean, and then rounded to the nearest half so that they can be binned together. The frequency for the aggregated scores for perceived severity is shown in Figure 17.

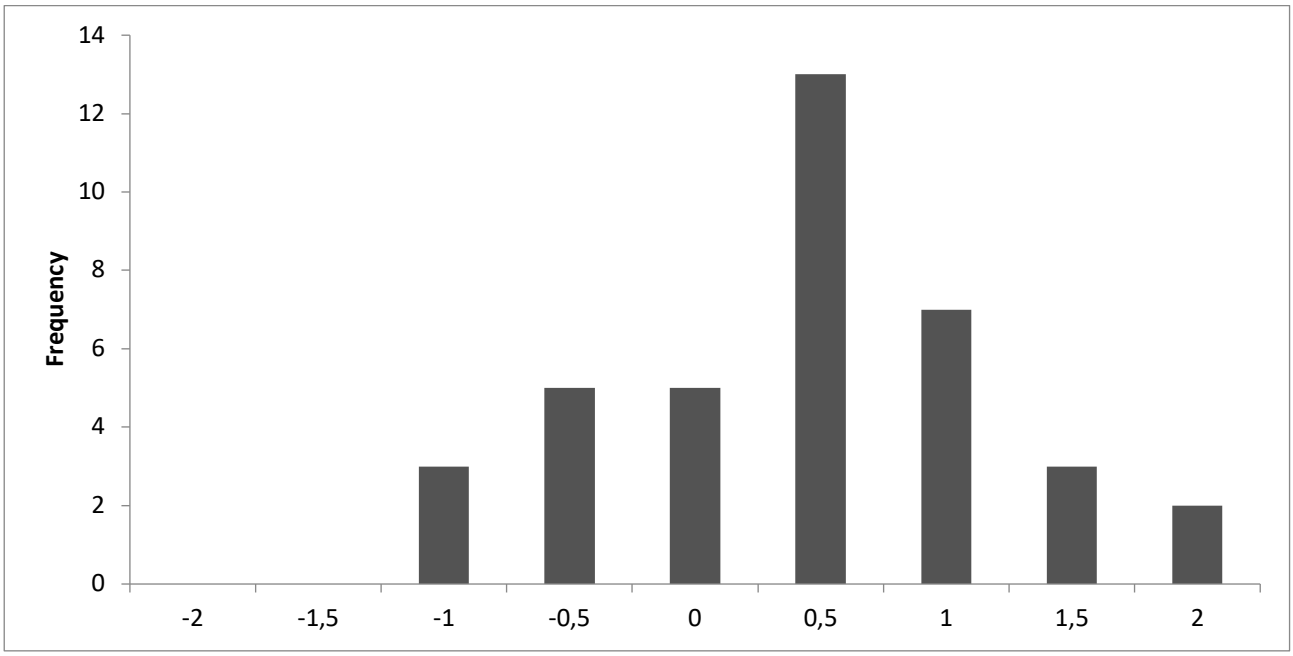


Figure 17: Perceived severity

The overall tendency of the general practitioners is that they think that the impact of a cyber incident could be severe.

6.2.2. Perceived susceptibility

This concept is about the perception a general practitioner has about the possibility that a cyber incident can occur. The perceived susceptibility is based on question 3.5 and 3.8. Question 3.5 asks, for example, if the general practitioner is sufficiently aware of the possibility with which an IT-risk can happen.

The score is calculated by assigning scores to the respective answers, i.e. +2 for *completely agree*, +1 for *agree*, 0 for *neutral*, -1 for *disagree*, -2 for *completely disagree*. These scores are then accumulated, divided by two to calculate the mean, and then rounded to the nearest half so that they can be binned together. The results are being shown in Figure 18.

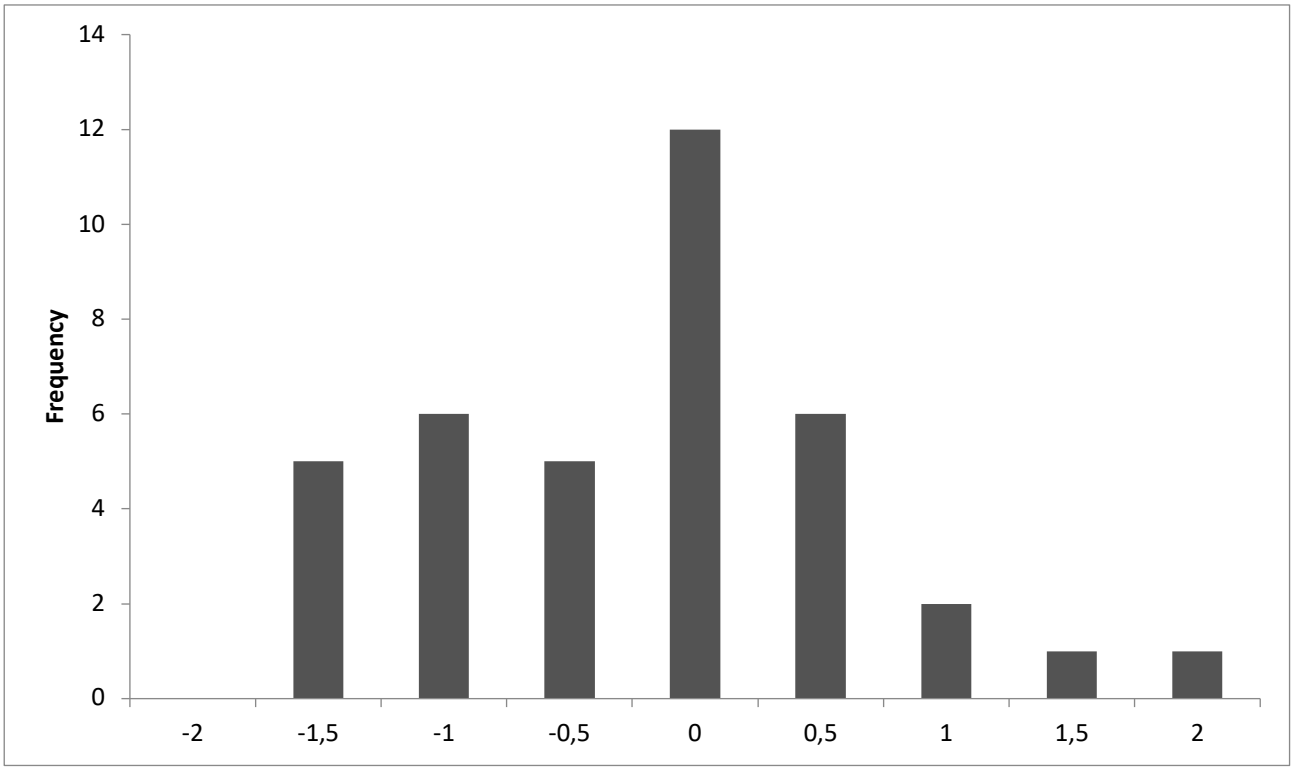


Figure 18: Perceived susceptibility

These results show that the majority of the general practitioners think that there is a small chance that they would be affected by a cyber incident.

6.2.3. Perceived costs

The perception of the cost is the economical barrier it cost to implement countermeasures, as well as the additional time or inconvenience to perform desired behavior. The measure for the perceived costs is a

derivative of question 4.4 and 4.5. *Existing measurements are a hinderance when I perform my work*, is one of the questions.

The score is computed by assigning scores to the respective answers, i.e. +2 for *completely agree*, +1 for *agree*, 0 for *neutral*, -1 for *disagree*, -2 for *completely disagree*. These scores are then accumulated, divided by two to calculate the mean, and then rounded to the nearest half so that they can be binned together. The results are being shown in Figure 19.

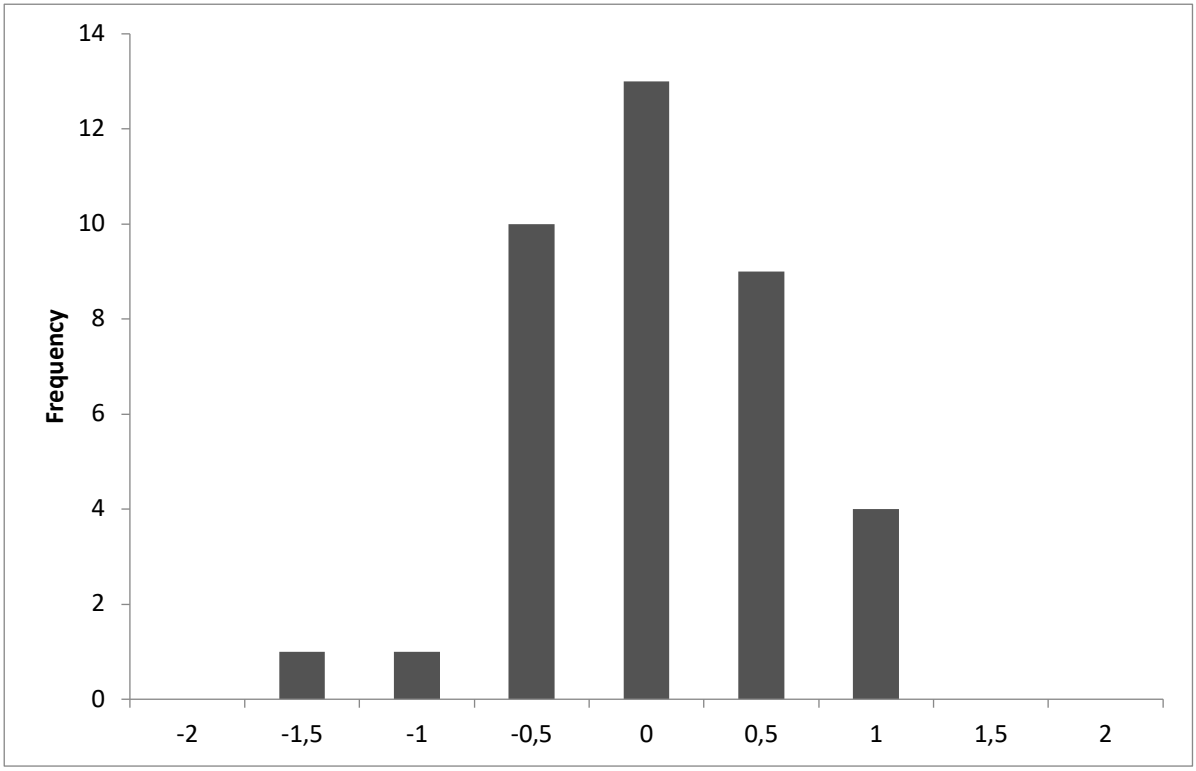


Figure 19: Perceived costs

Overall, the general practitioners feel the economic and non-economic consequences for themselves or their patients not as a burden.

6.2.4. Skills

Skills is about whether the general practitioner has the feeling that within the practice the ability to perform tasks and countermeasures the to reduce cyber risks are present. The measure for the is done by question 4.6 of the survey. The score is computed by assigning scores to the respective answers, i.e. +2 for *completely agree*, +1 for *agree*, 0 for *neutral*, -1 for *disagree*, -2 for *completely disagree*. The results are being shown in Figure 20.

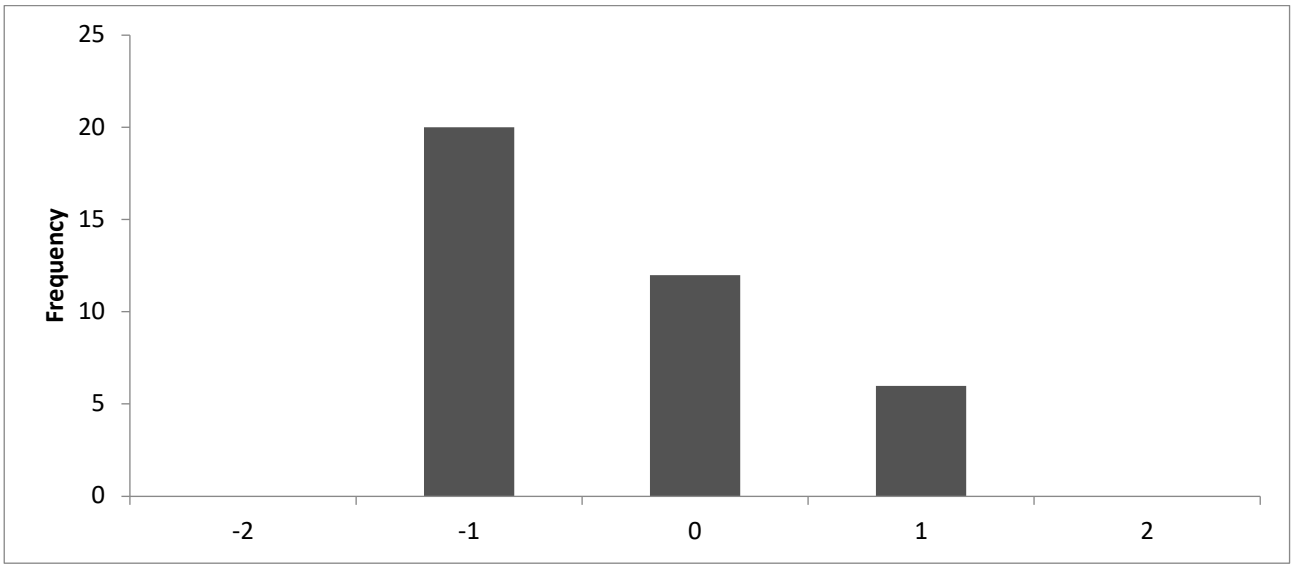


Figure 20: Skills

The perceived skills of the general practitioners are rated to be insufficient although none of the participants completely disagreed with the statement that there were not enough skills within their practice to mitigate IT risks.

6.2.5. Knowledge

For knowledge the question was asked if the general practitioner knew which counter measurements were taken to minimize the risk. This was question 4.2 of the survey. The score is computed by assigning scores to the respective answers, i.e. +2 for *completely agree*, +1 for *agree*, 0 for *neutral*, -1 for *disagree*, -2 for *completely disagree*. The results are being shown in Figure 21.

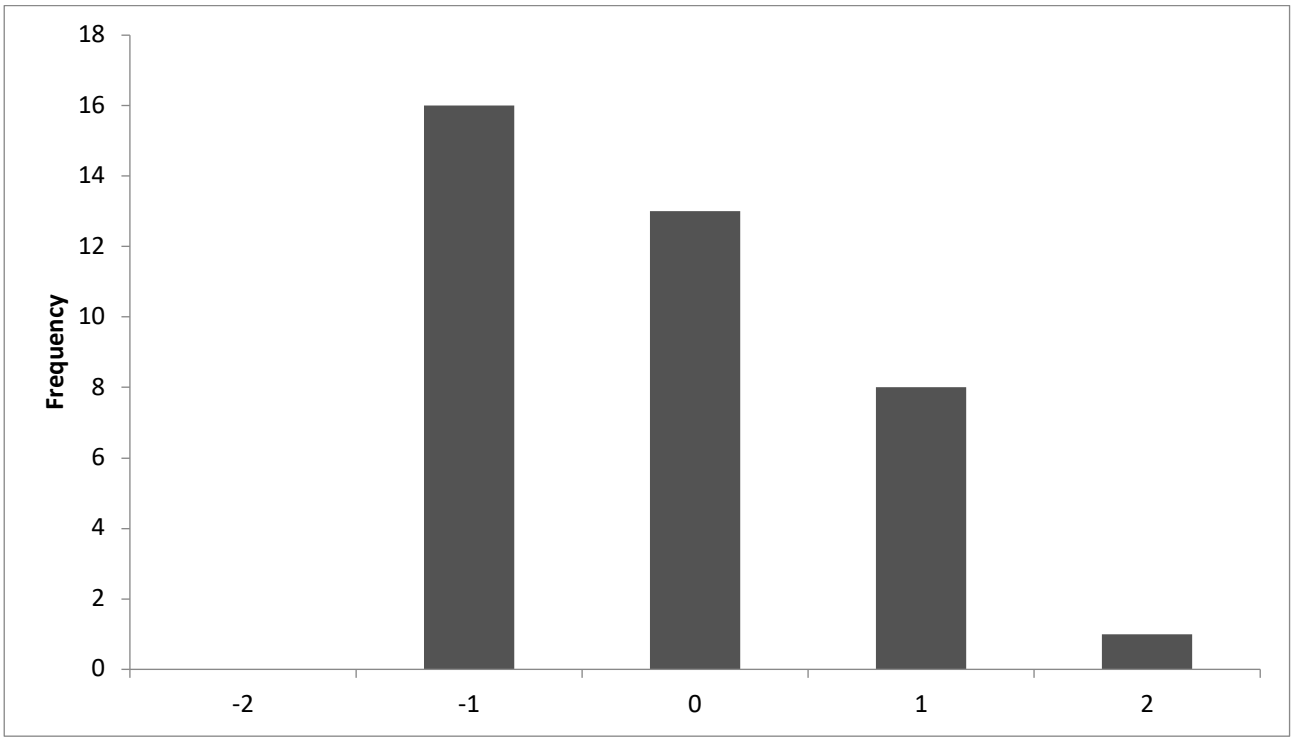


Figure 21: Knowledge

The plurality of general practitioners does not agree with the statement that they know which measures have been taken to minimize risk within their practice.

6.2.6. Self-efficacy

Question 4.10 of the survey measures the self-efficacy of the general practitioners. This question asked to what extend the general practitioner had confidence in that the practice could handle an incident. The score is computed by assigning scores to the respective answers, i.e. +2 for completely agree, +1 for *agree*, 0 for *neutral*, -1 for *disagree*, -2 for *completely disagree*. The results are being shown in Figure 21.

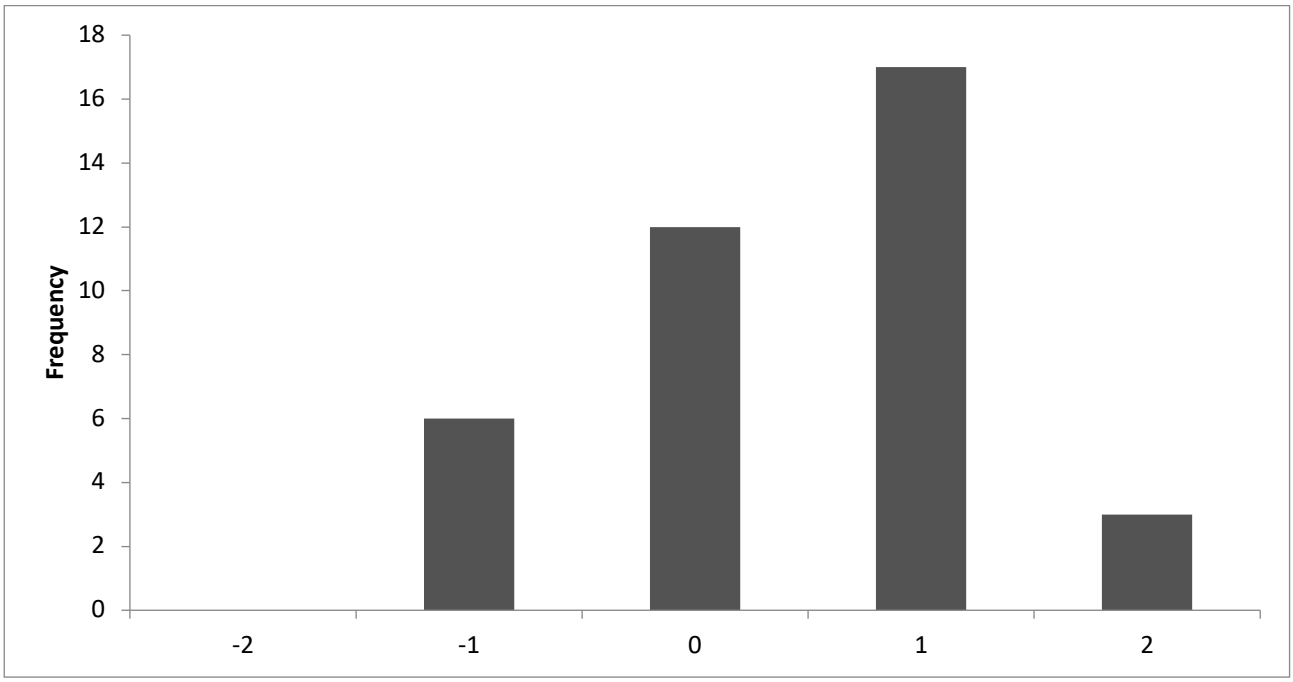


Figure 22: Self-efficacy

In general, the majority of the general practitioners think they will be able to overcome a cybersecurity incident would one occur.

6.2.7. Alignment related behavior

To measure the alignment related behavior, the measure is derived from question 4.3, 4.8, 4.9, and 5.7. With these questions, general practitioners had to answer in which extend they agreed with certain statements. These statements related ranged from how formal the communication between the practitioner and the ASP was, to how proactive the ASP came with new features. The score is computed by assigning scores to the respective answers, i.e. +2 for *completely agree*, +1 for *agree*, 0 for *neutral*, -1 for *disagree*, -2 for *completely disagree*. These scores are then accumulated, divided by four to calculate the average, and then rounded to the nearest half so that they can be binned together. The results are being shown in Figure 23.

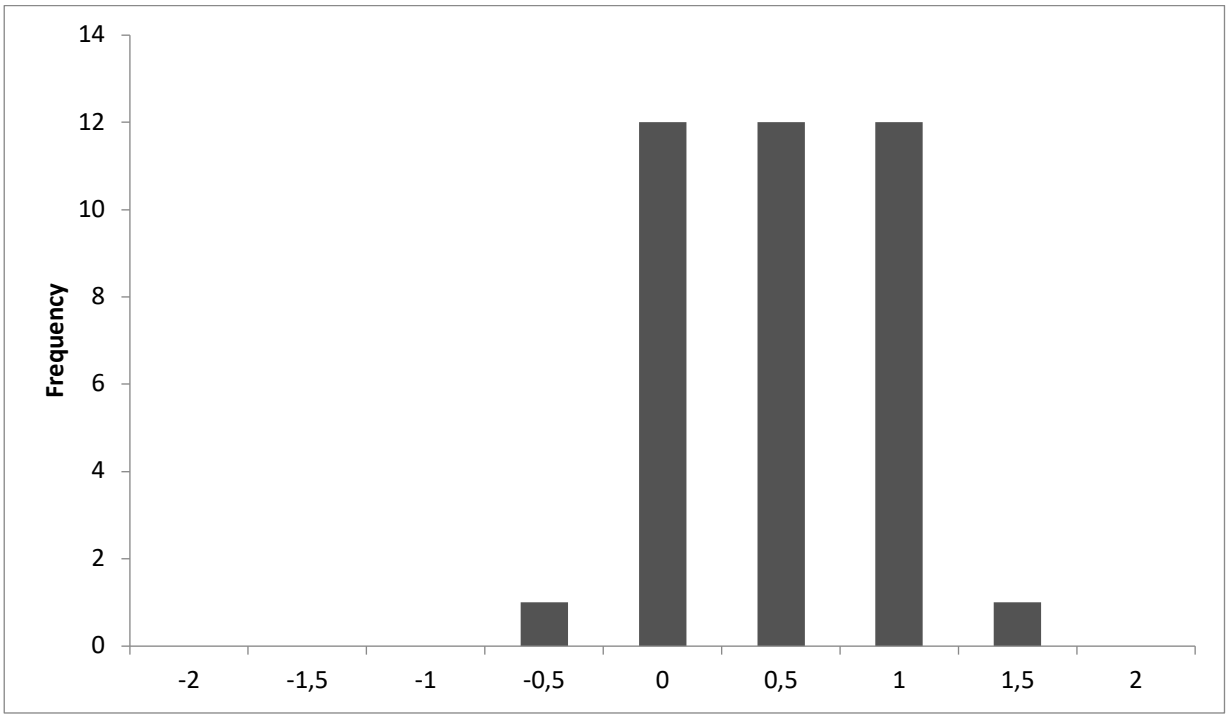


Figure 23: Alignment related behavior

General practitioners in the Netherlands are somewhat active in showing alignment related behavior. This is supported by a general practitioner saying that the technical administrator did come with new security standards, but that he was absent when the strategy was discussed and that he also did not come up with new functionality for the web site.

6.2.8. Cybersecurity

The score ranges from one to five. One means it has a pass on everything, while five means it failed on everything. 377 unique websites have been scanned, and the distribution of the scores can be seen in Figure 24. The mean is 3.8, the median is 3.7, and the mode is 3.6.

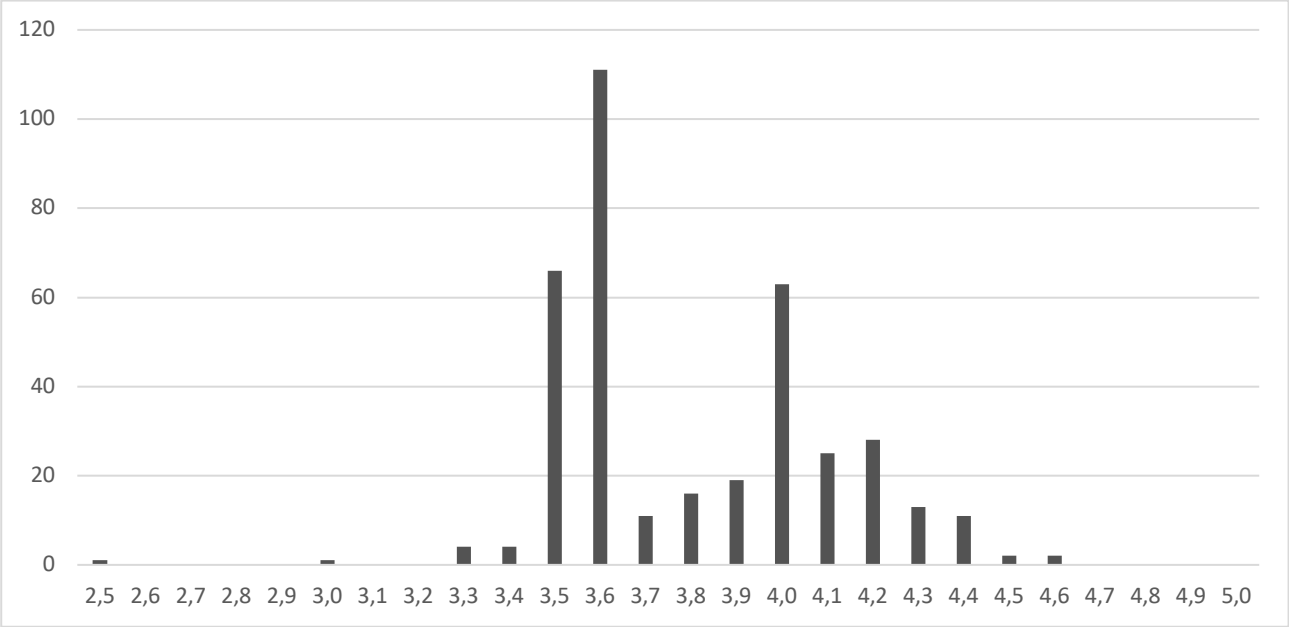


Figure 24: Distribution Websites Scores

The results of the web scan do not differ significantly if grouped by who the technical administrator was.

Table 13: Score grouped by third party

Count	Average score for scan, grouped by	
33	3,8	A professional third party
3	3,8	A friend or relative
5	3,8	Someone within my practice/group
1	3,6	Other:

In Table 14, the percentages of the separate sub scores can be seen. These sub scores show that some aspects of the tested web applications are more often sufficient, while others are more often insufficient.

Table 14: Websites Sub Scores

		Sufficient		Insufficient	
Connection	HTTPS	356	94%	21	6%
	TLS	168	45%	208	55%
	Certification validity	352	93%	25	7%
	Wildcard certificate	214	57%	161	43%
Management	SSH	334	89%	43	11%
	Telnet	377	100%	0	0%

	File sharing	253	67%	124	33%
	Remote desktop	377	100%	0	0%
	Management interfaces	108	29%	269	71%
Configuration	Directory listings	370	98%	7	2%
	Unnecessary files	323	86%	54	14%
	HTTP Headers	8	2%	369	98%
Security	Domain name security	335	89%	42	11%
	Blacklisting	377	100%	0	0%

6.3. Correlations

Although there was a low response rate for the survey, Table 15 shows the correlation between the variables as noted in the previous section: 6.2 Variables.

Table 15: Correlation matrix

	Score Scans	Perceived severity	Perceived susceptibility	Perceived cost	Skills	Knowledge	Self-efficacy	Alignment related behavior	Grade third party
Score Scans	1,00								
Perceived severity	-0,06	1,00							
Perceived susceptibility	0,18	0,72	1,00						
Perceived costs	-0,25	-0,17	-0,09	1,00					
Skills	0,12	-0,01	-0,03	0,05	1,00				
Knowledge	0,48	0,18	0,11	-0,14	0,50	1,00			
Self-efficacy	0,18	-0,03	0,10	0,05	0,25	0,35	1,00		
Alignment related behavior	-0,07	0,25	0,21	-0,02	0,37	0,18	0,40	1,00	
Grade third party	0,21	-0,17	-0,01	-0,11	0,26	0,13	0,01	0,01	1,00

With the low significance in mind, there are some interesting correlations that will be pointed out.

Perceived severity and perceived susceptibility: Correlation of 0.72

This correlation has been shown before in numerous articles. It is good that this research shows the same results to indicate that the set-up of the survey is correct on this area.

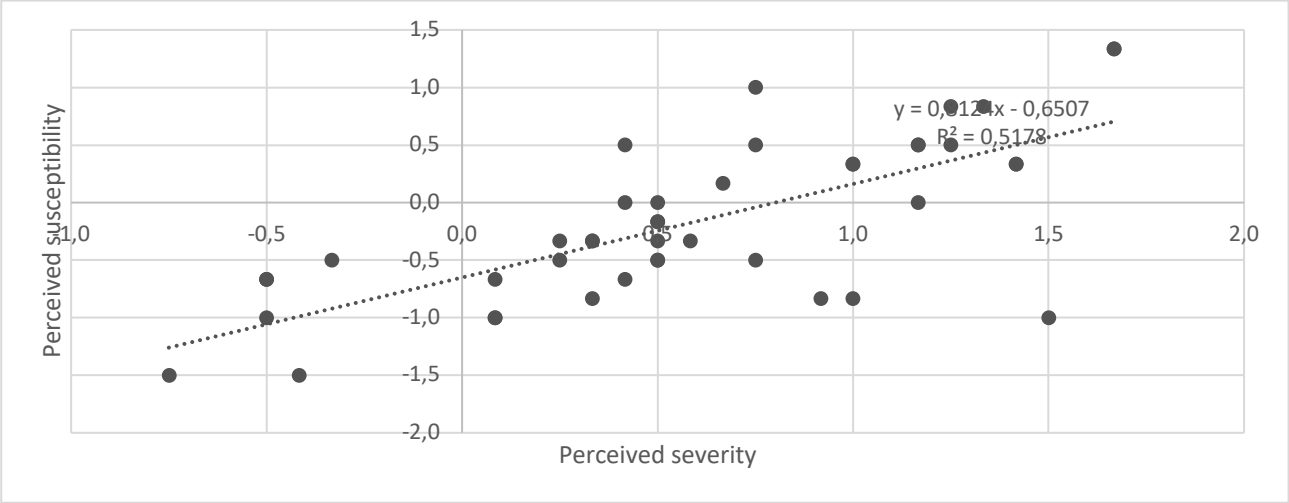


Figure 25: Perceived severity vs perceived susceptibility

Score Scans and Knowledge: correlation of 0.48

Because of the inverted score of the web scans, e.g. 1 is good, 5 is bad, this correlation shows that the higher the knowledge, the lower the actual security of the web scans. This could be because a general practitioner overestimates his/her own knowledge and therefor accepts additional risk.

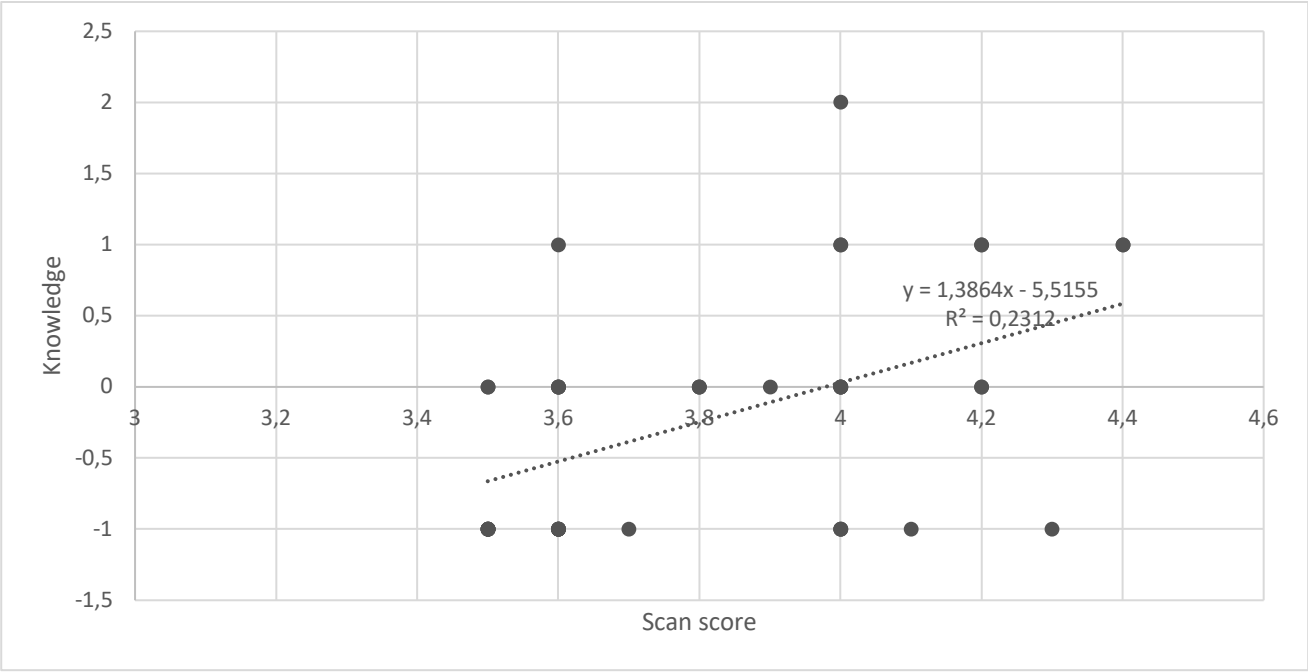


Figure 26: Scan score vs knowledge

Score Scans and Perceived costs: correlation of -0.25

Taken into consideration the inversion of the web score, in the following graph it is shown that a higher perceived cost is correlated with a lower score. This could indicate that general practitioners that are aware

of the economical and non-economical constraints that security measures have, have more secure websites. It is important to note that there is no proven causality, only a correlation.

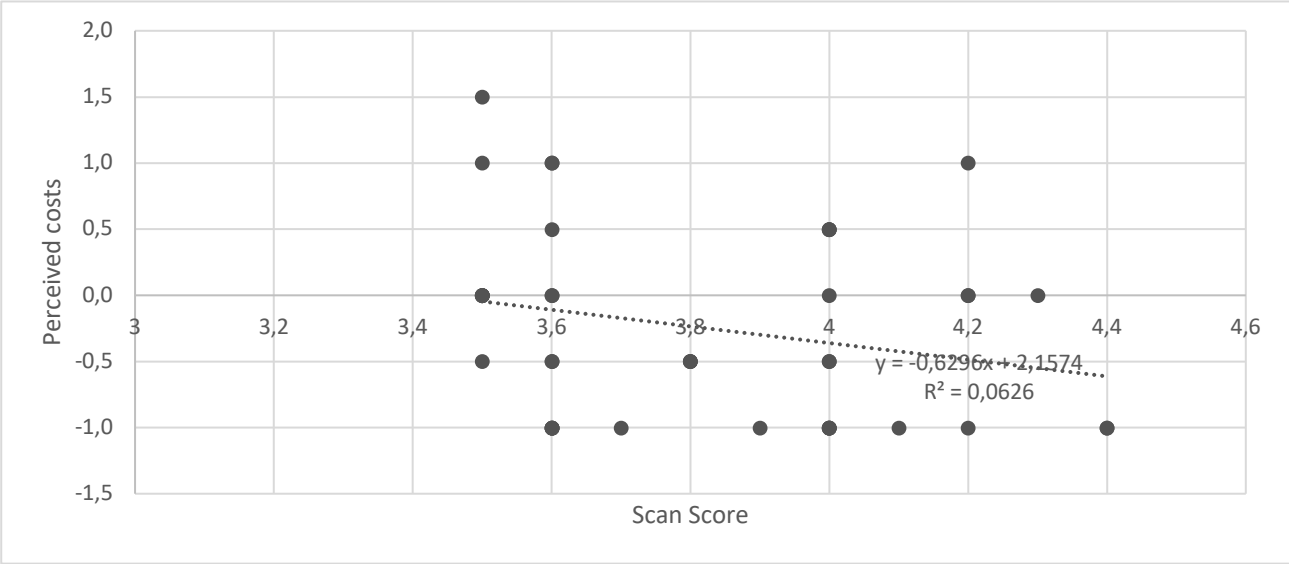


Figure 27: Scan score vs perceived costs

6.4. Hypotheses

Due to the low response on the survey, it is not possible to clearly reject or not reject a hypothesis. It is possible to give a rough estimate though with the low confidence in mind.

In Table 16, the hypotheses and their correlation are given, as well as the results of being disproven or not.

Table 16: Findings hypotheses

Hypothesis	Correlation	Result
H1: Perceived severity positively affects alignment related behavior	0.25	Not disproven
H2: Perceived susceptibility positively affects alignment related behavior	0.21	Not disproven
H3: Perceived cost negatively affects alignment related behavior	-0.02	Disproven
H4: Skills positively affects alignment related behavior	0.37	Not disproven
H5: Knowledge positively affects alignment related behavior	0.18	Not disproven
H6: Self-efficacy positively affects alignment related behavior	0.40	Not disproven
H7: ASP capabilities positively affects alignment related behavior	0.01	Disproven
H8: Alignment related behavior positively affects cybersecurity of web applications	-0.07	Disproven

H1: Perceived severity positively affects alignment related behavior

Because the data shows there is some correlation between the perceived severity of the general practitioners and the alignment related behavior, this hypothesis is not disproven.

H2: Perceived susceptibility positively affects alignment related behavior

The data from the survey showed that there is a correlation between the perceived susceptibility and the alignment related behavior. Therefore, this hypothesis is not disproven.

H3: Perceived costs negatively affect alignment related behavior

The analysis of the survey data showed that there was no correlation to be found, therefore this hypothesis has been labeled as disproven.

H4: Skills positively affect alignment related behavior

Within the analysis, it has been shown that there is a correlation between the skills a general practitioner has and the alignment related behavior he performs. Therefor this hypothesis has been labeled as not disproven.

H5: Knowledge positively affects alignment related behavior

The analysis of the data showed that there is a small but significant correlation between the knowledge a general practitioner has and the alignment related behavior he performs. Consequently, this hypothesis has been labeled as not disproven.

The confidence an actor has in himself to handle a situation correctly, will help him to ask for help and form correct partnerships. Because it is important for the general practitioner's practice to acquire knowledge and skills from outside his organization, this behavior will lead to alignment related behavior. Therefore, the next hypothesis is formed:

H6: Self-efficacy positively affects alignment related behavior

The survey data showed that there is a correlation between the self-efficacy of a general practitioner and their alignment related behavior. Therefore, this hypothesis has been considered as not disproven.

H7: ASP capabilities positively affect alignment related behavior

The capabilities of the ASP and the alignment related behavior did not show any correlation. Hence, this hypothesis has been labeled as disproven.

H8: Alignment related behavior positively affects cybersecurity of web applications

The last hypothesis is considered to be disproven because the data of the surveys and the data of the web scan showed there was no correlation between the alignment related behavior and the cybersecurity of the web applications.

7. Discussion

In this chapter, possible interpretations, as well as possible explanations will be given for the results as shown in the previous chapter.

One aspect that needs to be looked at is the correlation that the more knowledge a general practitioner thinks he has about the security of their website, the worse the actual security of their website is. This could be an indication that the general practitioner gets overconfident and pushes his ideas onto the third party. It cannot be said for certain that the general practitioner decides to let the technical details to be handled by someone else than a professional third party. This is because as Table 13 has shown, the web score does not differ significantly when the website is maintained by a friend or a professional third party.

Another interesting finding is the correlation that if the general practitioner thinks that the costs (both economical and non-economical) are higher, the website tends to be better: it is less vulnerable. This could mean that although the measures to decrease the vulnerabilities of the websites can be a burden for general practitioners, they do actually help. It is therefore important that an application service provider communicates this well with his client.

This could mean that the countermeasures that are a hassle for the practitioner do actually make the website more secure. Or that a GP is willing to spend more money, and therefore is more aware of it, on cybersecurity to make their website more secure.

There is only little to say about the correlation of perceived severity and perceived costs or the correlation of perceived susceptibility and perceived costs. The correlation here is -0.17 and -0.09 respectively. This could mean (keeping the low significance in mind) that the more a general practitioner thinks there is a risk, i.e. severity multiplied by susceptibility, the lower the alleged costs are because he sees that the potential benefit of the countermeasures helps mitigate the comprehended risk, e.g. the benefit outweighs the burden.

Alignment related behavior does not influence score scans, i.e. -0.07. This could indicate that the world of the general practitioner and the world of the application service provider are quite distinct from each other and are not likely to influence one another. If these two organizations would be better aligned first, it would be more probable that the web scan score would improve later on. It could be imagined that there is at least some level of alignment necessary to have an impact on the security level of the web application. If for example there is no alignment, the practitioner can think it is really important, but the ASP will not notice the attitude of the general practitioner. If there is at least some connection between the two, this attitude will be shared more easily and will be noticed.

The grade of the third party and the website score does correlate to some extend: 0.21. This could indicate that application service providers that are genuinely providing better services to practitioners also communicate this well to their clients.

Finally, alignment related behavior correlates well with skills, knowledge, and self-efficacy: 0.37, 0.18, 0.40 respectively. Because they are all part of the overall concept of alignment related behavior as described by Luftman, this is self-evident.

8. Conclusion

In this chapter, the conclusion is given to the three sub-questions as well as to the main question. After the discussion of the limitations of this research, a number of recommendations for future research are described.

8.1. Answers to research questions

First, the three-sub questions will be answered, and in the end, the research question as a whole.

1) *What is the current cybersecurity status of the websites of Dutch general practitioners?*

As seen in section 6.2.8 Cybersecurity, the majority of the web sites do not pass on multiple security characteristics. The overall tendency is that they are prone to security flaws, i.e. from basic techniques like not using HTTPS but HTTP, having invalid certifications, to the extent that management interfaces are open. To put it mildly, there is a great possibility that the vulnerabilities will be abused.

2) *How is the general business & IT alignment maturity of Dutch general practitioners and their application service provider currently?*

As seen in section 6.2, the results show that the alignment related behavior of the general practitioners is moderate. General practitioners do show some alignment related behavior, this is concluded from the surveys as well as the interviews. Application Service Providers do think critically about their area of expertise but do not come proactively with ideas that support the general practitioner's strategy of delivering care to patients. There is no significant behavior that describes a business & IT alignment of a high level of maturity, in terms as described in section 4.3.6 by Luftman.

3) *How should business & IT alignment maturity generally look like between the GP and their ASP to maintain a secure website?*

As seen in the literature explained in section 4.3, there are a few fundamental requirements to support a mature organization. Both parties should look for a shared strategy that they want to strive for. When this happens at the same time when the communication is at a level of understanding and unifying, the business and IT can focus on their aspects and create real value for the overall goal.

What is the most fit conceptual framework for creating Business IT alignment within a general practitioner's office in the Netherlands with regard to their website while keeping cybersecurity in mind?

The most fit conceptual framework is one that connects the separate worlds of the two organizations well, while still making sure that they are not bothered by unnecessary details that they have to focus on. There should be a common level of understanding. But there should also the possibility of delegating the tasks that are of each other's core focus. If this is the case, the ASP can focus on his job while bringing useful features to the general practitioner while keeping the security of web applications in mind.

8.2. Limitations

This study has some limitations. First of all, the questionnaire has been filled out by 51 general practitioners, of which only 43 were usable, while it was distributed to 477 email addresses and to multiple online message boards.

The most likely reason for this low response is that cybersecurity is not a priority of the general practitioners. This can be deducted from the 40 phone calls made to a random selection of non-responding general practitioners and the email conversations with the general practitioners' education centers. One employee of a center mailed: "*Unhappily, we cannot help you further; it does not have our priority. Although it is a relevant point, especially with the upcoming OPEN dossiers*".

Because the general practitioners could choose to answer the questionnaire themselves, the respondents could have had a hidden agenda. They may already have an interest in cybersecurity, thereby introducing bias because they might see the topic of cybersecurity in an overly positive or negative light.

Another inadequacy of this research is the possibility that the general practitioners filled in socially desired answers to the questionnaire. The questions tested the attitudes of the general practitioners as well as the actions. Because the survey was self-administered, the general practitioners could feel less obligated to answer truthfully.

The capabilities of the ASPs were only tested by the perception of the general practitioners. Not by actually measuring the characteristics of the cooperation between the two parties.

The web scanner used was a generic web scan than can also be used for other websites of other industries. This could mean that the rating used in this research is not specific to the use cases of general practitioners.

8.3. Recommendations for Future Research

To counter the limitations as noted above, multiple tactics can be implemented in future research.
To attract the interest of a larger pool of respondents, collaboration with one or multiple academic training institutions should be formed to distribute it evenly among the general practitioners. This would mitigate the limitations of a small sample group, as well as the bias that could come into play because of the self-selection of the general practitioners.

Another interesting area of future research is the difference between the attitudes and the actual actions performed by the general practitioners and their application service providers. Although they could have a positive attitude to a secure and less vulnerable IT environment and web application specifically, their real actions and decisions could be different. In light of the OPEN program, this would be useful to know.

References

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computer & Security*, 97-102.

Liang, H., & Xue, Y. (2009, March). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, pp. 71-90.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, 93-114.

Jorfi, S., & Jorfi, H. (2011). Strategic Operations Management: Investigating the Factors. *Procedia Social and Behavioral Sciences*, 1606-1614.

Byrd, T. A., & Turner, D. E. (2000). Measuring the flexibility of information technology infrastructure: exploratory analysis of. *Journal of Management Information Systems*, 167-208.

Duncan, N. (1995). Capturing flexibility of information technology infrastructure: a study of resource characteristics and their. *Journal of Management Information Systems*, 37-57.

Van Lier, J., & Dohmen, T. (2007). Benefits Management and Strategic Alignment in an IT Outsourcing. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*. Waikoloa: Institute of Electrical and Electronics Engineers.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 394-413.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theretical Models. *Management Science*, 982-1003.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, 273-315.

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess. *Journal of the Association for Information Systems*, 39-76.

Singh, J. (1986). Performance, slack, and risk taking in organizational decision making. *Academy of Management Journal*, 532-585.

Agnew, R. (2001). Building on the foundation of general strain theory: Specifying the types of strain most likely to lead to crime and delinquency. *Journal of Research in Crime and Deliquency* , 319-361.

Fishbein, M. A., & Ajzen, I. (1975). *Belief, attitude, intention and behaviour: An introduction to theory and research*. Reading: Addison-Wesley.

Davis, F. D. (1985). *A Technology Acceptance Model for Emperically Testing New End-User Information Systems: Theory and Results*. Cambridge: Massachusetts Institute of Technology.

Davis, F. D., & Venkatesh, V. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 186-204.

Henderson, J., & Venkatraman, N. (1990). *Strategic Alignment: A Model For Organizational Transformation Via Information Technology*. Cambridge: Center for Information Systems Research.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM SYSTEMS JOURNAL*, 472-484.

Henderson, J., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations . *IBM Systems Journal*, 472 - 484.

Luftman, J. (2000). Assessing Business-IT Alignment Maturity. *Communications of the Association for Information Systems*, 1-50.

Centraal Bureau voor de Statistiek. (2019, June 21). Zorguitgaven; kerncijfers. The Netherlands.

Centraal Bureau voor de Statistiek. (2019, July 15). Bevolking; geslacht, leeftijd en burgerlijke staat, 1 januari. The Netherlands.

Centraal Informatiepunt Beroepen Gezondheidszorg. (2019, October 1). BIG-register_Aantal_geregistreerde_zorgverleners_BIG_register_per_1_oktober_2019. The Netherlands.

Independer. (2015, August 18). *Wat houdt eerstelijnszorg en tweedelijnszorg in?* Retrieved from weblog.independer.nl: https://weblog.independer.nl/huisartsen/wat-houdt-eerstelijnszorg-en-tweedelijnszorg-in/

Nivel. (2017). *Cijfers uit de registratie van huisartsen - Peiling 2016*. Utrecht.

Van der Pluijm, I. (2017). *De Huisarts en de Zorggroup - Perspectief op ondernemerschap en samenwerking*. Rotterdam.

Tweede Kamer. (2017). *Vaststelling van de begrotingsstaten van het Ministerie van Volksgezondheid, Welzijn en Sport (XVI) voor het jaar 2018*. 's-Gravenhage: Rijksoverheid.

InEen. (2016). *Benchmarkbulletin Huisartsenposten 2015*. Utrecht: InEen. Retrieved from www.volksgezondheidenzorg.info.

Nederlands Huisartsen Genootschap. (2019, October 10). *Praktijkvoering*. Retrieved from nhgonline.nl: http://nhgonline.nl/mijlpalen/praktijkvoering/

Stichting Farmaceutische Kengetallen. (2018). *Data en feiten 2018 - Het jaar 2017 in cijfers*. Den Haag: Hemu.

Nederlandse Vereniging van Spoedeisende Hulp Artsen. (2019). *Feiten & Cijfers*. Retrieved from www.nvsha.nl: https://www.nvsha.nl/nvsha/feiten-en-cijfers/

Volksgezondheidenzorg.info. (2018). ziekenhuizen2018_rivm2. Bilthoven, The Netherlands.

Rijksoverheid. (2014). *Wet maatschappelijke ondersteuning 2015*. Den Haag: Overheid.

Rijksoverheid. (n.d.). *Hulp aan ouderen om langer thuis te blijven wonen*. Retrieved October 09, 2019, from www.rijksoverheid.nl: https://www.rijksoverheid.nl/onderwerpen/zorg-en-ondersteuning-thuis/hulp-aan-ouderen-om-langer-thuis-te-blijven-wonen

Rijksinstituut voor Volksgezondheid en Milieu. (2019, April 29). *National Immunisation Programme*. Retrieved from www.rivm.nl: https://www.rivm.nl/en/national-immunisation-programme

Jeugdzorg Nederland. (2019). *Zorg voor de jeugd in 2018*. Utrecht: Jeugdzorg Nederland.

GGD GHOR Nederland. (2019, October 10). *English*. Retrieved from www.ggdghor.nl: https://www.ggdghor.nl/english/

Tweede Kamer. (2019). *NOTA OVER DE TOESTAND VAN 'S RIJKS FINANCIËN*. Den Haag: Rijksoverheid.

Belastingdienst. (n.d.). *Bedragen zorgtoeslag per maand*. Retrieved October 09, 2019, from www.belastingdienst.nl: https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/toeslagen/zorgtoeslag/voorwaarden/inkomen/bedragen-zorgtoeslag-per-maand

Zorginstituut Nederland. (n.d.). *Advising on and clarifying the contents of the standard health care benefit package*. Retrieved October 10, 2019, from english.zorginstituutnederland.nl: https://english.zorginstituutnederland.nl/about-us/tasks-of-the-national-health-care-institute/advising-on-and-clarifying-the-contents-of-the-standard-health-care-benefit-package

Zorginstituut Nederland. (2017). *Pakketadvies in de praktijk*. Diemen: Zorginstituut Nederland.

Zorginstituut Nederland. (2019, October 10). *The Dutch healthcare system*. Retrieved from english.zorginstituutnederland.nl: https://english.zorginstituutnederland.nl/about-us/healthcare-in-the-netherlands

Landelijke Huisartsen Vereniging. (2019, October 10). *Organisatie*. Retrieved from www.lhv.nl: https://www.lhv.nl/vereniging/organisatie

Nederlands Huisartsen Genootschap. (2019, October 10). *The Dutch College of General Practitioners*. Retrieved from www.nhg.org: https://www.nhg.org/dutch-college-general-practitioners

Autoriteit Persoonsgegevens. (2019, October 10). *Mag ik als zorgverlener persoonsgegevens delen via e-mail?* Retrieved from www.autoriteitpersoonsgegevens.nl: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg?qa=mail&scrollto=1

NEN. (2019, October 10). *Waarom een norm voor veilig mailen?* Retrieved from www.nen.nl: https://www.nen.nl/Alles-over-NEN-7510/NTA-7516.htm

Nictiz. (2017). *eHealth-monitor 2017*. The Hague: Nictiz and NIVEL.

ICT&health. (2018, September 7). *LHV ziet verbeterslag HIS, vooral bij e-health*. Retrieved from www.icthealth.nl: https://www.icthealth.nl/nieuws/lhv-ziet-verbeterslag-his-vooral-bij-e-health/

Van der Tang, L. (2014, June 17). *Kijken bij de buren*. Retrieved from www.zorgvisie.nl: https://www.zorgvisie.nl/blog/kijken-bij-de-buren-1543381w/

Nederlandse Vereniging van Doktersassistenten. (2017, April 11). *Koppelen van patiëntendossiers eenvoudig……?* Retrieved from www.nvda.nl: https://www.nvda.nl/nieuws/koppelen-patientendossiers-eenvoudig/

Eikelenboom, S. (2019, October 10). *Peperduur patiëntenportaal houdt innovatie tegen*. Retrieved from www.ftm.nl: https://www.ftm.nl/artikelen/peperduur-patientenportaal-houdt-innovatie-tegen?share=8V4hbZQ2PLngN8lVfI7I2wt5%2BFJxJ7jqnOuPWdELB2ZkGrhwfqqiEdOB%2BBBO

Vereniging van Zorgaanbieders Voor Zorgcommunicatie. (2019, October 11). *Hoe werkt het Landelijk Schakelpunt?* Retrieved from www.vzvz.nl: https://www.vzvz.nl/over-het-lsp/hoe-werkt-het-landelijk-schakelpunt

Landelijke Huisartsen Vereniging. (2019, October 11). *Persoonlijke GezondheidsOmgeving (PGO)*. Retrieved from www.lhv.nl: https://www.lhv.nl/uw-praktijk/ict/persoonlijke-gezondheidsomgeving-pgo

Patiëntenfederatie Nederland. (2019, October 11). *Persoonlijke gezondheidsomgeving*. Retrieved from www.patientenfederatie.nl: https://www.patientenfederatie.nl/themas/persoonlijke-gezondheidsomgeving/

Adviescollege toetsing regeldruk. (2019). *Advies over de (uitwerking van) gespecificeerde toestemming bij elektronische gegevensuitwisseling (Wabvpz)*. Den Haag: ATR, Adviescollege toetsing regeldruk.

MedMij. (2019, October 11). *Veelgestelde vragen zorgaanbieders*. Retrieved from www.medmij.nl: https://www.medmij.nl/veelgestelde-vragen-zorgaanbieders/

Landelijke Huisartsen Vereniging. (2019, October 11). *Online inzage in het patiëntendossier*. Retrieved from www.lhv.nl: https://www.lhv.nl/uw-praktijk/ict/online-inzage-het-patientendossier

Nederlands Huisartsen Genootschap. (2019, October 11). *OPEN: online patiëntinzage in de eerstelijnszorg*. Retrieved from www.nhg.org: https://www.nhg.org/actueel/nieuws/open-online-patientinzage-de-eerstelijnszorg

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating perceived behavioral control, computer anxiety and enjoyment into the technology acceptance model. *Information System Research*, 342-365.

Yayla, A., & Hu, Q. (2009). Antecedents and drivers of IT-business strategic alignment: empirical validation of a theoretical model . *17th European Conference on Information Systems*, (pp. 1-13). Verona.

Luftman, J., & Brier, T. (1999). Achieving and Sustaining Business-IT Alignment. *California Management Review*, 109-122.

Nationaal Cyber Security Centrum. (2013). *Wifi-beveiliging: De onderschatte schakel in netwerkbeveiliging*. The Hague: Nationaal Cyber Security Centrum.

Nationaal Cyber Security Centrum. (2012). *Cloudcomputing & Security*. The Hague: Nationaal Cyber Security Centrum.

Cyberveilig Nederland. (2019). *Cybersecurity Woordenboek*. The Hague: Cyberveilig Nederland.

Erlingsson, U., Livshits, B., & Xie, Y. (2007). End-to-end Web Application Security. *11th Workshop on Hot Topics in Operating Systems* (pp. 1-6). San Diego, CA: Microsoft Research.

National Institute of Standards and Technology. (2001). *Underlying Technical Models for Information Technology Security*. Gaithersburg, MD: U.S. Department of Commerce.

National Institute of Standards and Technology. (2015). *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* . U.S. Department of Commerce.

SANS Institute. (n.d.). *Glossary of Security Terms*. Retrieved November 28, 2019, from www.sans.org: https://www.sans.org/security-resources/glossary-of-terms/

National Institute of Standards and Technology. (2012). *Special Publication 800-30*. Gaithersburg, MD: U.S. Department of Commerce.

US Code Section 3542. (2011). Retrieved November 28, 2019, from www.govinfo.gov: https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf

Mitchell, R. C., Marcella, R., & Baxter, G. (1999). Corporate Information Security Management. *New Library World* , 213-227.

Magnusson, R. S. (2004). The changing legal and conceptual shape of health care and privacy. *Journal of Law, Medicine and Ethics*, 680-691.

International Telecommunication Union. (2008). *Recommendation ITU-T X.1205*. Geneva: ITU.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 13-24.

Wetenschappelijke Raad voor het Regeringsbeleid. (2019). *Voorbereiden op Digitale Ontwrichting*. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid.

Deloitte. (2015). *Cybersecurity of network-connected medical devices in the Netherlands 2015*. Amsterdam: Deloitte The Netherlands.

Deloitte. (2016). *Cyber security of network-connected medical devices in (EMEA) Hospitals 2016*. Amsterdam: Deloitte The Netherlands. Retrieved from https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cyber-security-van-apparatuur-in-ziekenhuizen-kwetsbaar.html

Verhoeven, K., & Dijkstra, P. (2016, June 3). *Kamervragen zonder antwoord nr. 2016Z11086*. Retrieved from zoek.officielebekendmakingen.nl: https://zoek.officielebekendmakingen.nl/kv-tk-2016Z11086.html

Schippers, E. (2016, July 7). *Kamervragen (Aanhangsel) 2015-2016, nr. 3098*. Retrieved from zoek.officielebekendmakingen.nl: https://zoek.officielebekendmakingen.nl/ah-tk-20152016-3098.html

Van Teeffelen, K. (2017, January 6). *Ziekenhuizen beveiligen sites niet goed* . Retrieved from www.trouw.nl: https://www.trouw.nl/nieuws/ziekenhuizen-beveiligen-sites-niet-goed~b8f5d976/

de Volkskrant. (2018, November 26). *Persoonlijke chats van cliënten met psychische problemen buitgemaakt door hackers*. Retrieved September 26, 2019, from www.volkskrant.nl: https://www.volkskrant.nl/nieuws-achtergrond/persoonlijke-chats-van-clienten-met-psychische-problemen-buitgemaakt-door-hackers~b6ec2d95/

Raad van Bestuur Elkerliek Ziekenhuis. (2019, April 10). *Phishing actie raakte Elkerliek ziekenhuis*. Retrieved September 26, 2019, from www.elkerliek.nl: https://www.elkerliek.nl/Elkerliek/Nieuws-overzicht/2019

RTL Nieuws. (2019, April 10). *Groot datalek bij Jeugdzorg: dossiers duizenden kwetsbare kinderen gelekt*. Retrieved September 26, 2019, from www.rtlnieuws.nl: https://www.rtlnieuws.nl/tech/artikel/4672826/jeugdzorg-datalek-dossiers-kinderen-utrecht-email

SAVE: Samen Veilig. (2019, July 5). *Uitkomst onderzoek naar datalek*. Retrieved September 26, 2019, from www.samen-veilig.nl: https://www.samen-veilig.nl/uitkomt-onderzoek-naar-datalek/

Hijink, M., & Raemakers, R. (2019, April 17). *Motie van de leden Hijink en Raemakers over het laten uitvoeren van pentests over toegankelijkheid van medische dossiers*. Retrieved September 26, 2019, from www.tweedekamer.nl: https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2019Z08051&did=2019D16344

Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, 92-97.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 269-282.

Nycz, M., Martin, M. J., & Polkowski, Z. (2015). The cyber security in SMEs in Poland and Tanzania. *7th International Conference on Electronics, COmputers and Artificial Intelligence*. Bucharest: IEEE.

Centraal Bureau voor de Statistiek. (2018, December 21). ICT-gebruik; bedrijfstak, -grootte, 2018.

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's. *Online Journal of Applied Knowledge Management*, pp. 14-26.

Authoriteit Persoonsgegevens. (2019). *Jaarverslag 2018*. Den Haag: Autoriteit Persoonsgegevens .

Authoriteit Persoonsgegevens. (2018, May 31). *AP geeft uitleg over grootschalige gegevensverwerking in de zorg*. Retrieved from autoriteitpersoonsgegevens.nl: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg

Nictiz, & NIVEL. (2017). *eHealth-monitor 2017*. The Hague and Utrecht: Nictiz and NIVEL.

Nederlands Huisartsen Genootschap. (2019, July 29). *Dossier E-health*. Retrieved October 1, 2019, from www.nhg.org: https://www.nhg.org/actueel/dossiers/dossier-e-health

Babbie, E. (2007). *The Practice of Social Research*. Belmont, CA: Thomson Wadsworth.

Thomas, G. (2017). *How to do Your Research Project - A Guide For Students*. London: SAGE Publications Ltd.

Kvale, S. (1996). *InterViews: an introduction to qualitive research interviewing*. Thousand Oaks, CA: SAGE Publications, Inc.

Lofland, J., & Lofland, L. H. (1995). *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis*. Belmont, CA: Thomson Wadsworth.

Krueger, R. A. (1988). *Focus Groups*. Newbury Park, CA: SAGE Publications Ltd.

Saunders, M., Lewis, P., & Thornhill, A. (2010). *Research Methods for Business Students*. Harlow: Pearson Education Limited.

Bell, J. (2005). *Doing Your Research Project*. New York City, NY: Open University Press.

Presser, S., & Blair, J. (1994). Survey Pretesting: Do Different Methods Produce Different Results? *Sociological Methodology*, 73-104.

Polivka, A. E., & Rothgeb, J. M. (1993, September). Redesigning the CPS questionnaire. *Monthly Labor Review*(116), pp. 10-28.

Nicholls, W. L., Baker, R. P., & Martin, J. (1996). The effect of new data collection technology on survey data quality. In L. Lyberg, P. Biemer, M. Collins, E. De Leeuw, C. Dippo, N. Schwarz, & D. Trewin, *Survey Measurement and Process Quality* (pp. 221-248). New York City, NY: Wiley-Interscience.

Krosnick, J. A., & Presser, S. (2010). Question and Questionnaire Design. In J. D. Wright, & P. V. Marsden, *Handbook of Survey Research* . San Diego, CA: Elsevier.

Peter, J. P. (1981). Construct Validity: A Review of Basic Issues and Marketing Practices. *Journal of Marketing Research*, 133-145.

Mitchell, V. (1996). Assessing the reliability and validity of questionnaires: an empirical example. *Journal of Applied Management Studies*, 199-207.

Application Service Provider (ASP). (2019, December 9). Retrieved from www.gartner.com: https://www.gartner.com/en/information-technology/glossary/asp-application-service-provider

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric Theory*. New York City: McGraw-Hill.

Nationaal Cyber Security Centrum. (2015). *ICT-Beveiligingsrichtlijnen voor Webapplicaties*. The Hague: Ministerie van Veiligheid en Justitie.

OWASP. (n.d.). *https://owasp.org/www-project-top-ten/*. Retrieved June 30, 2020, from https://owasp.org/: https://owasp.org/www-project-top-ten/

A. Appendix 1: Survey questions with variable

Table 17: Survey questions with variable

Question	Variable	Face Validity
Q1.1	-	Descriptive text
Q2.1	-	General information
Q2.2	Knowledge	If there was a lot of regard to IT systems, general practitioners are probably more likely to have knowledge
Q2.3	Perceived severity	If there was a lot of regard to the risks of IT systems, general practitioners are probably more likely to have a higher perception of severity
Q2.4	-	General information
Q2.5	-	General information
Q2.6	Cybersecurity of web application	This link will be used as input for the web scanner
Q2.7	-	General information
Q2.8	-	General information
Q2.9	Alignment related behavior	The perception where the responsibility should be for the security of the patient website
Q3.1	-	Descriptive text
Q3.2	Perceived severity	If the general practitioner agrees with this statement, he is more likely to have a higher perceived severity
Q3.3	Perceived severity	If the general practitioner agrees with this statement, he is more likely to have a higher perceived severity
Q3.4	Perceived severity	If the general practitioner agrees with this statement, he is more likely to have a higher perceived severity

Q3.5	Perceived susceptibility	If the general practitioner agrees with this statement, he is more likely to have a higher perceived susceptibility
Q3.6	-	Descriptive text
Q3.7	Perceived severity	The general practitioner estimates what the impact of a consequence would be. A higher estimate would mean that he is more likely to have a higher perceived severity.
Q3.8	Perceived susceptibility	The general practitioner estimates what the impact of a consequence would be. A higher estimate would mean that he is more likely to have a higher perceived severity.
Q4.1	-	Descriptive text
Q4.2	Knowledge	If the general practitioner agrees with this statement, he has knowledge about the mitigation measures
Q4.3	ASP capabilities & Alignment related behavior	If the general practitioner agrees with this statement, he has knowledge about the mitigation measures
Q4.4	Perceived costs	If the general practitioner agrees with this statement, he is more likely to think that the mitigating measurements are a hinderance
Q4.5	Perceived costs	If the general practitioner agrees with this statement, he is more likely to think that the mitigating measurements are a hinderance
Q4.6	Skills	If the general practitioner agrees with this statement, he is more likely to have the skills needed to cope with risks within his practice
Q4.7	Perceived costs	If the general practitioner agrees with this statement, he is more likely to think that the mitigating measurements cost effective. (This is the opposite of Q4.4 & Q4.5)

Q4.8	ASP capabilities & Alignment related behavior	If the general practitioner agrees with this statement, he is more likely to have the skills needed to cope with risks outside of his practice
Q4.9	Alignment related behavior	If the general practitioner agrees with this statement, he is more likely to stay up to date with current countermeasures to mitigate risks
Q4.10	Self-efficacy	If the general practitioner agrees with this statement, he is more likely to think that he will be able to solve incidents within his practice
Q5.1	-	Descriptive text
Q5.2	Alignment related behavior	If a general practitioner has asked a third party to manage the content of their website, the alignment related behavior is higher
Q5.3	Alignment related behavior	If a general practitioner has asked a third party to manage the technical aspects of their website, the alignment related behavior is higher
Q5.4	ASP Capabilities	If an organization has or wants certifications, the organization is capable to provide the technical support
Q5.5	ASP Capabilities	If the organization has specific certifications, the organization is capable to provide the technical support
Q5.6	Avoidance behavior	If the general practitioner knows about the interval of the checks, he is more involved in the security aspect of the patient web application
Q5.7	ASP capabilities & Alignment related behavior	If a general practitioner agrees with the statements, it has been shown in the Strategic Alignment Model that there is more alignment between the GP and the ASP
Q5.8	ASP capabilities	If a general practitioner is satisfied with the ASP, it is likely that there is more alignment between the GP and the ASP

Q5.9	Perceived costs	If the general practitioner mentions any of the options other than “No idea”, it means that there is a higher perceived cost
Q5.10	ASP capabilities	If the organization wants specific certifications, the organization wants to be capable of providing the technical support
Q5.11	Knowledge	If the general practitioner knows which test are performed on his web application, he is more likely to have knowledge about countermeasures
Q5.12	Perceived cost	
Q5.13	Perceived cost	If the general practitioner budgets ad hoc or after an incident, he is more likely to think that the mitigating measurements are a hinderance
Q6.1	-	Descriptive text