BECOMING A QUANTUM SAFE ORGANIZATION: WHY IT IS IMPORTANT AND HOW TO GET THERE

Thesis

Exploring the need and readiness for quantum safe communication, and the strategies that can be formulated as a result.

Marnix ter Haar
Management of Technology

TU Delft

BECOMING A QUANTUM SAFE ORGANIZATION: WHY IT IS IMPORTANT AND HOW TO GET THERE

Exploring the need and readiness for quantum safe communication, and the strategies that can be formulated as a result.

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

Marnix ter Haar

Student number: 4480260

To be defended in public on 23/9/2022

Graduation committee

Chairperson: Dr. J.R. Ortt, section ETI
First Supervisor: Dr. J.R. Ortt, section ETI
Second Supervisor : Prof.dr.ir. M.F.W.H.A. Janssen, Section ICT

Executive summary

The quantum computer is a very promising technology that could benefit society in many different ways. The computing power it could deliver would see useful applications in pharmaceuticals, finance and other areas. However, it can also be applied maliciously, to break current cryptographic algorithms. This would threaten data security across society, and has massive implications. This is called the quantum threat, and it is a threat that is ever increasing with advancements in quantum computing. Estimates for when the quantum threat will break current encryption standards vary between 5-30 years. This requires migration to new quantum safe encryption technologies across the internet. Organizations are also affected, they find themselves in a complex multi actor environment in which they need to prepare themselves for the quantum threat.

To do this effectively managers need to be equipped with the means to devise an appropriate strategy for their particular organization. This begins with understanding how the quantum threat will affect their organization. How big the impact would be of their encryption breaking, and how vulnerable the organization is to an attack by a quantum computer. In this thesis this is referred to as the need of an organization. A model of need is constructed in this research, to provide the first tool a manager can use to think about strategy. Once a manager knows what their need is, they now want to know how to get to a state of being protected from the quantum threat. This question forms the second part of the research, and is called the readiness of an organization. The readiness model constructed here lays out what the path is towards becoming a quantum safe organization. The models provide a useful framework for thinking about strategies to becoming a quantum safe organization. Strategic implications are also given based on the models developed.

Method

The method used to construct the models initially involved a mix of literature study and own contribution. Once the need and readiness models were constructed they were validated and further improved through three cases. The cases were selected according to different levels of need and different industries.

A holistic multiple case study design was used, with adaptions to case questions in between cases. This was done to improve the results in successive cases, as it became apparent that certain questions were obsolete and certain were missing. Two of the cases used interviews as the data collection method, while the third used grey literature(news articles, press releases and other internet sources). This was done out of necessity, but proved to work quite well as the organization in the third case and a lot of information in public.

The cases provided useful validation and new insights that allowed for the adjustment of the need and readiness model. Having the models now complete, strategy implications were now possible to make with the models as the frame and basis for them.

Findings

The first research question concerned the need of organizations for becoming quantum safe. The research resulted in a need model that consists of two main subconstructs, communication pattern and sensitivity of information. The complete model can be seen in Figure 1. Communication pattern consists of the attack surface of an organization among other elements. Attack surface indicating how exposed the organization is to cyber-attacks, here the focus if put on encryption as this is threatened by the quantum computer. The model combines this with sensitivity of information,

which is a measure of how big the impact would be if that particular data is hacked by a quantum computer.

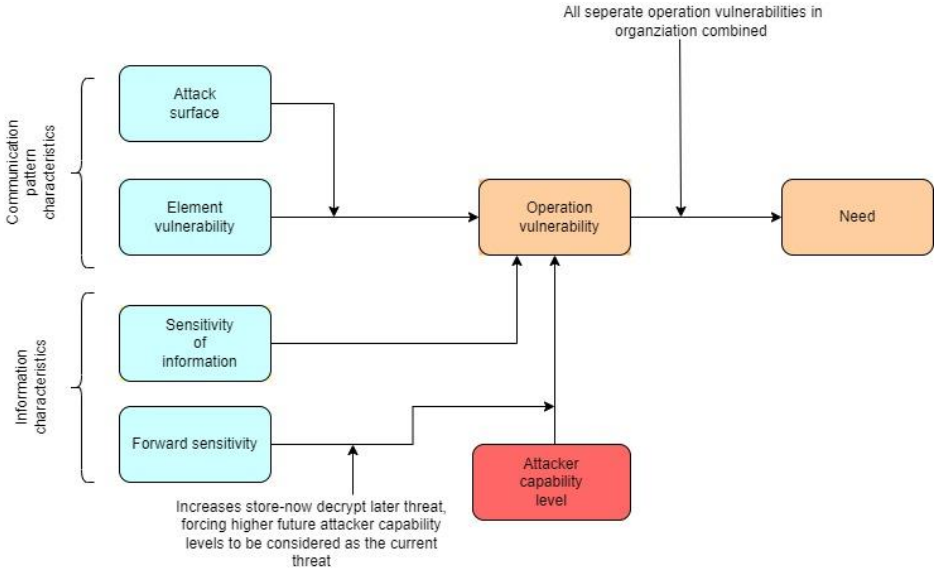

Figure 1: Final need model

The second research question concerned the construction of a readiness model. To construct the readiness model it was first necessary to understand the differences between different readiness streams first. It was apparent that there are two distinct ways to approach readiness, and different literature streams took different perspectives. The two interpretations are:

Readiness progress: How far the organization is in reaching a state of full readiness.

Readiness adaptability: Capacity to implement quantum safe communication technology

Once this was cleared up the thesis focused on one interpretation, readiness progress. The model constructed here splits this process into four phases, the initiation, adoption, implementation and post-implementation phase, as can be seen in Figure 2

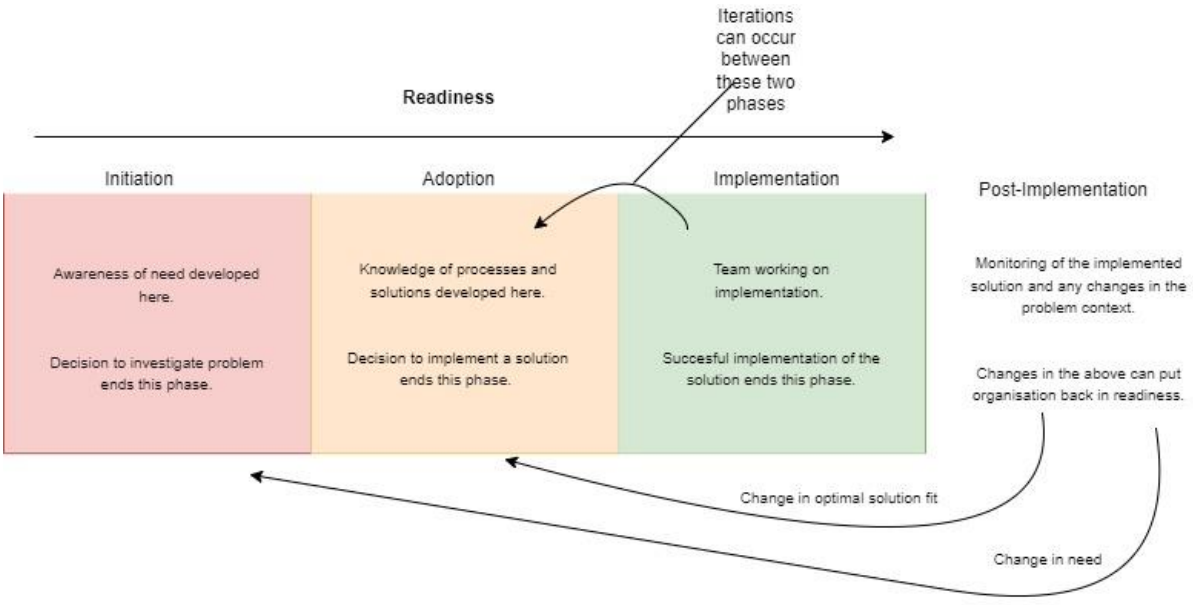

Figure 2: Final readiness model

Next to the phases some important factors where identified that influence how the readiness process will unfold, firstly:

> **Degree of R&D:** The level of involvement in development of quantum safe technologies.

This influences how resource intensive the process will be, and the ability the organization has to integrate the complicated quantum safe technologies. The next important factor is:

> **Crypto agility:** How easily an organizations IT systems can change underlying encryption.

This is an essential aspect that will influence the difficulty of incorporating new cryptographic technology. Finally, an important addition to the seemingly linear model is that in reality these processes are iterative:

> **Iterative nature:** The process of becoming ready in an organization is not linear, it involves different parts of the organization being at different stages, and iterations between attempted implementations and earlier phases.

Next to these findings directly related to the second research question there were some interesting observations concerning the discrepancy between need and readiness. Although the need of the organizations studied here were all relatively high, the readiness of two of the three was comparatively low. This points at a possible market wide issue, where organizations are underestimating their need and how long the migration process will be.

The last research question concerned strategic implications. The models formed a good framework for discussing strategy. It allows for a manager to begin by considering their organizations need and how this impacts their general strategy. Following this, the readiness model allows for a structured approach to strategy in logical phases. Out of these models a number of strategic implications were formulated. The discussion was also split between external and internal strategy These two aspects are related as this is a multi-actor problem in which stakeholders need to coordinate to come to shared solutions. Nonetheless the focus was on internal strategy, for which the need and readiness models formed a good basis. One of the important findings in strategy was the difference between organizations that have high degrees of R&D and low degrees of R&D. The degree of R&D refers to how involved organizations are in the development of quantum safe technologies. Organizations in the low category are dependent on external parties for the development of quantum safe technologies, and need to prioritize cryptographic agility to be able to implement the technologies into their IT. Furthermore, per phase of the readiness model concrete strategy implications were formulated, as can be seen in Table 1.

Table 1: Strategy recommendations per readiness phase

Initiation	Adoption	Implementation	Post-implementation
Understand need Understand complexity Involve people Learn from others Understand external dependence	Understand and develop crypto agility Inventorize operations Prioritize operations Collaborate	Plan for long process Manage iterative nature	Monitor changing technological context Monitor implemented solution

From two of the cases there was a noteworthy finding, namely the adoption of a wait and see strategy. Two of the organizations studied stated that waiting for the market to develop technological solutions and then adopting them is their strategy. This strategy has a number of pitfalls. From the organizations perspective this potentially underestimates how difficult integrating new technology is in this case, and that preparation before these products are on the market Is necessary. Also, from a market perspective this attitude could be problematic. If a lot of organizations adopt this there could be insufficient pressures to develop the necessary technologies in time.

Scientific contribution

A number of scientific contribution have been made, firstly in need literature. A distinction is made between the broad general need definition and specific need. Specific need is in this case formulated for the quantum threat. General need is defined as a gap between the current and the desired end state. This gap is hard to define in many cases, as the states are composed of many elements. The specific need here is approached by looking at the gap between the current and desired state of specific elements, and taking the combination of these as the need. Figure 3 shows this.

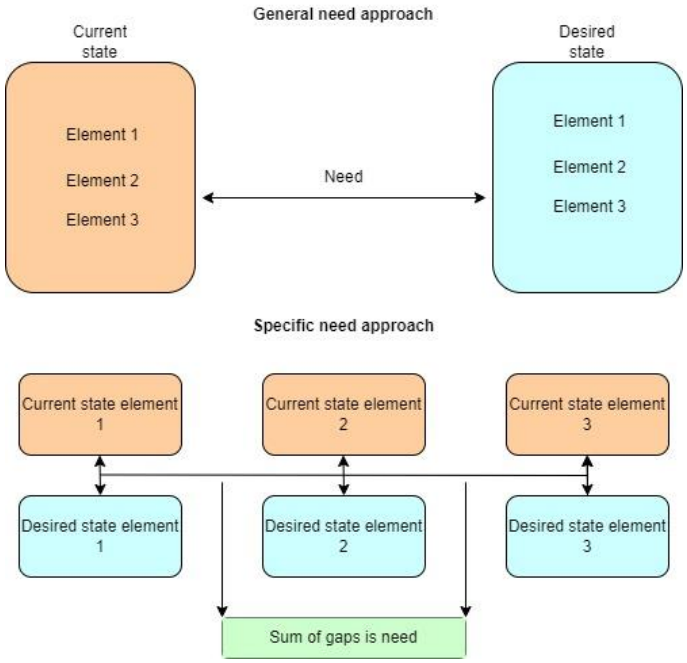

Figure 3: General need approach vs. specific need approach

The next scientific contribution is in clearly splitting the different readiness literature interpretations and streams. The literature uses different interpretations which leads to confusion, here it is outlined that there are two distinct interpretations:

1. A desired end state, meaning that a change or solution has been fully implemented.
2. The ability to change or implement a solution, meaning the ability to implement a change or solution. In other words, the ability to reach a desired end state.

The first falls under readiness progress as defined in this thesis, the second as readiness adaptability. Figure 4 shows what literature stream fall under each interpretation.

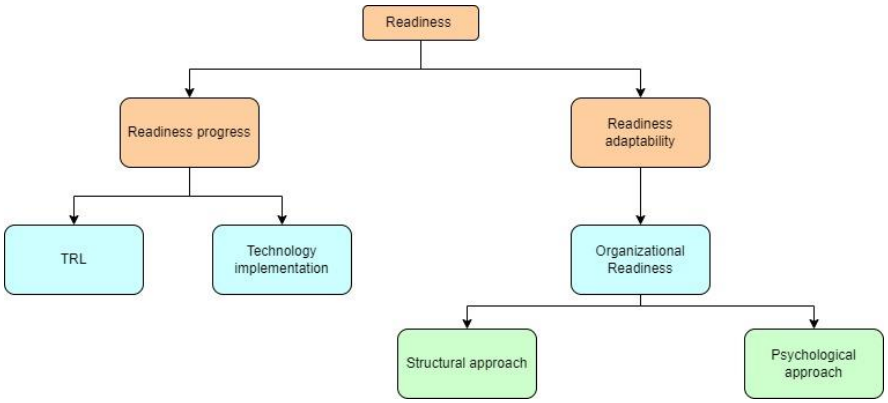

Figure 4: Tree diagram of different readiness streams

The final contribution lies in the approach to strategy through the use of the need and readiness model. This approach allows a manager to first understand the general strategy considerations based on their need. Then, a more detailed strategy per phase of readiness can be formulated.

Overall, the thesis provides a theoretical basis for managers to prepare for the quantum threat. Combining need and readiness into a frame for devising the strategy of an organization.

Table of Contents

List of Figures

List of Tables

List of definitions

Readiness: The extent to which an organization is protected from the quantum threat.

Readiness progress: How far the organization is in reaching a state of full readiness.

Readiness adaptability: Capacity to implement quantum safe communication technology

General need: The gap between the current and desired end state

Specific need: The impact of the quantum threat on an organization's operations.

Attack surface: "The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment." (Ross et al, 2020)

Element vulnerability: The vulnerability of system elements on an attack surface.

Confidentiality: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542].

Integrity: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

Availability: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

Operation vulnerability: Attack surface multiplied by the element vulnerability and multiplied by the sensitivity of information of a particular operation.

Degree of R&D: The level of involvement in development of quantum safe technologies.

Crypto agility: How easily an organizations IT systems can change underlying encryption.

1 Introduction

Quantum mechanics is an area of physics that is not intuitive, as it differs so from the mechanics we are used to in our daily lives. It is a perplexing field that has a lot of very interesting properties that seem impossible. These properties do not only make it an interesting field, but it also lays the foundation for some potentially radical innovations. One of these innovations is the quantum computer, which utilizes quantum principles to perform certain types of computations very efficiently. One type of computation it will be effective in threatens current encryption systems. These computers are not yet powerful enough to pose a threat, but this is likely to happen in the near future. Expert estimates for when this will happen range between 5 and 30 years from now (Dyakonov, 2019).

This threat to current encryption systems can lead to a crisis in data security if no action is undertaken. Organizations with highly sensitive data are the most concerned and have often already implemented counter measures. The first to have done so are governmental parties such as secret services. Commercial parties are also concerned, for instance financial services which deal with sensitive financial information.

This worry is spurring developments towards a potential solution, which is being searched in technologies such as quantum key distribution (QKD) and post quantum cryptography (PQC). Many universities are involved in the development, with the largest quantum technology hubs currently in China and the United States. The Netherlands has also set its intention on accelerating its quantum technology development, with a recent state investment of 615 million euros into the Dutch quantum technology consortium, Quantum Delta NL (Swayne, 2021). The faculty of Applied Physics at the TU Delft plays a large role in quantum technology in the Netherlands, especially with the QuTech research institute. The 615 million euro investment is into quantum technology in general and not specifically in the solutions for the quantum threat. As this is a problem that concerns data security interest and funding to so solve this problem will come from many places.

With a powerful enough quantum computer on the horizon and market adoption of PQC and QKD accelerating we are at an interesting point in time with respect to these technologies. Making choices about what technology to adopt and in what area to deploy the technology is becoming more urgent. Organizations will need to make such choices as well, they must be proactive in protecting their data to ensure their business in an era of quantum computers. Before being able to make such choices organizations need to have an understanding of how the quantum threat will affect their business specifically. Organizations will then be able to adapt their strategy to operate effectively in the new technological environment. To do this organizations must develop an understanding of what their data security needs are with respect to the quantum threat. If they know their need, they are able to prioritize if necessary, assign the right level of resources and develop the right strategy. This is a significant challenge, especially since the problem involves the complex socio technical system of the internet. There are many stakeholders with different interest that interact complexly with each other.

Next to understanding the need an organization has, having a way to determine the readiness is important. This indicates how far they are in the process of becoming quantum safe. Being able to accurately determine this and to see what the path is to full readiness is a useful tool for managers to

develop the best strategy for their organization. So, need and readiness are the focus of the thesis. Further context to the thesis is outlined in the next section.

1.1 Research context

The context was already outlined to a certain extent above, here some more context is added regarding this thesis specifically. The general problem the research falls under is the quantum threat, which is an area that has been gaining more and more attention. A lot of research has been done and is being done on technical aspects of the problem. This is complex research, as it involves a lot of different technologies related to the internet that need to work together. However, not only the technical aspects of this problem are complex. It is a complicated multi actor problem, there are many stakeholders involved that have a lot of dependencies on each other.

The position of an individual organization in this socio-technically complex problem then becomes very interesting. Managers want to be able to navigate it properly, and need the tools to do so. That is what this research is contributing to, as part of the field of management literature.

1.2 Research gap

Identifying a research gap began with the general idea to look at the level of the individual organization in the problem of the quantum threat. The idea was to see what an organization must do to effectively navigate the problem. To do this an organization would first need to know how it will be effected by the threat, which led too looking into need literature. After this, an organization would need to know what to actually do to implement a technological solution. The latter led to looking into readiness literature.

There is a lot of literature on both need and readiness. Need literature is broad and often applied to consumer psychology, as will be explained further later. Applying it to this problem area and at the organizational level has not been done in literature and is the first gap this research looks to fill. Readiness literature has different stream under it, a number of them were explored here in the initial study. The stream of organizational readiness seemed the most logical to explore first, as an organizational perspective is taken. Although the research ended up taking a slightly different path, this was still a good starting point. There was also a gap here, no literature looked into the organizational readiness of implementing quantum safe technologies specifically. In the research implementation literature turned out to be relevant and was also used. There is not any literature on the implementation process specifically for the quantum threat at the organization level, another gap in research.

Next to this, the combining of these two concepts has not been done at least in the context of this problem area. Why this is useful is explained further in the relevance section. Finally, the combination of these two concepts provides managers with a unique framework around which strategies can be formed. With the research gap identified, the problem formulation was now possible.

1.3 Problem statement

As explained above there are two key concepts of interest identified, need and readiness. The combination of these concepts provides a tool for managers to understand where their organization stands with regards to the quantum threat, and what process they need to go through to protect their organizations. Having a tool to measure these two aspects gives managers a framework to

develop their organizations strategy with regards to the threat. This leads to the following main research question:

> **RQ:** *What strategies can be formulated from knowledge of an organizations need and readiness for quantum secure communication?*

The three elements in the research question lead to three sub questions, the first one being:

> **RQ1:** *What determines organizations need for quantum secure communication?*

Here what need entails is first explored, then what determines the need. The goal of the question is to have a comprehensive instrument that allows an organization to determine its need. This part of the research is theory building in nature, the goal is to build the instrument, validate it to a certain extent but not to apply it thoroughly in practice. The readiness element forms the next research question:

> **RQ2:** *What determines the readiness for the quantum threat*?

The first step here is again to understand what the main concept entails, which was more difficult than first thought. In the exploration of the literature it was clear that there are two main ways readiness is interpreted in different streams of literature. The full extent of how this is split up in literature is explained further on in the readiness literature section. For now only the two different types of readiness are defined for this thesis. The first interpretation of readiness looks at how far in the process of becoming quantum safe the organization is. The second interpretation looks at how adaptable the organization is, how ready are they to implement change towards becoming quantum safe. To use an analogy to clarify; the first part looks at how far they are on the journey, the second part at how fast they can move. For the rest of the thesis the different aspects of readiness will be addressed with the following terminology:

> **Readiness:** The extent to which an organization is protected from the quantum threat.
>
> **Readiness progress:** How far the organization is in reaching a state of full readiness.
>
> **Readiness adaptability**: Capacity to implement quantum safe communication technology

Readiness progress ended up being the focus of this thesis, why this occurred is explained in the literature section. The readiness adaptability concept is still addressed in the readiness literature section. The strategy element of the main research question forms the last sub research question:

> **RQ3:** *What strategy best fits the need and readiness of the organization?*

This question is the logical result of the other sub questions, once a manager knows where their organization stands in terms of need and readiness they want to know what to do. So strategies are formulated for the organization, with a focus on the internal strategy. As will be seen later, internal strategy cannot be discussed separately from external strategy, so this will be discussed as well. This research question is addressed in a different way than the other two. As the need and readiness models form the framework for the strategy, it is not addressed in the literature study. Rather, the outcomes of the interviews and cases, together with the models are used to formulate strategy implications.

1.4 Perspective

Two perspectives are taken in this thesis. Firstly, the problem is dealt with from a managerial perspective. Meaning that an organizational level is looked at, with an understanding of the context within it operates. In scope it is further elaborated how this context is dealt with.

There is also an academic perspective on the thesis, meaning that a certain theoretical perspective is taken on the problem. These are the theories of readiness, technology implementation theory and need theory. The general field is management literature, as this is taking the managerial perspective. Readiness theory is quite broad and there are different variations on the theory. What these differences are, and which particular version will be used in this thesis is explored in literature. This theory is brought the organizational level to fit with the goal of this thesis. Also, technology implementation theory will be used to create the appropriate readiness model for this context. Need theory is quite broad and not well defined in literature, as will be shown. The aspects of need that are useful will be used here to make a need model.

1.5 Scope

In outlining the scope of this thesis finding the right balance in what to consider and what not proved difficult. What was immediately clear is that the technical complexity of the problem is very high, as it is dealing with encryption in IT systems. IT systems in organizations are numerous and complex, they are also part of an even more complex ecosystem. The first thought was to somehow simplify the scope here, by for instance only looking at certain types of systems and organizations. The thesis developed differently, instead of going into all the details of the different systems a more zoomed out analysis was applied. This made more sense as the perspective taken is a managerial one, at the top level of organizations. With the analysis at this level of resolution strategies can be formulated well, without getting lost in the details.

The next question in scoping was what kind of organizations to consider. As this thesis looks to establish a measure of need and readiness, organizations that are at different levels are interesting to analyse. That way trends can be seen between organizations. For this reason, the scope in terms of organizations is broad, meaning that the model is generic and applicable to a lot of organizations. The common theme is the quantum secure communications problem. One scope limitation that has been defined is that SMEs are not considered, only organizations larger than that. This to limit some of the extra variables that are at play with smaller organizations. The scope includes both private and public organizations, as this difference does not have a significant effect on the model.

The details of the technological problems and solutions will also not be dealt with in depth here. Enough will be explored to have an understanding of what the technological problem consists of in order to place the model. However, there will not be any elaborate comparison of the different technological solutions for quantum safe communication technology.

The thesis is also not looking to measure need and readiness for a statistically relevant set of organizations in order to compare any possible correlations between the two concepts. That being said, with the limited data to do that some observations on this point are made, as it has interesting implications for possible further research. Rather, the goal of applying the need and readiness to some cases is to validate it and improve to a certain extent. The research is theory building in nature.

The final aspect that needs to be pointed out is that this thesis will only be dealing with the defensive implementation of quantum safe communication technologies. So not opportunities of selling these technologies as an organization.

1.6 Relevance

Relevance is discussed in two parts, societal and scientific relevance.

1.6.1 Societal relevance

To begin with the thesis is relevant from a societal perspective as it provides a tool for managers to make their organizations quantum safe.

This is of significant importance, as the impact of the quantum threat can be enormous if the correct measures are not taken. As the modern organization is so heavily dependent on data in many cases, a breach in data security would devastate businesses. Next to this, solving the quantum threat is very challenging as it involves a complex social technical challenge, it is a multi-actor problem. The time it will take to transfer to quantum safe technologies will be long, if it is to be completed before the quantum computer is here steps have to be made now. Research is an important part of this process.

Next to benefiting organizations, it also benefits society as a whole. Society is dependent on organizations for a lot services, it is of importance that they can entrust them with their data. This goes for employees, customers and other involved parties.

Even on a geopolitical level it is relevant, organizations becoming quantum safe is of importance here. This is because geo political blocks can leverage quantum technologies to attack other economies, steal intellectual property and other disturbances.

Without setting out to do so, the findings of the thesis also brings some possible concerns to light. From the results it seems that need is generally quite high in organizations, and that this is not always accompanied with high states of readiness. This could indicate a problem, but needs to be investigated further before concrete conclusions can be made.

1.6.2 Scientific relevance

Scientifically the thesis is also relevant in a number of different ways. Firstly, it brings the concept of need into a new technological context and adjusts it accordingly. Also, the thesis makes a distinction between the general definition of need and case specific need. It also suggest another way to define the gap between the current and the desired end state(Different than in the general definition of need). It also provides a new model to determine need on the basis of communication pattern and sensitivity. Especially the way communication pattern is broken down into different components to give a model for sensitivity of operations inside and organization is a relevant scientific contribution.

Similarly to need, readiness is also brought into a new technological context and adjusted accordingly. It also clarifies the different interpretations of readiness comprehensively, giving useful reference for future researchers looking into readiness literature. It can give them the tool to see which interpretation is useful for the goals of their research. It then combines the different approaches into a readiness model specifically for the quantum threat.

Finally, something novel this thesis also does is combining the measures on need and readiness into one comprehensive instrument. The combination of the two concepts is a useful framework for an organization to formulate strategies out of. It allows a manager to understand the urgency for its

organization(need), so that priorities and resources can be allocated appropriately. Also, it provides a manager with a clear view of the process the organization must go through to reach full readiness, allowing for effective strategy formulation as well.

1.7 Method

An overview of the structure of the report is given in Figure 5 on the next page. The method taken in this thesis is a mix between literature review, reasoning, and interviews. The research began with literature review, out of which the research gap and problem formulation described above resulted. In this literature review details about the technology where explored, and literature on need and readiness. It became clear that the literature was too broad and that in order to make useful model a different approach was needed than a traditional linear one. Linear meaning first a complete literature review followed by the models.

The method of reasoning and literature review were used simultaneously. The models were built by using reasoning and backing certain steps up with literature. Literature often gave new insights for the correct line of reasoning as well. In the presentation of the thesis this might not be completely apparent, as all the literature used is discussed separately before the models.

The need model resulted in three categories. As these are quite simple categories the choice was made to put the cases studies into the appropriate category from own reasoning. It was not done through an interview method or otherwise, but was validated in them. The readiness model followed the same method as described above, but also included interviews. These interviews where used to validate the model, and to improve them where necessary.

The interview rounds and case were done using a iterative research design. Semi structured interviews were used to validate and discuss the models and potential strategies associated with them. After each interview, the interview design was adjusted to get better results. The details of this method worked are explained further in the relevant chapter.

The third research strategy on strategy was approached differently. Rather than being explored in literature, the point was to use the need and readiness model as a framework to formulate strategies. For this reason, the strategy implications are discussed upon completion of the models, after the interviews and cases.

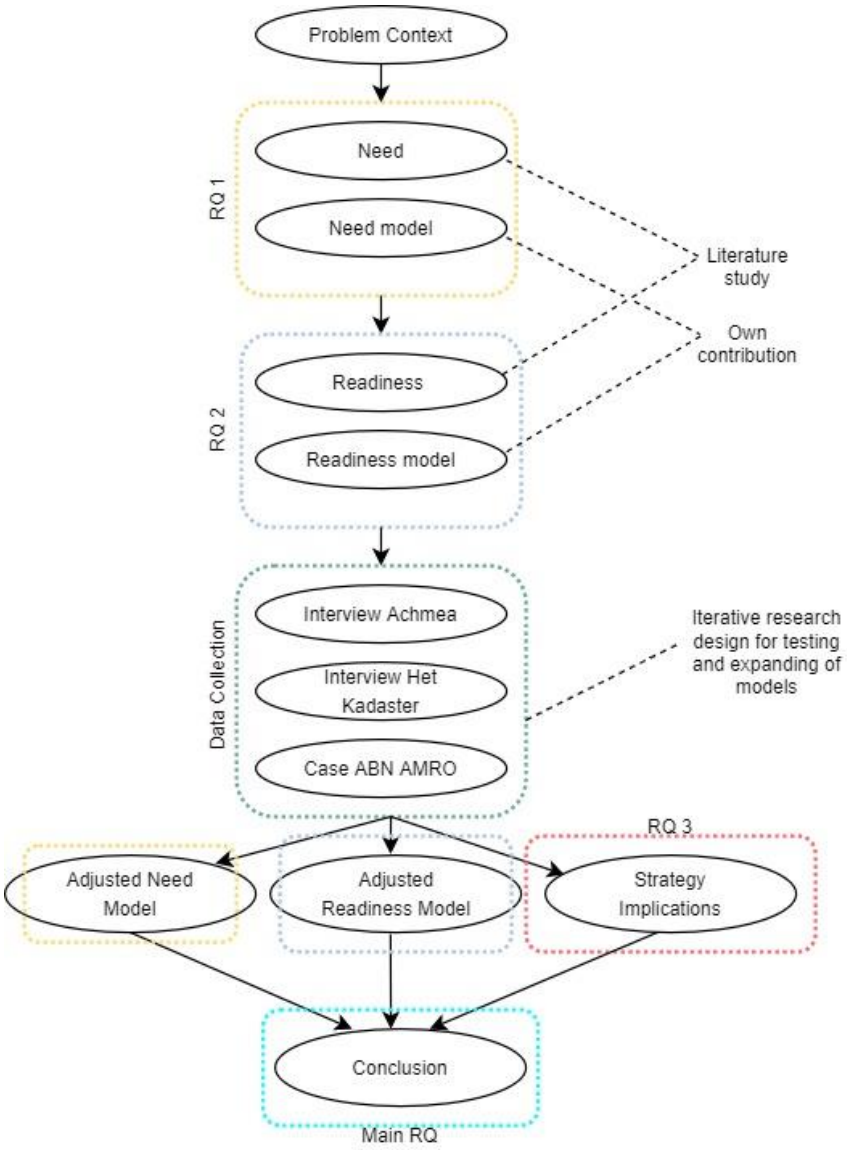

Figure 5: Research structure, with indication of the method used.

2 Problem Context

The goal of this chapter is to give context to the problem, to help place the models described later This is done by highlighting some of the important characteristics of the technologies and the problem in general. There are three parts to this chapter, a discussion of the technology threat, the technology solutions and the problem characteristics. The technology threat is explored to give at least some understanding of what the problem exactly is. This gives context, but is not used extensively in the rest of the thesis. The technological solutions are approached with the same goal in mind, to give an idea of what the technologies are and what they will involve. Lastly, a description of the problem characteristics will be given. This discusses what makes the quantum threat so significant and challenging, by talking about characteristics like the multi-actor aspect of the problem.

2.1 Technology threat

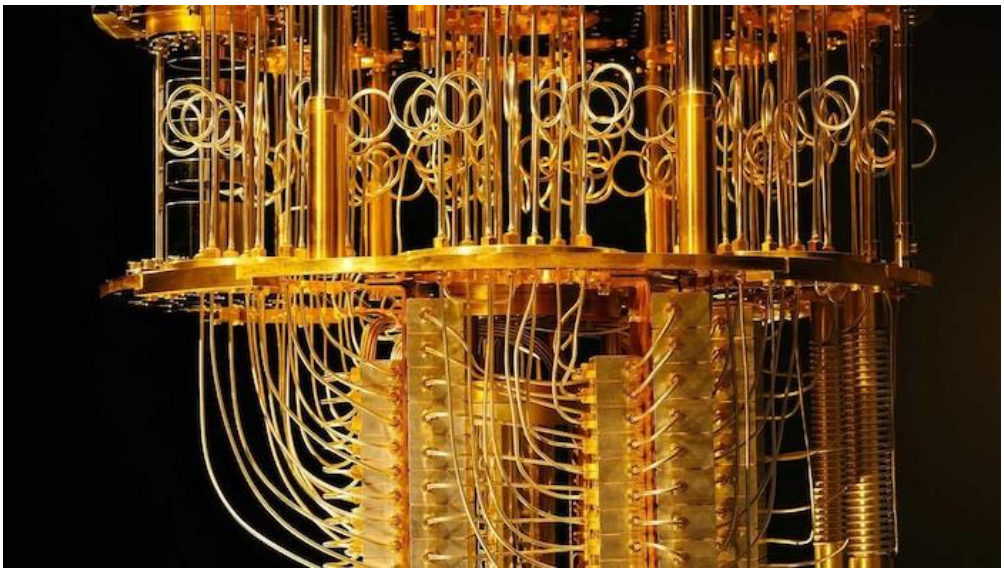

Figure 6: Close up of a quantum computer

The technology threat is explored by looking at two aspects, the quantum computer and what is threatened within current encryption. First a note about the source of the text below, the text heavily cites the source Ortt et. al. 2022. It uses text from that work written by the same author as this thesis and adapts it to the purposes here.

2.1.1 The quantum computer

Quantum computers are more efficient than classical computers in certain types of calculations. This is a result of the quantum computer being based on qubits, as opposed to normal bits in classical computers. The qubit is not a binary system like the bit, due to superposition properties from quantum mechanics a qubit can hold more information than a bit. A bit can hold the value of 0 or 1, a qubit can hold the values of 0, 1 or a superposition of both 0 and 1. This is a perplexing fact that results from quantum mechanics, and allows for certain computations to go much more efficiently.

Without going into too much detail yet, the combination of quantum computing and the quantum algorithms made by Shor (1994) and Grover (1996) will pose a threat to current encryption systems. Once powerful enough, such a computer could solve factorization problems very efficiently with the

Shor algorithm, which threatens an important component of current encryption systems. Which part of encryption it threatens is explained later on, first the estimates of when such a quantum computer is available is discussed.

The estimates vary among experts, there were a number of papers that described expert projections, such as the publication by Dyakonov (2019) in IEEE spectrum volume 56. Here the expert estimates for when a powerful enough quantum computer to break current cryptography is available is between 5 and 30 years from now. The range is wide as it should be, because stating that it will be powerful enough to break current encryption is not specific enough. There are many different types of encryption systems right now which would require a different computing level from a quantum computer. In comparison, the white paper by QED-C, 'A guide to a quantum-safe organization', gives a more elaborate illustration of when a strong enough quantum computer will be developed. It is in line with the 5 to 30 year range but provides more detail. Interesting about the article by Dyakonov is that the author has a significantly less optimistic view of the development time of a useful quantum computer. His view is contrary to most experts, and he substantiates it with logical arguments. On a theoretical level there is also still discussion on whether a large-scale quantum computer is even possible at all. This having to do with a lack of understanding of the transition between quantum mechanics and classical mechanics when scale is increased. In other words, once a quantum computer reaches a certain size it could stop following quantum mechanics and become classical. Nonetheless, most papers do view the threat of quantum computers as imminent. Also, the fact that it is uncertain means that communication systems have to be adjusted for the case that the large quantum computer does develop, the risk is too great to do nothing.

2.1.2 Current encryption

Encryption is the process of converting data into a code, to prevent unauthorized access. This is done through the use of a digital key, which converts the plaintext (the data to be protected) into a cipher text, as shown in Figure 7. The cipher text is not legible without the key, and can safely be communicated over public channels. This process occurs for most information being sent over the internet.

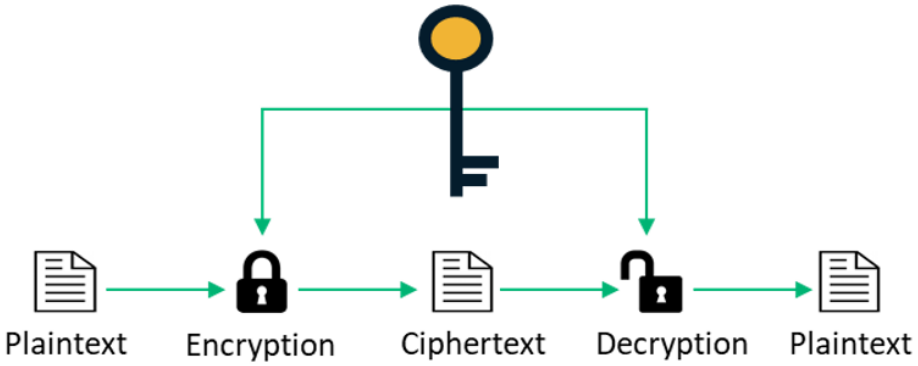

Figure 7: The encryption process (symmetric encryption)

As long as the key is secret the cipher text is impossible to decipher. However, this is exactly the part that quantum computers threaten, they can potentially be computationally so fast that they can do a brute force type attack to find what the key is. A brute force attack consists of trying all possible

combinations of a key until the right one is found. To be completely accurate this is not exactly what a quantum computer will do, they will be able to do a more sophisticated version of a brute force attack. These involve Groover's and Shor's algorithms, and are explained in more detail in a moment.

To be more accurate about what is threatened about current encryption systems some more details need to be explained. In Figure 7 an example of symmetric encryption is given, but this is not the only type. Current encryption systems consist of many different encryption algorithms, most of which fall under two main categories:

Symmetric-key algorithm: A type of algorithm that uses the same key for the encryption and decryption of data. This is not useful for data in transit if both the sending and receiving party do not have a shared secret key (Stallings, 1990).

Asymmetric-key algorithm: A type of algorithm that uses a public and a private key that are mathematically linked through a one-way problem. The public key can be distributed openly without compromising security, allowing two parties with their individual private key to transfer data securely. The private key does not need to be communicated, making it easy to keep secret (Karit, 2016).

These types of encryption form the basis of communication over a public channel, such as the internet. The two types above are combined into so called protocols, which are standard ways of exchanging data safely on the internet. An example of such a protocol is called the TLS protocol, which is used to connect a client to a server on the internet. In other words, when opening a URL to a website such a protocol occurs in milliseconds, ensuring safe browsing. Below the line of code and diagram explaining the steps in a TLS protocol are shown.

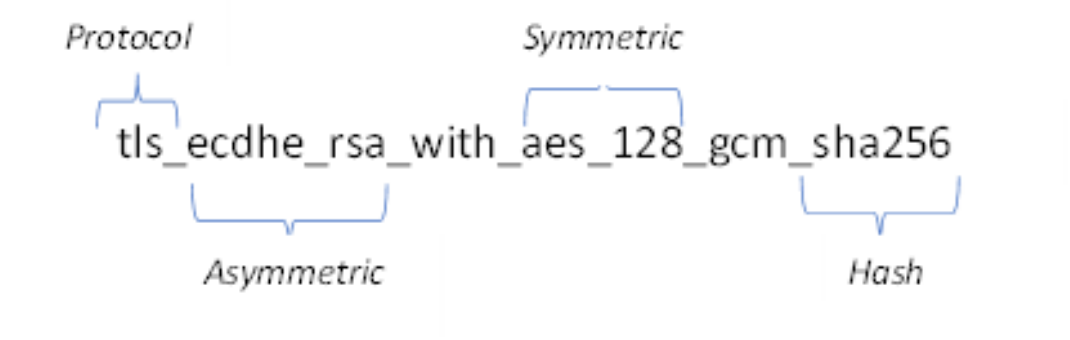

Figure 8: TLS line of code indicating contents of protocol (Krynitsky, 2021).

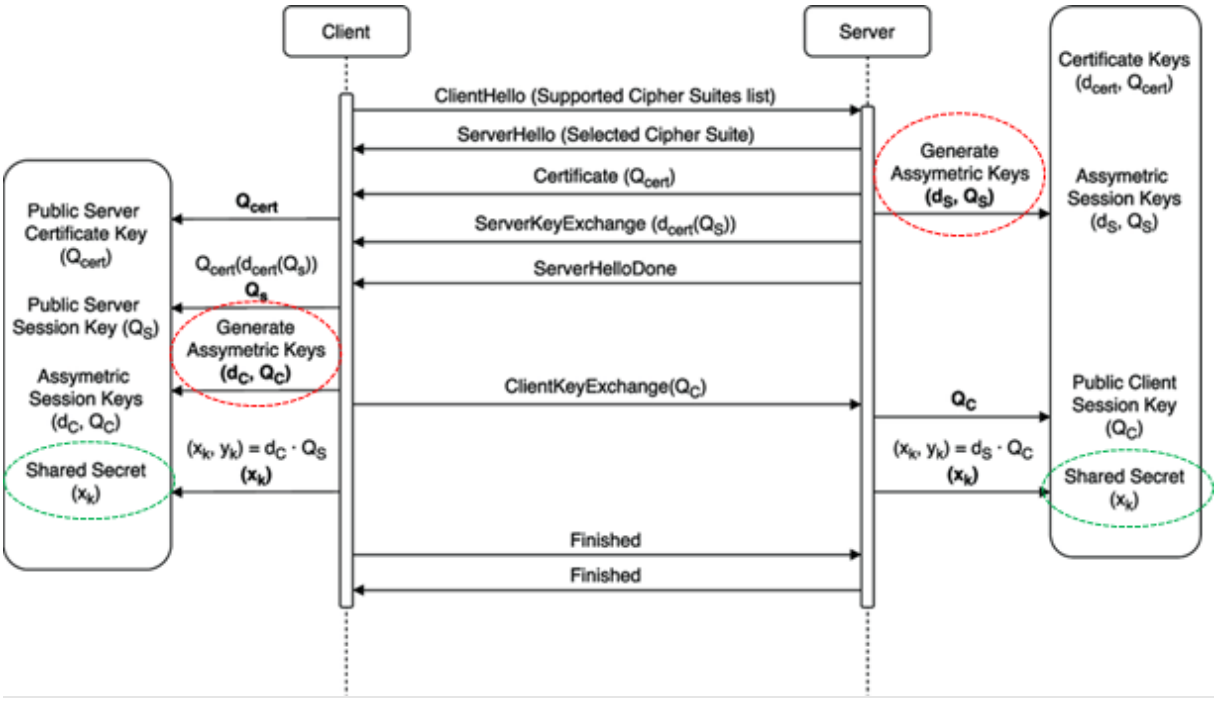

Figure 9: Example of a TLS protocol, a schematic of the protocol (Suarez-Albela et al, 2018).

Above a schematic of a typical protocol used on the internet. In red the asymmetric key creation is highlighted; this is then used to create the shared secret circled in green. Once the shared secret is established the TLS handshake is finished, the data exchange can now occur safely with symmetric encryption.

The details of how the protocol works is not important, there is one take away that is important here. Symmetric and asymmetric algorithms serve different purposes in the protocol. The asymmetric algorithm creates a shared key between two parties, these can be parties that do not know each other. Once this shared key is established, the actual data can be communicated over the channel, which is encrypted with a symmetric algorithm. These different algorithms have different quantum security implications, they are not equally threatened by the quantum computer. The most threatened is asymmetric encryption, symmetric algorithms are less threatened. With a long enough key size, symmetric algorithms are not threatened at all by quantum computers. Table 2 gives an overview of different algorithms and how quantum proof they are. Quantum proof does not refer to whether they are quantum proof now, all the algorithms below are still safe for the moment. It refers to how quantum proof they are when a large quantum computer is developed, of the size that could be developed in the next 5-30 years.

Table 2: Quantum security level of different standard encryption technologies. Modified from: (Muller et. Al., 2020)

Algorithm	***Type***	***Key Sizes (Bits)***	***Quantum Proof?***	***Algorithm Function***
RSA	*Asymmetric*	*1024, 2048*	*No*	*Key distribution*
DH	*Asymmetric*	*1024, 2048*	*No*	*Key distribution*
ECDHE	*Asymmetric*	*256, 384*	*No*	*Key distribution*

AES	*Symmetric*	*128* ***256***	*No* ***Yes****	*Encrypting bulk data*
ECC	*Asymmetric*	*256, 384*	*No*	*Key distribution*
ECDSA	*Asymmetric*	*256*	*No*	*Key distribution*
SHA-2	*Hash*	*256* ***384***	*No* ***Yes****	*Authenticate data*

**Quantum safe currently, developments in quantum algorithms could change this.*

Why certain algorithms are quantum proof and other not has to do with there being different underlying mathematical problems that can be cracked by a quantum computer in different ways. The before mentioned Shor and Grover algorithms can be used by quantum computer to break encryption. Shor's algorithm is a polynomial-time quantum computer algorithm for integer factorization (Shor, 1994). This is good at solving the problem underlying the RSA algorithm, it reduces the effective bit security from 112 for a classical computer to just 25. The effective bit security indicates how many operations it takes for a computer to solve the problem. An effective bit security of 25 would require 2^{25} operations, which is not a lot. For reference, the national institute of standards and technology (NIST) security standards require an effective bit security of at least 112 (Ortt et. al., 2022)

Grover's algorithm is a function that produces a particular output value (Groover, 1996). This algorithm reduces the bit security of AES, but not drastically. The effective bit security of AES-256 reduces from 256 to 128, which is still very secure. Table 3 shows a comparison of effective bit security between classical and quantum computers.

Table 3: Security comparison of two main encryption technologies (Martin, 2021)

Type of Attack	Symmetric Encryption			Public Key Encryption		
		Key Length	Bits of Security		Key Length	Bits of Security
Classical Computers	AES-128	128	128	RSA-2048	2048	112
	AES-256	256	256	RSA-15360	15,360	256
Quantum Computers	AES-128	128	64	RSA-2048	2048	25
	AES-256	256	128	RSA-15360	15,360	31

With this understanding of standard encryption technologies, the problem quantum-proof technologies are trying to solve is a lot clearer. Most importantly, asymmetric-key algorithms are the most vulnerable and are the technology that must be replaced. Symmetric-key algorithms are not the issue, especially if AES-256 is used. These unsafe encryption protocols need to be replaced, as these algorithms underly so many applications on the internet and in digital communication this is a huge challenge.

2.2 Technology solutions

From the literature it was clear that there are two main technologies that are proposed to solve the anticipated problems described above. Those are quantum key distribution (QKD) and post quantum cryptography (PQC). These are not strictly substitutes for each other but are likely to find different

application areas. There are also some other technologies that could provide a solution, although these are less discussed in literature. On example is third party key management systems, another is the use of dark fibre networks.

QKD leverages an important principle from quantum mechanics, the observation principle, to make eavesdropping impossible. In short, when observing a quantum state the state alters, which is information that can be used to detect eavesdroppers. Once detected the communication channel can immediately be terminated. When the channel is deemed safe a shared secret key can be generated between two parties, which can be used for symmetric encryption (which is quantum safe). Such a channel can only be an optical one as qbits in the form of photons are used, specialized hardware is required to use QKD (Mehic et. al., 2020) (Muller et. al., 2020).

PQC algorithms are a software-based technology and replaces the asymmetric algorithms with algorithms that cannot easily be broken by quantum computers. There is currently a standardization process taking place, as there are many candidate algorithms (NIST, 2020). Although PQC algorithms do not require hardware changes in most cases, they do increase the data usage in protocols significantly.

Some of the other technologies include dark fibre, the physical distribution of keys and third-party key management systems like Kerberos. Kerberos is a protocol that has the potential to be quantum safe (Schwenk et. al., 2019). This system is however impractical in large scale applications such as the internet, it is more useful in enterprise networks. Dark fibre is unused fibre that can used as a private channel and the physical distribution of keys involves distributing symmetrical keys through physical messengers to be used in encryption.

There are more technologies next to the ones described above that can play a role in making communication quantum safe. The left column in Table 4 gives a list of a number of these(Ortt et al, 2022).

Table 4: List of different quantum safe technologies and possible hybrid combinations

Quantum safe technologies	Hybrid combinations
Post quantum cryptography	PQC and QKD
Quantum key distribution	PQC and traditional cryptography
Physical distribution of keys	Market segmentation
Trusted digital third party key distribution	Network division
Isolating network parts	Dynamics
Extending current keys	-
Quantum internet	-
Other technologies	-

As can be seen there is quite a range of technologies that could be applied. The point is that it is hard to predict how the market will develop around these technologies, which is an aspect that makes the problem complex.

What makes it even more complex is the fact that these technologies will end up forming hybrid combinations. The right column in Table 4 gives an overview of some of the types. This hybridization is a natural result of applying technologies to a complex system such as the internet. The hybrid

combinations take a number of quite different forms. The hybrid combinations of PQC, QKD and traditional cryptography refers to the being used in combination over the same communication channel. Here some clarification of the other hybrid types:

Market segmentation: Different markets will use different solutions as they have different requirements in things like the required security level, the amount of data communicated and the attack surface of its communications.

Network division: Different layers of the network will use different technologies, for instance the backbone of the internet with QKD and last mile with PQC.

Dynamics: Over time the best solution might shift, first PQC and then QKD for example.

This adds extra complexity to the market situation, and the development is very hard to predict. It will take time before this complexity is navigated and solutions are implemented across the market. This while time is essential, as the development of a powerful quantum computer draws nearer day by day.

2.2.1 Timeline

The problem at hand can be seen as a race of sorts, between the development of the quantum computer and development of defensive quantum safe technologies. As mentioned before the development timeline of the quantum computer is quite uncertain, ranging between 5 and 30 years from now. The development timeline of the defensive technologies, such as PQC and QKD, is also uncertain. An important aspect of these two defensive technologies that will prolong their development timeline is that implementing the technologies will take long. In the case of PQC, migrating protocols across the internet to new standards can take a decade. In smaller scale applications such a migration will not take as long, in fact there are already some applications of QKD and PQC on the market (Ortt et. al., 2022).

To assess the maturity of PQC and QKD Ortt's pattern of development and diffusion (Ortt & Schoormans, 2004) can be used. The model distinguishes three hallmarks, the invention of the technology, the first introduction and the start of large scale production or diffusion of a technology. Between those hall marks there are three phases, the development, adaptation and stabilization phase. Ortt et. al. 2022 asses PQC and QKD according to this model and places both technologies in the adaptation phase. This can be seen in Figure 10 and Figure 11.

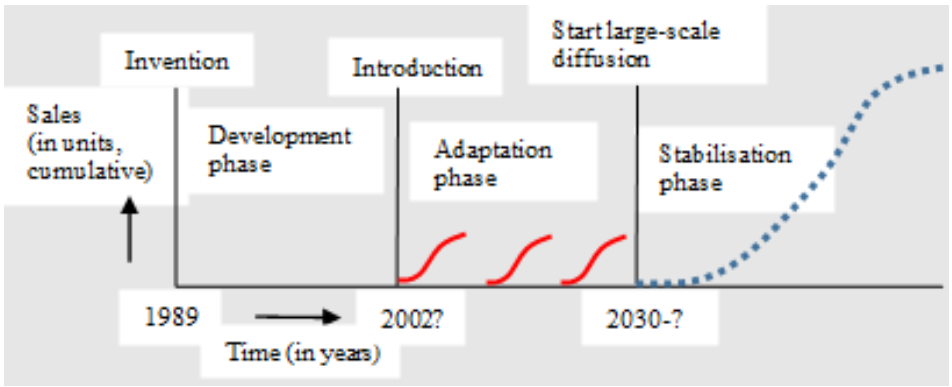

Figure 10: Pattern of development and diffusion of QKD (Ortt et. al. , 2022)

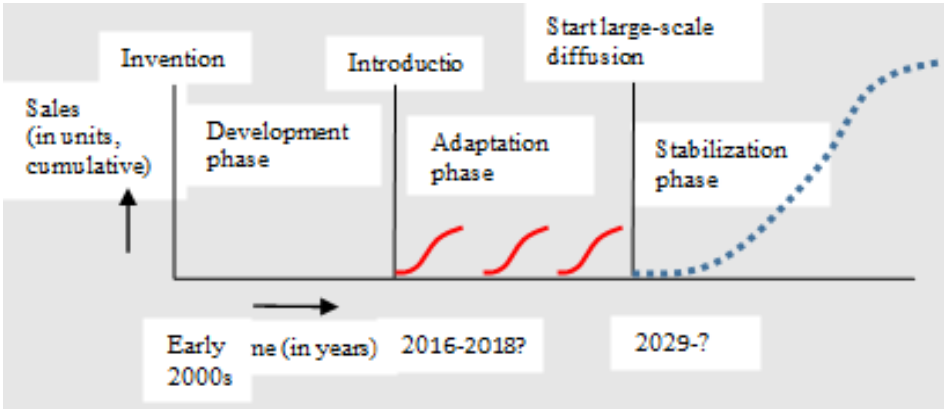

Figure 11: Pattern of development and diffusion of PQC (Ortt et. al., 2022)

Being in the adaptation phase indicates that the technologies are indeed being implemented in certain niche markets already, especially those with high security needs. For both technologies large scale diffusion is predicted to occur around 2030, after which some time will pass until it is diffused across the market.

As a result there is a range of time in which quantum safe communication technologies could be implemented. This will differ for different parties in the market, and will consist of many different technologies in different hybrid combinations. The range of implementation is approximately from now until 2040, by which time large scale diffusion is likely to have diffused the technologies into the market sufficiently to protect from the quantum threat. As the range of the development of the quantum computer is 5-30 years, there is a period of risk where stakeholders are unprotected from a potential quantum computer attack. The longer stakeholders wait with implementing quantum safe technologies, the more likely a breakthrough in quantum computer development will put them at risk.

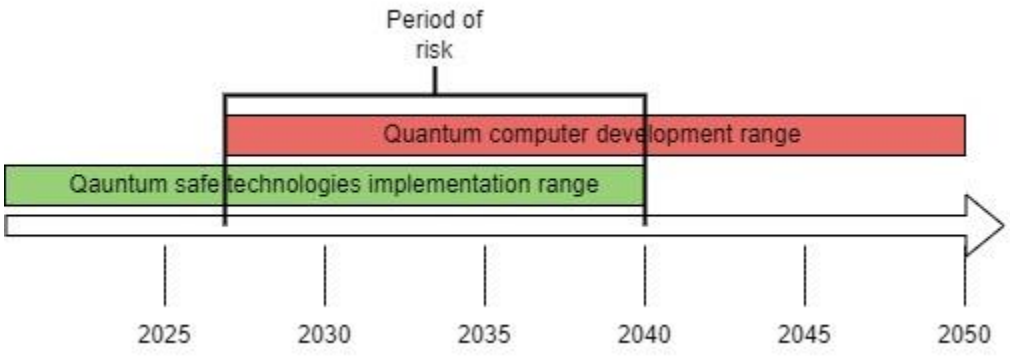

Figure 12: Timeline of the quantum threat highlighting the period of risk

There are a number of characteristics to the problem that make the race described above even more of a challenge for the defensive side, those looking to protect their communication form the quantum threat. These characteristics are discussed next.

2.3 Problem characteristics

Here some of the characteristics are explained that make this problem a challenge. These characteristics are especially important in strategic considerations of organizations , as will be seen later. The characteristics discussed here come out of (Ortt et al, 2022).

Uncertainty: There is uncertainty in two ways, firstly it is not known if and when a quantum computer will be powerful enough to break encryption. This has been highlighted above already, with estimates ranging between 5 and 30 years. There is also uncertainty in how the market will develop around the different quantum safe communication technologies, and how it will exactly be integrated into the current infrastructure.

Asymmetrical nature: The 'battle' between the quantum computer and technologies protecting communication against it is asymmetrical. An attacker only needs to have one quantum computer to be able to attack communication across the whole internet, while the protective technologies have to be deployed everywhere on the internet. In other words, once a powerful quantum computer is developed it can immediately be used to decrypt data, but the protective technologies still need to go through a long deployment process when developed.

Lack of urgency and clear business case: This is a result of the previous two characteristics. It is unclear when the threat will happen so many parties do not yet see urgency. The business case is hard to sell because of the uncertainty, but also because of the defensive nature of the investments to be made. The latter meaning that investing in quantum safe technology does not give a clear return on investment, it prevents losses due to security breaches in the future. This stand in contrast with investment in the quantum computer, which has potential to give massive return on investment in many application areas.

Store now decrypt later: This makes the consequences of a lack in urgency even worst. Encrypted data can be stored now by attackers, who can then wait for the development of the quantum computer to decrypt it. Certain information can still be sensitive in the future, meaning that action has to be taken now.

Technically complex: The problem is technically complex on a number of levels. The individual technologies themselves are complex, but this is not unique as high tech innovations are often very complex. The second level of complexity is more challenging, and that is the complexity of the entire ecosystem into which it must be integrated, the internet. There are a lot of dependencies and cascading effects when something like encryption has to be changed, something that lies underneath a lot of applications run over the internet. This will make solving the problem a unpredictable process where a lot of unforeseen setbacks can occur.

Multi actor nature: Next to technical complexity the actor network is also complex. There are many stakeholders involved in the internet who will need to coordinate efforts to eventually ensure internet wide security. This includes standardization bodies, regulatory bodies, the government, big tech firms and other organizations. As the internet plays such a central role in society it affects almost everybody to at least a certain degree. Organizations will need to coordinate with other actors as the technological solutions have to be compatible so that communication can work over the internet as it does today.

These characteristics of the problem make it an interesting area to study with a lot of challenges. In this thesis these aspects come back mostly in the interviews, cases and strategic implications later on.

2.4 Conclusion

There are two main themes that characterize the problem context, those are uncertainty and complexity. The first source of uncertainty is when(even *if* according to some experts) the quantum computer will be powerful enough to threaten encryption used on the internet. The estimates range from 5 to 30 years, making the uncertainty quite significant. The development of the technological solutions are also uncertain, in terms of the timeline of development and what roles the different technologies will play in the ecosystems. Next to the main solutions of PQC and QKD there are a number of others, all of which can form different types of hybrid combinations in the ecosystem. This uncertainty leads to lack of urgency and difficulty for stakeholders to navigate the problem. Managers will also be faced with the challenges such uncertainty brings, on top of this the complexity of the problem brings even more challenges.

The internet itself is already a very complex system, changes to it are often a challenge. Especially in this case, as the encryption underlying so much of the internet has to be changed. The already complex current encryption systems have to be replaced by complex solutions, while the multi actor network needs to come together to implement solutions that work for all. The complexity makes it a problem that will require a lot of resources and attention to solve, and could lead to a chaotic implementation of technological solutions. This is especially the case if the development of a powerful enough quantum computer occurs soon, in which case actors will scramble to implement any solution they can.

As will be explored further next, in the face of this complexity and uncertainty a manager would need to know to what extent this problem effects their organization. They need to understand their organizations need.

3 Need

In this chapter sub research question one is answered:

What determines organizations need for quantum secure encryption technologies?

First the method used in the chapter is explained, followed by a description of need literature, then the model of need and finally the categorisation of the cases according to need.

3.1 Need Method

The broadness and lack of clear definition of need, combined with a technologically complex problem area made finding an initial direction a challenge. The method consisted of going back and forth between literature and own reasoning. As literature was not specific or very applicable to this problem own reasoning played a larger role in developing the model. This involved going very broad at first, looking at many aspects that could determine need. This quite quickly got overly complex and too focused on details of organisations, while the goal actually is to have a more zoomed out view organisation. Nonetheless, doing this proved an important step, as it allowed to see what all the possible aspects are. After this it is possible to simplify the model to the most important underlying aspect, without missing any important ones. This process is outlined in the sections below, and it is concluded with a complete model.

3.2 Need literature

The need literature search is brief, which is due to the fact that need is not a specifically defined concept in literature. It quickly became clear that defining need in a way that suits this thesis best makes more sense. One source is discussed below that outlines the broadness of the concept of need in literature. After this the concept of communication pattern is discussed, closely related to the concept of attack surface on which literature was also discussed. The, literature on sensitivity of information is discussed. This is also discussed briefly, as only a quite simple categorization of sensitivity was needed for the purposes here.

3.2.1 Need a broad concept

Finding a useful need model is a challenge as the concept is very broad and has many aspects. From literature it is clear that the concept is not very well defined, having many different flavours. In the most general sense, need is defined as follows:

General need: The gap between the current and desired end state

It is discussed often in the context of consumer psychology, and also in the context of human resources management (Leigh et al, 2000). It is an intuitively logical concept, but it is often used in the way that suits particular research. The very general definition given above is applicable in many different ways, and this makes it difficult to use. There is in fact a distinction to be made between the general need concept and case specific need. In order for the concept to be useful a context specific need has to be formulated, which is now going to be done for the quantum threat. As will be seen in the model developed here using an desired end state as a reference point is not straightforward in the context of this problem, rather another approach is used.

To prevent scope creep and an overly complex model a number of simplifications had to be made. These are discussed in the explanation of the need model.

3.2.2 Communication pattern

One of the concepts that is used to define a need model here is the communication pattern. The definition of communication pattern with which the literature study was started was not completely in line with what was found. Initially it was considered as the type of digital communication in the sense of what channel, with which actors and with how many parties. For example, whether the organization communicates certain information over the public internet, or whether they have a large supplier network with which they communicate. In literature communication pattern often referred to a psychological perspective, how people communicate with each other. What turned out to deliver more relevant literature was the concept of attack surface from cyber security. This concepts deals with communication pattern at a more general level. It often takes a more technical approach, which is not necessary here. Nonetheless, the general idea of the concept fits the purposes here well. Attack surface is defined by NIST as:

> **Attack surface:** "The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment." (Ross et al, 2020)

In other words, it looks at the amount of exposure to possible attacks the IT system has. For the concept of need this approach makes a lot of sense, as will be seen later. There is a lot of computer science literature that looks to make a model attack surface (Howard et al, 2005)(Manadhata et al, 2011)). These are often too technical, but some of the elements which such literature highlights are useful to discuss. Every organization has a so called attack surface composition, which is the collection of all elements where an attack can occur. To name a few, this could be IP addresses, internet ports and cloud services. In this problem context, every place where some form of encryption is used is a potential attack surface. The extent to which the attack potential is then significant is dependent on the quality of the encryption. This is the point where the quantum threat plays a significant role, especially as it threatens public key infrastructure.

The point just made about encryption quality determining how likely an attack is at that point is an important one to highlight further. Although attack surface says something about the amount of potential entry points an attacker could use, it does not specify the strength or weakness of that entry point. This is clearly important as well, and it is not the same thing as sensitivity of information(this is discussed further in the next section). This only has to do with the risk associated with the entry point, and not the impact of information leakage. Here this will be referred to as element vulnerability.

> **Element vulnerability:** The vulnerability of system elements on an attack surface.

In other words, the element vulnerability determines how significant the attack surface is in terms of potential attacks. This concept will be a part of the overall need definition later on. The determining of attack surface is a difficult process and too in detail for this thesis. The general idea discussed here is enough for the purposes here. In the need model communication pattern is discussed further.

3.2.3 Sensitivity of information

This concept plays a central role in the need model, so some of the relevant literature is explored here. The goal is to find a way to categorize sensitivity of information in a way that allows for differentiation on the impact of information leak. An authoritative source to consult on this is the National Institute of Standards and Technology (NIST). The 'Standards for Security Categorization of Federal Information and Information Systems' (Bement, 2004) defines sensitivity of information

along three dimensions. It uses confidentiality, integrity and availability. This is commonly referred to as the CIA triad in the field of cyber security. Also, it defines three levels of impact, low medium and high. Table 5 below shows the definitions.

Table 5: NIST definition for sensitivity of information(Bement, 2004)

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The concepts confidentiality, integrity and availability have long histories and are not traceable to a single event or publication. The combination of the three concepts into one triad found its origins in the late 90's(Intellipaat, 2022). The CIA triad is the most standard model used to discuss security of information and is still widely used. It is not the only model found in literature. In 1998 Donn Parker suggested and alternative model, called the Parkerian Hexad. It contained six elements instead of three, confidentiality, integrity, possession, authenticity, utility and availability(Parker, 1998). This model is not widely used, but it goes to show that there are different ways of looking at sensitivity of information. This model will not be explored further, as it goes into a level of detail that is not necessary for this thesis. Also, sticking to the most widely used model makes more sense for the generalizability.

The NIST publication was a result of the E-government act of 2002, where the US government recognized the importance of information security for national security and the economy. For this they defined this standard for categorizing information. It is an official standard for the government, but is widely used outside of government and internationally.

First, it defines confidentiality as: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542].

Then integrity as: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

And finally, availability as: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

Not all of these categories are affected by the quantum threat in the same way. Confidentiality and integrity are both affected directly by the quantum threat. A quantum adversary could decode underlying cryptography of data and break confidentiality, but could also gain access to change data, thereby breaking the integrity. Availability is also affected by the quantum threat but in a different way. In this case the attacker does not need to decode information to break availability, they must simply block access. This does not have to be a quantum adversary. However, some of the technological solutions that are implemented to protect against the quantum threat could be more vulnerable to availability issues. This is something to consider in implementing these technologies.

For the purposes here the three sub-categorizations of sensitivity of information are unnecessary detail. So instead of looking at confidentiality, integrity and availability only sensitivity of information is considered.

The most relevant aspect of this literature is the low, moderate and high categorizations. It looks at the impact that a breach of data security (along the different categories defined above) would have on the operations of an organization, the assets of an organization and individuals. A low categorization has a **limited** impact, medium has a **serious** impact and high has a **sever or catastrophic** impact. In reality the impact data leak has would be a continuum, reducing it to three levels could be argued to be an oversimplification. However, in this thesis the goal is to say something about the need of a range of organizations. In doing this each organization cannot be analyzed in depth, this also goes for the sensitivity of information that they deal in. This is even harder to do on an organization level as there are many different information types with different categorizations being dealt with. So three categorizations is sufficient for the purposes here.

3.3 Need Model

Three steps are taken to get to a simplified model of the need of firms. First the definition of need is given, which is fairly meaningless on its own. Then two main aspects of need in the context of quantum secure communication are delineated. These two aspects are further unpacked, this is where the indicators to be measured are laid out.

3.3.1 Definition

In a very general formulation that comes out of literature need is defined as the gap between the current and the desired state. This formulation needs to be adjusted in a number of ways to be relevant for this thesis. The first issue is that this definition implies that the desired state is known, but in the case of the quantum threat there is not a lot known about the end state. It is not clear when encryption will be cracked by quantum computers, it is even not certain if it will happen at all (Dyakonov, 2019). Nonetheless, organizations must act as if the quantum computer will become powerful enough to break encryption, they cannot take the chance given that the consequences are so large.

Next to this, the desired end state is not the same for every organization. It is dependent on the impact of the data of a firm becoming unsafe. Specifically, the impact on its operations, this gives the definition:

Specific need: The impact of the quantum threat on an organization's operations.

Another reason this definition is more useful in this thesis is that it simplifies need. To be able to categorize organizations according to need easily only the current state is looked at. Essentially, this approach takes need as a function of vulnerability. Note though, that in the concept of vulnerability there is also an implied gap, between a unsafe and safe state. In that sense, there is still a gap in

there. Rather than having the gap defined between two total end states, the gap is defined between sub elements of all the components. This is much more useful as these can be more easily assessed.

Now to take the definition apart more. Operations is a broad term, but the fact that the definition refers to the quantum threat implies that cyber operations are the subject. More specifically, the cryptographic algorithms they are based on. In need the cryptographic algorithm level is not dealt with, the operations are analysed at the level of function for the business. Also, when referring to operations one immediately runs into the problem that there are many operations in an organization. Ranging from daily operations as simple as sending emails to handling client data. Email falling in the category of general operations, as almost every firm has to deal with them. Then there are also more business specific operations, which are usually more relevant to look at in terms of need. Another important realization is that some operations are run on externally managed systems. For instance, a firm might use Microsoft Teams for internal communication and file sharing, the firm will not be able to directly manage the underlying cryptographic algorithms. These nuances are useful to understand, especially when considering strategies to improve quantum readiness. For the purposes of measuring need here this is too much detail to be feasible. Some simplifications have to be made.

One way to simplify is to take a step back and just look at the function of the operations in the organization. Here you look at what the key variables are that determine the impact of the quantum threat on an operation. There are two variables that indicate the impact, both having a slightly different effect. Firstly, the communication pattern or attack surface. This includes what channel, what actors and how many users there are. Most importantly, it also looks at what encryption is used. This impacts need as it determines the exposure to attacks the organization is vulnerable to. The second variable is sensitivity of information, this affects need in how much impact information leak would have. Both are discussed separately below, beginning with communication pattern.

3.3.2 Communication pattern

As explained in the literature chapter determining the communication pattern or the attack surface of an organization is a very involved process. Here a general view is taken, where first the significance of public key infrastructure (PKI) reliance is highlighted. As explained in the technology threat section, current asymmetric encryption is most directly threatened by quantum computers. Current PKI relies on these encryption methods and PKI is what is often used to communicate over the internet. Nowadays, virtually all organizations have a presence on the internet and run operations over it. Although this does mean virtually all organizations will be exposed to the quantum threat, it does not mean they will have equally large attack surfaces on the internet.

This is dependent on how many operations they run over the internet. For example, an organization that makes use of IoT networks with many small devices connected runs many operations over the internet. Next to how many, the concept of element vulnerability as defined earlier has impact. In the example of IoT the element vulnerability can be quite high, as they are often not secured with very heavy encryption algorithms. Element vulnerability is also increased when communicating with unknown or less familiar actors. An unknown actor could be a unverified client, a less familiar actor could be a new supplier. Those are just some examples of how the communication pattern over the internet matters for vulnerability. Next to the internet there are also different ways to communicate digitally, for example over local networks or private networks. These do not use PKI, have less users and less attack surface in general.

It is clearly complex to determine this, and is something that organizations need to do for themselves. Not only to determine need, but also in determining what to prioritize in solving. As will

be seen later, communication pattern also plays a role in the readiness of an organization for the quantum threat, but in a different way. Here communication pattern has to do with exposure to threats, in readiness it influences the type of solution fit that is best suited. This in turn impacts the process of solution implementation, for instance in terms of resources and time required. Given the complexity of determining the communication pattern of an organization, and the fact that virtually all organizations rely on PKI to some extent, this aspect will be weighed less.

3.3.3 Sensitivity

Information, or in this case data, has different levels of sensitivity associated with them. Data sensitivity in this thesis is defined as:

Data that must be protected from unauthorised access to safeguard privacy, security or a competitive advantage of an organization and its clients.

Again, there is a wide range of data types with different levels of sensitivity. For instance, some aspects of sensitivity of information have legal requirements. This is for instance the case with privacy laws. But there are also data types that do not have legal requirements but are still very sensitive, for example intellectual property of an organization. To deal with this wide range of information types categorizing them into levels simplifies the problem. To do this three levels are defined: low, moderate and high sensitivity.

Low: These are data types with little to no repercussions if this data is disclosed. This could for instance be published research or information already available in the public domain.

Moderate: These are data types with moderate repercussions if this data is disclosed. This could for instance be company plans or intellectual property.

High: These are data types with high repercussions if this data is disclosed. This could for instance be IT systems security information, social security numbers, health data or biometric data (such as face-scan and fingerprint).

3.3.4 Combination of communication pattern and sensitivity

To get the overall need of an organization the two have to be combined somehow. This is not as simple as having an overall ‘score’ of both and multiplying them. To begin with, an organization will have a combination of communication patterns unique to it, all having different implications for its attack surface and therefore need. Also, the separate means of communication an organization uses will have different types of information running over it. This is an important detail, given that an organization might be running its more sensitive information over its more secure channels. That would imply that even though they might have large attack surfaces in certain parts of its IT infrastructure and have very sensitive information, if they are not on the same channel the need might not be as high as thought when looking generally. Next to this, in the literature section the concept of element vulnerability was introduced. This was a measure that influenced how significant the attack surface in terms of vulnerability to attack. These variables all combine into the concept of operation vulnerability:

Operation vulnerability: Attack surface multiplied by the element vulnerability and multiplied by the sensitivity of information of a particular operation.

This then determines the vulnerability per operation and not the organization as a whole. To get the need of the whole organization all the operations would need to be mapped. The overview given in Figure 13 below shows what the need model now looks like. The question is then what determines the overall need, one option is to take the average of all the operation vulnerabilities. The other is to

take the operation with the highest vulnerability and take that as the need. The first method could cause the need to be underestimated if there are many low vulnerability operations and one high one. Yet, the impact of that one operation being hacked could be very significant. So, taking the operation with the highest vulnerability as the need makes more sense. In the case mentioned above where one operation has high vulnerability, a relatively small intervention could then significantly reduce the need and make the organisation ready. This is an example of how need and readiness influence each other, and is explored further in the need vs. readiness section.

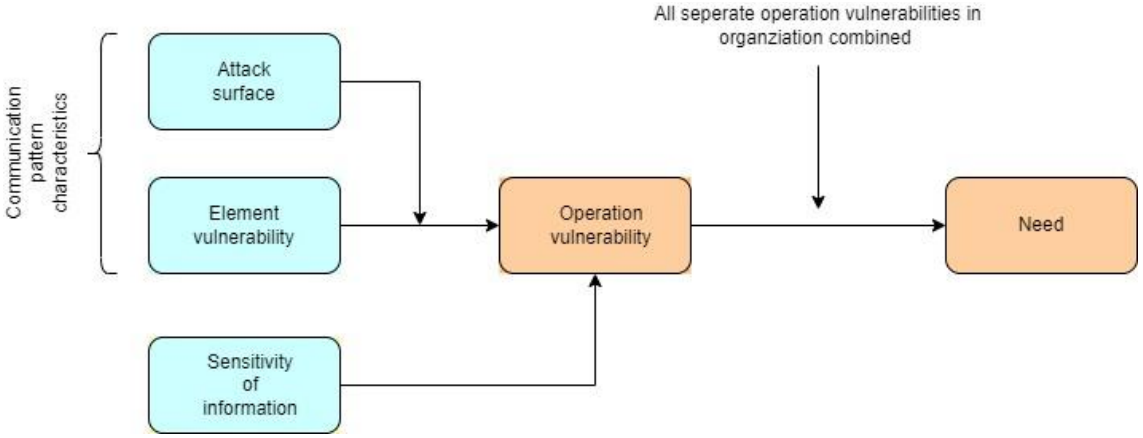

Figure 13: Overview of communication characteristics that determine need

Although interesting, the details of how to exactly calculate need best is not of much use here as it will not be used. It is however useful to understand better what makes up need, and the insights presented above are useful for an organization to think about its need and how to act on it. So, the most accurate way to determine need would be to map the attack surfaces, determine the element vulnerability of the surfaces and the sensitivity levels of the information per operation. These would then be combined somehow to determine the overall need. This is not feasible to do within this thesis, so here compromises are made.

Here communication pattern will be weighed less than sensitivity of information. There are two justifications for this simplification. Firstly, due to PKI reliance of virtually all organizations it can be said that organizations in general will have an issue. Secondly, determining attack surfaces and element vulnerability is very complex and organization specific, this is not feasible to do here. It is easier to determine the level of sensitivity of information an organization is dealing with in general. So, the three categories described in sensitivity of information, low, medium and high, will mainly be used to categorize organizations. The categorization of organizations is done in the case selection in chapter 5, based on the model and discussion above.

3.4 Theoretical contribution need

This chapter contributes to theory by first making a distinction between general need and specific. The broad general definition of need is difficult to apply and needs context specific definition. This is done here by taking need as a function of impact of the quantum threat on an organizations operations. The model looks at the vulnerability of each operation in an organization, which is determined by communication pattern characteristics and sensitivity of information. The question then is how this approach relates to the general definition of need. The general approach looks at the gap between the total desired end state and the current state. This is a very unwieldly way of looking

at it, as both states are made up of many different things. At first glance it may seem that the approach used here does not have a gap between states in it. However it does, it is embedded in the sub elements of what makes up need. For instance, take the element vulnerability construct of the model, the implied gap here is between a safe element and an unsafe element. A similar gap is implied in attack surface and sensitivity of information. What the approach of need does here is illustrated in Figure 14.

Short side point, the need gap of sensitivity of information is slightly nuanced. It is not possible to make information less sensitive, it is an inherent property of the information. The only thing that can be done is to prevent it from being shared to unwanted parties. In that sense it could be said that this element has a fixed need, which impacts the overall need in a constant fashion. This is a nuance in how these things would be combined to form the overall need.

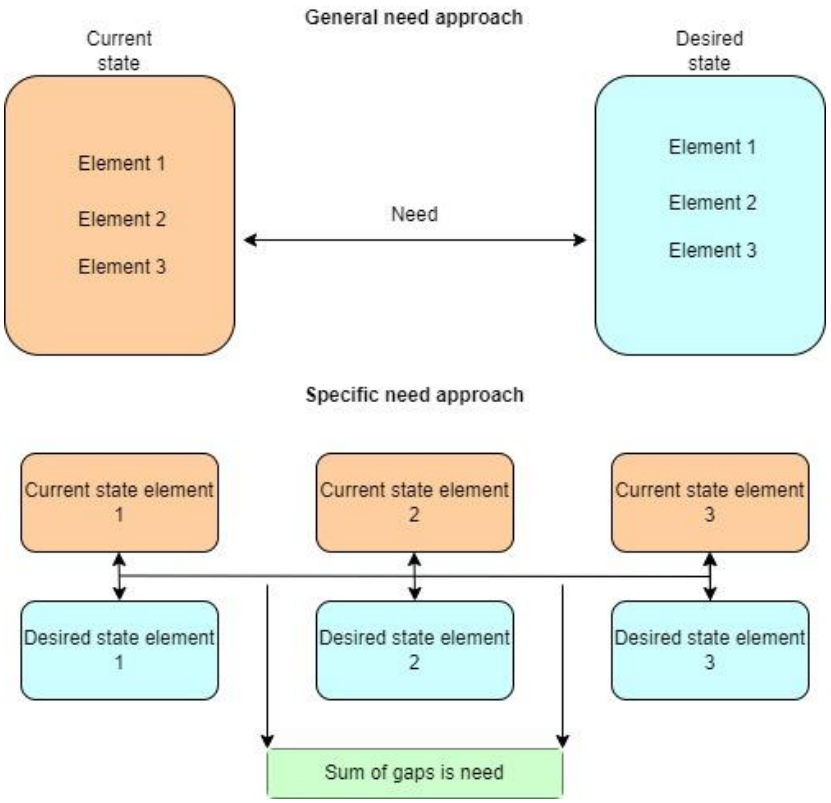

Figure 14: General need approach vs. specific need approach

Next to making a more practical and useful approach for need, this chapter also makes a quantum threat specific need for organizations. This is the second theoretical contribution of the chapter.

4 Readiness

In this chapter sub research question two is the subject:

> *What determines the readiness for quantum secure encryption technology adoption*?

First the method used in the chapter is explained, followed by a description of the readiness literature and then by the readiness model itself. The model is also operationalised in a readiness scale, out of which the interview questions arise.

4.1 Readiness method

The method here again involved a mix between literature and reasoning initially. First the different readiness streams were explored. From this initial literature it was possible to start defining a readiness model. This began by taking a definition of readiness that fits, then deducing what the aspects are that determine readiness. This combination led to the model, and after the operationalised readiness scale. The next step in the method was to validate and improve the readiness model in interviews.

4.2 Readiness literature

As a reminder, readiness, readiness progress and readiness adaptability are defined in the following ways:

> **Readiness:** The extent to which an organization is protected from the quantum threat.
>
> **Readiness progress:** How far the organization is in reaching a state of full readiness.
>
> **Readiness adaptability**: Capacity to implement quantum safe communication technology

In this section it will be explained why these definitions were chosen, and why readiness progress is the focus of this thesis. In order to find the best readiness approach for this thesis a number of literature streams where explored. Chronologically, organizational readiness literature was first explored, followed by technology readiness literature. Later, technology implementation literature was explored and proved to be very relevant. During this literature study there were a number of issues with definitions of concepts that led to confusion. In the end the reasons for this were understood, this is first clarified here.

The underlying issue causing confusion in readiness literature is the ambiguity of the term readiness. The dictionary definition of the readiness is: 'The state of being fully prepared for something.'(Oxford languages). The problem with this definition is the ambiguity of 'something'. The term can be interpreted in two ways:

1. A desired end state, meaning that a change or solution has been fully implemented.
2. The ability to change or implement a solution, meaning the ability to implement a change or solution. In other words, the ability to reach a desired end state.

To put it in terms of the quantum safe communication problem. Readiness could be seen as being fully prepared for the quantum threat, meaning that a solution has been implemented. That solution could be many things, such as PQC, QKD or any combination of these and other technologies. This would be in line with the first interpretation.

Taking the second interpretation, readiness would mean being able to implement a solution that would protect the organization from the quantum threat(not that it has been implemented). If an organization deems PQC the best solution for them, readiness would then be determined by the organization having the right resources, staff, finances etc. to implement PQC. Important about this interpretation is that readiness can change during the entire process of implementing change.

These interpretations have to be kept apart, it must be clear when referring to one and not the other. This is why there are two sub divisions of readiness in this thesis, readiness progress and readiness adaptability. Readiness progress is in line with the first interpretation, it is a measure of how close an organization is to implementing the required solution. Readiness adaptability is in line with the second interpretation, it is a measure of how well the organization can implement the solution. Figure 15 gives an overview of how the literature is divided.

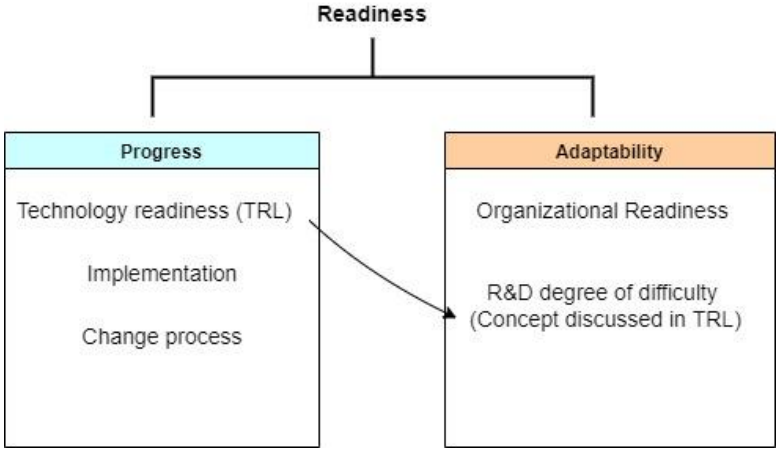

Figure 15: Overview of the readiness literature division

The literature streams explored use different interpretations of readiness. In technology readiness assessment literature (TRL) and technology implementation (change process) the readiness progress interpretation is used. In organizational readiness literature the readiness adaptability interpretation is used. As a result of that the literature stream relevant to readiness progress are grouped and discussed first, followed by the readiness adaptability literature.

4.2.1 Technology Readiness

Technology readiness assessment (TRA) literature is one of the readiness literature streams that falls under the readiness progress interpretation. The focus here is on a technology itself. Meaning, how far in the development is it to being an actually proven and usable technology. It looks at technology development from a project perspective, so a linear process every technology goes through to reach full maturity. Mankins (1995) is the first paper describing the technology readiness levels (TRL), which is the most widespread TRA. The TRL found its origins at NASA, which explains the project perspective it takes as space missions are done with such an approach.

The overview paper by Mankins (2009) further explains TRA's and explains how they work. These types of assessments can be done at different scales, from an R&D team doing it internally to a highly formalized process with external parties and peer reviewing. The first point of note are the different types or components of a TRA. As mentioned, the most well know is the technology readiness levels

(TRL), which will be described in more detail below. There are also other aspects, such as the need for clear evidence that TRL's are actually met, but also the research and development degree of difficulty. The latter being a measure for how hard reaching higher TRL's will be, which is related to the readiness adaptability concept taken in this thesis. The TRL scale uses a variety of levels with different conditions a technology has to adhere to reach that level. Figure 16 below shows what this looks like.

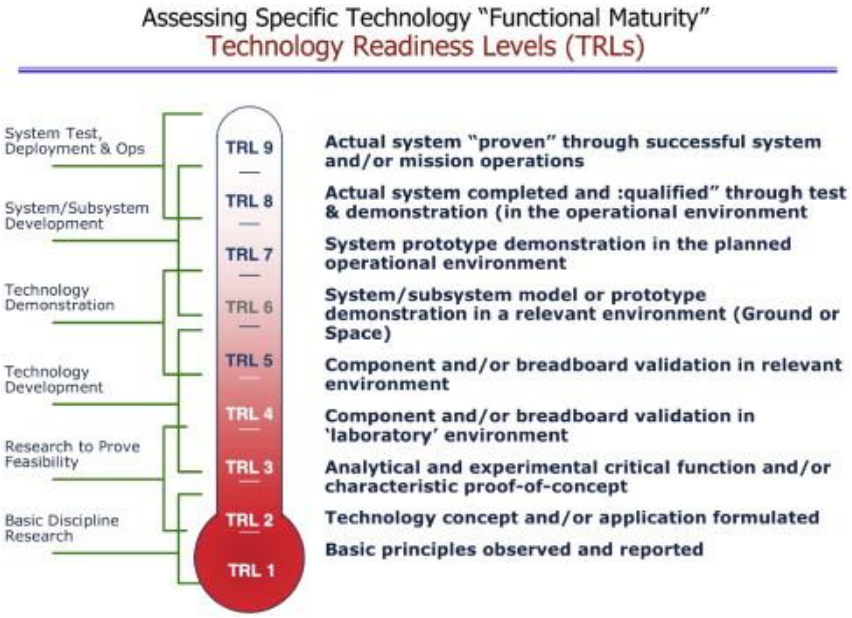

Figure 16: Technology readiness levels

In the 1995 Mankins paper there is also an indication of the cost to achieve each level. It also discusses some of the limitations, for example that technologies consist of many sub technologies that might be at different levels of development. Also, the rate at which technologies progress between levels can be very different, that is why the research and development degree of difficulty metric is very important.

This scale nicely defines the progress of an individual technology towards full readiness. The TRL manages to define quite concrete milestones while still being applicable to many technologies, which makes it useful for comparing technologies in terms of their readiness, apart from the limitation of different rates of development technologies might experience. The applicability of this literature to the goals of this thesis are limited. All though a scale with milestones indicating the readiness of organizations for the quantum threat seems similar at first glance, there is a significant difference. Namely, this thesis looks at the readiness of an organization, not a specific technology.

TRL is also limited in its use here as it takes a very linear view on readiness. In the context of a single technology this can be argued as a decent approach, especially if the perspective of one project is taken, as in the case of NASA. Once this is applied to a technology which is seeing many parties in the market developing it, such a linear approach becomes more questionable. An evolutionary model might be more appropriate in that case, as there are many versions of the technology competing, reaching certain stages of readiness and then failing. Also, different components of a technology could be at different levels of readiness. Take a rocket for example, it could be that most components are at a TRL of 9, but the booster engine technology is only at TRL of 3. On average it may then have a high TRL, but a key component is at a low TRL acting as a bottle neck for actual use

of the full technology. So even in the case of technology readiness the linear TRL approach has limitations.

In the case of an organization this linear approach is also problematic, it follows a more evolutionary model. An organization is composed of many different departments which can be at different levels of readiness to each other. There can be progress made in readiness through the implementation of a program, it could then fail and set the organization back in readiness. A different approach is needed, so technology implementation literature was explored. This is still quite a linear approach, but it deals in more general phases which allows for the more evolutionary nature to still fit within the phases.

4.2.2 Technology implementation

The perspective taken by this literature stream is again in line with the readiness progress definition taken in this thesis. This literature was a logical follow up of TRL literature as it is also looking at stages or levels, but then in the context of implementation into an organization. This is relevant for the perspective of this thesis. The literature here is not referred to as readiness literature, but it is still in line with the readiness progress definition. The literature is referred to as implementation literature(as in the case of Lai and Mahapatra 1997), and in other cases as change process literature (as in the case of Weiner et. al. 2008). These are literature streams that are used for a variety of different types of change that an organization can go through. This makes it so that the concepts have to be tailored to each situation, and also makes a lot of literature not exactly relevant. Nevertheless, as will be explained below there are some very general phases organizations go through to implement change. Here these will be explored, discussed for relevance and in the readiness model chapter it will be applied to the problem of this thesis.

The scale used in a TRL focuses on the technology itself, while this thesis looks at the implementation of technologies in an organization. Technology implementation or change process literature looks at technology transfer into an organization. The overview by Lai and Mahapatra (1997) outlines the literature in technology implementation research, specifically in information technology(IT). Implementing IT into an organization has many similar elements to implementing quantum safe communication technologies. A big difference is how the end user in an organization is impacted, which is more significant in the case of many IT systems than in the case of quantum safe communication technologies. The implementation steps that do not have to do with the end user are largely overlapping. The overview paper refers to other literature, two papers are discussed in more detail below.

Thompson (1965) describes technology transfer as a sequence of three processes: initiation, adoption and implementation. Scheirer (1983) goes a step further and describe 7 stages, as can be seen in Table 6. These stages can be seen as substages of Thompson's model, with two additional post-implementation stages. Both make an important distinction between adoption and implementation. Adoption includes activities such as gathering information about the innovation, assessing its applicability, generating interest among relevant decision makers in organization and all steps up to actually deciding to use an innovation. Implementation comes after the decision to adopt, including activities such as assembling resources, training relevant staff and adapting organizational practices. The first stage, initiation, has to do with becoming aware of there being a problem and a possible solution, this is the stage where the first awareness is created.

Table 6: Technology development and transfer processes (Schreier, 1983)

OUTLINE OF TECHNOLOGY DEVELOPMENT AND TRANSFER PROCESSES WITH SUGGESTED ANALYTIC TECHNIQUES

Process Phase	Analytic Technique
1) Basic Research	• Descriptive exploration • Laboratory experiments
2) Technology Development and Testing	• Device testing • User task analysis • Field demonstrations • Assessment of concomitant organizational changes • Cost/benefit projections
3) Diffusion of Information	• Market analysis • Communication and change agent assessment • Field experiments
4) Adoption	• Organizational decision analysis • Rate of adoption studies
5) Implementation	• Degree of implementation assessment • Analysis of organizational processes supporting implementation • Field experiments on implementation methods
6) Assessment of Outcomes	• Field experiments • Management information systems • Cost/benefit or cost/effectiveness analyses • Productivity or profit indicators • Assessment of staff satisfaction
7) Institutionalization (Routinization)	• Analyses of chains of events • Case studies • Long term organizational change assessment

The different phases outlined in Table 6 above are useful for thinking about the implementation of quantum safe communication technologies, and elements of it will be used in the readiness model developed for this thesis. The analytic techniques that are outlined in the right column discuss how to actually measure the progress in each phase, this is not relevant for the purposes here.

As mentioned, Thompson's model can be considered a more simplified version of Scheirer's model, it groups phases 1-3 of Scheirer into initiation and leaves out all post implementation phases. What is included in the initiation stage is dependent on the kind of technology implementation being discussed. Specifically, at what stage of the technology development process does the organization get involved. The first two phases described in Table 6 are very early stages of technology development. A lot of IT systems being incorporated into organizations have already have already been developed past these stages externally to the organization. This makes these stages irrelevant, which is also the case for the quantum safe communication problem.

The stages after implementation can generally be categorized into the post-implementation stage, as is done in a lot of literature. In IT technology implementation this is an important stage, because the ecosystem within which IT systems operate is constantly changing. Advances in IT technology creates new threats to existing systems and new opportunities which can improve your organisation even further. This process is always ongoing, meaning that the solutions the organisation has implemented constantly have to be evaluated against the new situation. If it turns out to be inadequate, a new implementation process has to be started. This is also the case for the quantum threat, it is essentially a battle between encryption strength and capabilities to break this encryption. Such a race means that constant monitoring of the threat is needed.

As will be seen in the readiness model chapter, elements of Thompson and Scheirer are combined to make the best fitting model for this situation. Further literature that was explored in this problem area shared a common issue that made it often less applicable for the situation of this thesis (Lunenburg, 2010). Usually it concerns technology implementation that involves interaction between employees and technology. As this problem is mainly 'under the hood', not something employees

will notice, the results from these studies becomes less relevant. In the end this means that a more tailor made approach was used.

4.2.3 Organizational Readiness

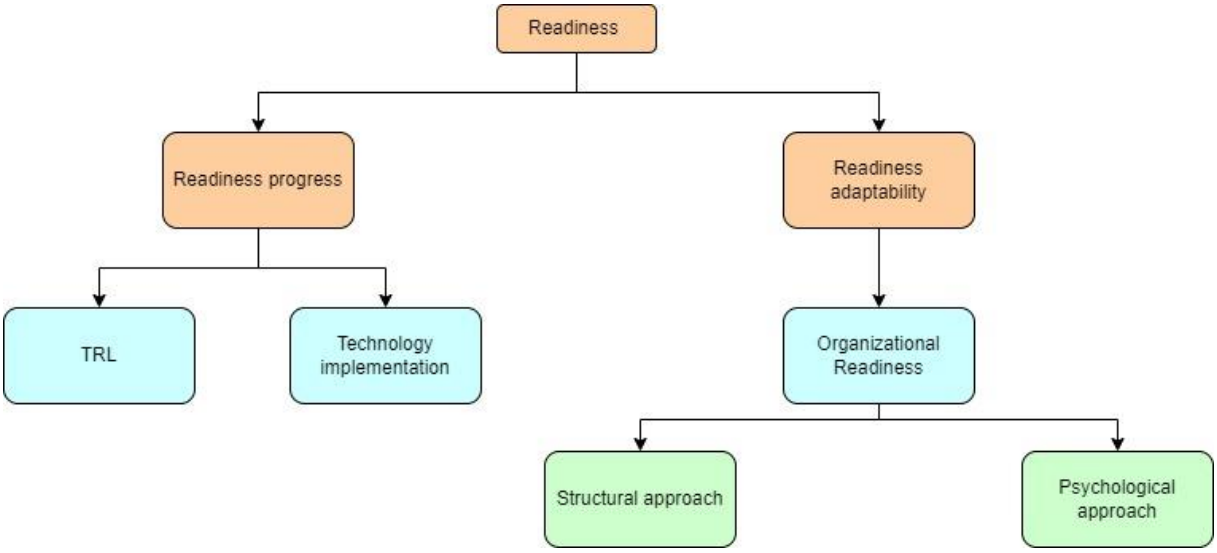

Figure 17: Tree diagram showing where the literature streams fall within the readiness definitions taken in this thesis

This literature stream falls under readiness adaptability as defined in this thesis, as shown in Figure 17. Chronologically this was the first literature stream explored, the first time without the confusion of the terms fully hashed out. Eventually it was clear that the readiness progress was more the focus of the thesis, exploring this literature was instrumental to coming to that conclusion. It also clarifies the different approaches to readiness, and sets-up a topic that can be the subject of further research. Furthermore, it helps think about strategies to a certain extent, as it breaks up the components that make up organizational readiness that could be used as different areas of strategic focus.

It quite quickly became clear that organizational readiness has quite a range of definitions used depending on the research the concept is discussed in. Importantly there are two general perspectives taken on the concept, within which all definitions fall. Those are the two approaches highlighted in green in Figure 17.

One of the perspectives taken on organizational readiness is a psychological one, Weiner et al. (2008) defines it as “the extent to which organizational members are psychologically and behaviourally prepared to implement organizational change”. This perspective looks at the individual within the organization to say something about the organization as a whole. The concept can be studied at other levels as well, such as the organizational level. For instance, some define it as “an organization's plan for change and its ability to execute it” (Narine & Persaud, 2003). Importantly about both the definitions above, they can be applied to quite general forms of change. This could be a change in organizational practices, change of management structures or adoption of technological changes, among other possibilities.

The other perspective taken is a structural one, which looks at attributes such as resources, processes, skills and other attributes that can be attributed to the organization as a whole, rather than individuals. The definition given above from Narine and Persaud falls within this category. The paper by Sharasbi and Paré (2014) does a literature review on organizational readiness in change management literature. Weiner et. al. (2008) does as similar review, in health services research and other fields. Both argue that there are the two views mentioned above, the psychological and the

structural view. Sharasbi and Paré lay out an overview of some of the differing definitions found in literature, as can be seen in Table 7.

Table 7: Different organizational readiness definitions from literature (Sharasbi and Paré, 2014)

Characteristics	Structural view	Psychological view
Philosophical (theoretical) position	Determinism	Human agency / Behavioral theory of the firm
Factors theoretically assumed as the main drivers for organizational changes	Organization structural attributes (e.g., resources, processes, structure, skills)	Organization members' beliefs and mindsets
Organizational readiness construct reflect	Organizational capacity and acquisition of required structural factors for executing the change	Organizational members' collective cognitive and emotional capability and willingness for executing the change
The main evaluation references	High level managers and decision makers	Organizational members affecting or being affected by the change.
Examples of definitions found in the literature	- The efficient use of human, physical, and knowledge resources and the processes employed to transform these resources into services (Collins et al. 2007) - Capacity to implement change designed to improve performance (Devereaux et al. 2006) - Participation of people in the telehealth change activities and existence of supportive infrastructure and sufficient resources that facilitates the change (Kerber and Buono 2005) - The level of fit between the information technology innovation and organization (Snyder-Halpern 2001)	-The cognitive precursor (state of mind) to the behaviors of either resistance to, or support for, a change effort (Eby et al. 2000) -The extent to which individuals are cognitively and emotionally inclined to accept, embrace, and adopt a particular plan to purposefully alter the status quo (Holt et al. 2007) -The extent to which organizational members are psychologically and behaviorally prepared to implement organizational change (Weiner et al. 2008) - The degree to which those involved are collectively primed, motivated, and technically capable of executing the change (Holt et al. 2010)

The structural view is more relevant for the problem being dealt with in this research. The structural view is about the organizations capacity to change, whereas the psychological view is about emotional and cognitive abilities to change. The latter is often done in the context of the implementation of technologies that affect all employees in an organization. Think of the introduction of an information system such as email. Every employee will have to adjust psychologically to using the system. In this case the technological context influences which approach is more relevant. The technology change of migrating to a quantum safe encryption technology, that being QKD, PQC or another option, is not a change that every individual in the organization will be effected by equally. This change is related to the underlying security of IT systems within a firm. This means that although the organization must be ready to adopt the change, not every individual plays as large a role in this readiness. Certain groups, such as the management in charge of strategy and the group responsible for the IT systems will be more relevant to study.

Having said that a structural view is more relevant, a psychological perspective is still relevant for certain individuals in the organization. Mainly the decision makers and possibly the team that has to implement the technology. However this will not be discussed here further, but is something to consider if doing further research on organizational readiness in the context of this problem area.

Weiner et. al. (2008) also had some interesting findings in its literature review. 55% of studies did not give a conceptual definition of the construct organizational readiness. This indicates that the authors of these papers relied on the common sense of readers. It also indicates that it is a vaguely defined concept in many cases, leading to different interpretations of the concept. This is evident in the wide range of interpretations found in literature. This study also noted that the authors taking a structural approach often crafted their own unique conceptions of readiness. This because the type of

organizational change significantly influences the indicators that are of interest. Janom et. al. (2014) also points this out: as a result of the wide range of possible types of change, and the varying contexts within which organizations adopt change, the theoretical framework has to be tailored to each situation.

Sharasbi and Pare further identifies dimension which make up organizational readiness, this is shown in Figure 18.

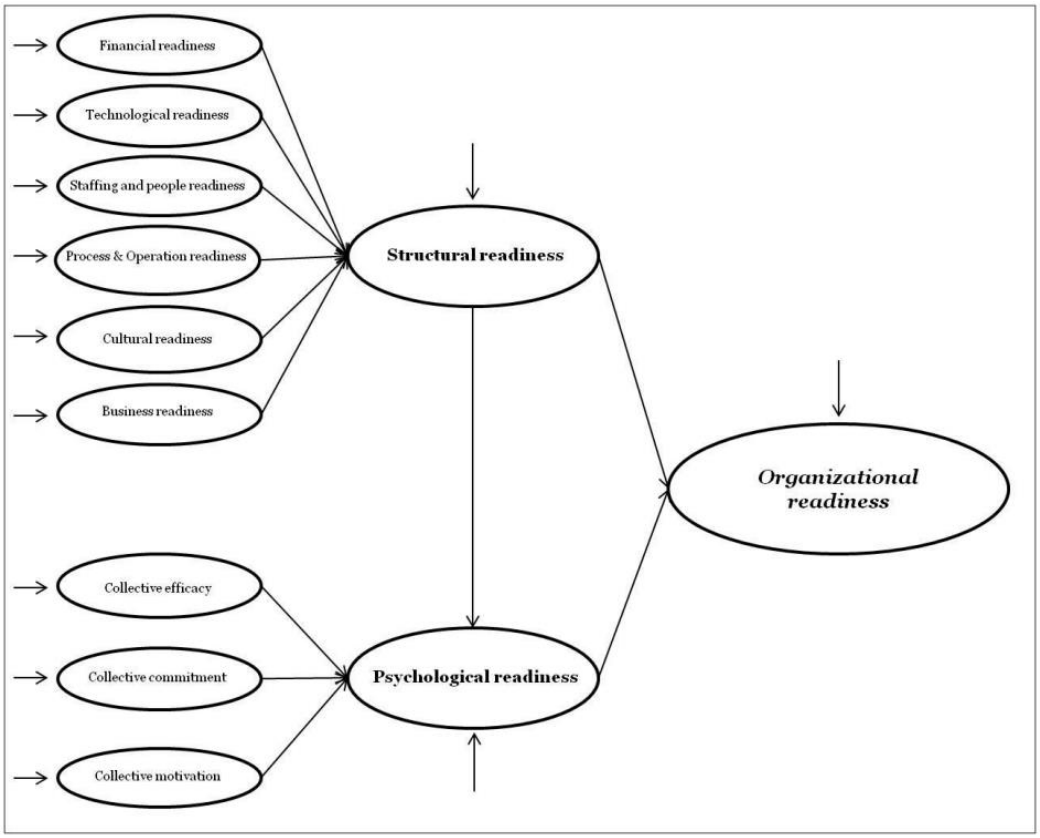

Figure 18: Subdimensions of organizational readiness(Sharasbi and Paré, 2014)

The sub dimension are a useful way of looking at a more detailed level at the readiness types, it is again split up between the psychological and the structural view. Here we will only focus on the structural view. Notice that here it also refers to technological readiness, but this is in a different sense than the TRL's discussed previously. Here it takes the perspective of any technology within the organization that is related to the adaptation of the new technological solution. So it is not focused on one technology as in TRL.

Some sub categories of structural readiness are of more interest than others to the quantum safe communication problem. This is in line with the insight about the need to tailor an organizational readiness framework per situation, pointed out by Jenom et. al. For instance, the aspect of cultural readiness will play less of a role in this problem, as only a small group of the organization will be involved in the change.

Understanding that there are different sub categories is useful for understanding the entire concept better, and allows to identify differences in how researchers approach organizational readiness. In further research this insight is useful, but also when thinking about strategy in this thesis. The different dimensions of readiness also correspond to different areas of focus in strategy. If it is

known what the readiness is per dimension and what the weight of that dimension is for overall readiness, then strategic priorities can be made.

Another important insight from the 2008 Weiner et. al. literature review is that different research is focused on different stages of the change process. This also means that in different stages different variables are of importance, and that literature must be carefully screened for this aspect before referring to or comparing literature. Next to that it is also interesting that the following four stages are considered: adoption, implementation, post-implementation and a separate category where the stage was not specified. This is similar to Thompson (1965) discussed in the change process literature, except for there not being an initiation stage and there being an additional post-implementation stage. As will be explained later, the initiation stage is an important part of the process of implementing quantum safe communication technology. However, this part of the process does not yet require much concrete action on an organization level, so it is logical that organizational readiness is not discussed with respect to this stage much. If it is, it likely falls under the adoption stage in the model used in Weiner et. al. (2008). The fact that the stages are pointed out as something separate again emphasises that organizational readiness is really concerned with the adaptability concept in this thesis, not where in the process of implementation the organization is.

To conclude, the literature on organizational readiness has a range of definitions used depending on the research. The main reason for this is that the change an organization has to be ready for can take many forms. With each form different aspects of the organization are relevant to study, leading to tailored approaches per research. Nonetheless there are common themes in the definitions used, the main one being that definitions fall into two perspectives, the structural and the psychological perspective. Again, the type of approach that is more suited depends on the type of change the organization is dealing with. This does not mean the same problem cannot be approached from both perspectives. In this thesis the structural view is more relevant.

For this thesis a couple of insights are relevant from this literature study. Firstly, doing the study helped clarify the confusion around readiness, making clear what form is relevant for this thesis. It helps clarify what direction further research could go in and it helped clarify the subcategorizations of organizational readiness which is useful for strategic thinking. Finally, the study can be used to make an appropriate definition of the readiness adaptability concept, which can be seen as the organizational readiness definition of this thesis. This is done in the next section.

4.2.4 Readiness Definition

In this section the concept of readiness is defined in three different ways. The definition of readiness with regards to the quantum threat, then two sub definitions having to do with the different approaches to readiness discussed above in the readiness literature section. We begin by relating readiness quite directly to the subject of this thesis, making organization ready for the quantum threat. So the readiness definition used here is:

> **Readiness:** The extent to which an organization is protected from the quantum threat.

Can also be seen as technology implementation readiness, in the sense that once the right technology is fully implemented the organization is safe. As will be explored further in a moment, the level of protection required is dependent on need. It could be that in organizations where need is very low full readiness is already achieved. The model has to account for this.

It is also useful to think of readiness in terms of how far the organization is to reaching full readiness, as this allows to think about the stages an organization must go through to get there. This is the first approach to readiness as discussed above in the TRL and change process literature.

Readiness progress: How far the organization is in reaching a state of full readiness.

The last sub definition of readiness takes the perspective of adaptability, how able is an organization to become ready. Here the definition follows from the organizational readiness discussion above. The structural approach in this literature stream is most appropriate, and the fact that the concept has to be tailored to the situation at hand is used. For these reasons the following definition is defined, adapted from the literature definition ' capacity to implement change designed to improve performance' (Devereaux et. al. 2006):

Readiness adaptability: Capacity to implement quantum safe communication technology

4.2.5 Need vs. Readiness

The concepts of need and readiness are linked to each other in a number of ways, here this is discussed. The question is if some cross dependency is an issue for how they are used in the models, this is explored here.

Need is a measure of how much impact the quantum threat will have on the organization, and readiness is a measure of how far the organization is in being protected from the quantum threat. If you take one extreme in need, that being that an organization has no need what so ever, then they are by definition at full readiness already. This seemingly without taking any steps to increase readiness. However, as will be seen later, this actually does not mean the organization has to take no steps. The organization would still need to determine first that it has no need for quantum safe technologies, which would make the following phases of readiness instantly completed. In such a case the model for readiness would still stand. This shows that need affects readiness by impacting how quickly or easily an organization will be able to go through the readiness phases.

One of the sub constructs of need also has an impact on readiness, that being the communication pattern. If there is a large attack surface and many actors involved in the communication pattern of an organization, then implementing a solution will be more difficult. This makes the readiness process slower. Again, notice it affects the rate at which an organization can move through the readiness phases, it does not alter the model. So, even though the concepts are not completely separate, the influence they do have on each other does not make either model invalid.

4.3 Readiness Model

Here the readiness model is constructed out of the literature described above, and own contribution. This is followed by an operationalization of the model in the readiness scale section.

To make the appropriate readiness model for this thesis need plays an important role and forms a starting point for the model. Important theoretical basis for the model comes from Schreier's [19] model outlined in Table 6. Thompson's technology adoption phases, initiation, adoption and implementation, forms an important frame for the phases outlined in this model. Aspects from these will be combined into a new readiness model. Figure 19 gives an overview of the model.

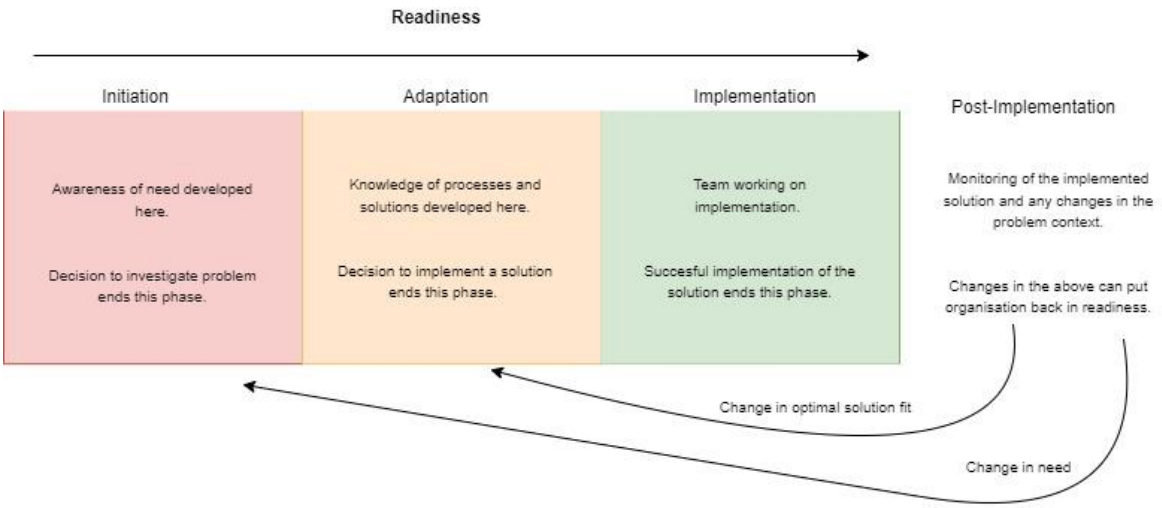

Figure 19: Overview of the readiness model

4.3.1 Initiation

As mentioned before, the first two phases from Schreier are not relevant here. The concept of initiation from Thompson can be combined with need to think of the first phases of the readiness model. Initiation in this case only consists of one key point, the awareness of need.

4.3.1.1 Awareness of need

The first step in initiation is becoming aware of the need your organization has for quantum safe communication technologies. Before this has the occurred the organization cannot assess its readiness with respect to the quantum threat. Awareness of need starts with knowing about the quantum threat, then how your organization could be affected by it. Knowing about the quantum threat can have different degree's, certain individuals in an organization having heard of it is different than it being actively discussed in the organizations management. The second step in awareness of need is knowing how your information is affected by the quantum threat. This can be assessed by determining the organizations need.

There is an apparent flaw in using awareness of need as a beginning point of readiness. An organization with a very low need could, without knowing it, already have the technology in place to be completely ready for the quantum threat. At least, they can reach a state of full readiness quicker than an organization with high need. However, this does not mean that the organization does not need to go through all the same phases as organizations with high need. They do, but they do so at a higher rate. Say we have an organization with very low need that is in fact fully ready for the quantum threat from a technological perspective. The fact that they are unaware means they are not ready from a management perspective. This is an important distinction, as the technological situation

can change over time the organization needs to know where it is at now and adapt if necessary. Considering these points, the apparent issue of need affecting readiness is not significant. What it does affect is *the rate at which* firms can go through the different readiness phases.

Initiation ends once the need is understood and further action is decided to be taken. No concrete steps have been taken in exploring solutions yet.

4.3.2 Adoption

As outlined in Schreier, adoption includes activities such as gathering information about the innovation, assessing its applicability, generating interest among relevant decision makers in an organization and all steps up to actually deciding to use an innovation. Here, gathering information does not begin by looking at the possible solutions, but by looking at the processes within the organization.

4.3.2.1 Knowledge of processes

This has to do with knowledge of which operations will be affected and to what extent, what kind of communication pattern they follow and what cryptographic algorithms are underneath. In this problem context this can be very complex, and it differs per organization. The size of the organization plays a role, but also what their range of operations is. Organization will also have different quality overviews of what all their processes are at their disposal in the beginning. These aspects will determine how long it takes for an organization to get sufficient knowledge of its processes.

When understanding the relevant processes external parties also play a role. How the organization is dependent on third parties is of concern, but also who the relevant partners are and what might need to be coordinated with them. A lot of IT systems used by organizations are licensed from third parties, for example the use of Microsoft Teams. The organization does not have direct control over the algorithms used in such programs. These situations require a different approaches than internally managed IT systems. The ecosystem the business operates in needs to be considered for more reasons, some IT systems may be used by multiple parties which all need coordination. Regulations and standards may also play a role in certain situations. These are all factors that are external to the organization and that play a role in the solution the organization should adopt.

As explained in the need section, different operations within a firm will have different levels of need. This is also necessary knowledge to tailor the solution to the organization. Sufficient knowledge of processes entails a level of understanding that allows the organization to properly choose the best technological solution for them. To do this an understanding of the solutions is needed simultaneously, so the best fit can be found.

4.3.2.2 Knowledge of solutions

This aspect of the adoption phase is also a complex one, due to the number of technological solutions there are and how complex each of them is. As outlined in the literature review on the different solutions, there are two main technologies to consider, PQC and QKD. Then there is also another category of solutions, which includes technologies such as Kerberos and the physical sharing of symmetric keys. Each of these technologies has different strengths and weaknesses, which makes them each applicable for different situations. This is a huge topic in itself; in the strategies chapter this is discussed. Important here is that quite a process has to be undertaken before these solutions are properly understood.

Important to note here is that certain technological solutions are not yet ready to implement. The technologies are still developing, which is largely outside the control of the organization. In certain cases an interim solution could then be taken. This would then be implemented, and once the more

optimal solution is technologically ready the implementation of this technology can begin. With need, knowledge of processes and solutions in mind, the right solution fit can be chosen and the implementation process can begin.

4.3.3 Implementation

Referring back to Schreier, once the decision to adopt has been made the implementation phase begins. This includes activities such as assembling resources, training or hiring the relevant staff and adapting organizational practices. In the case of the quantum safe communication technologies this phase often involves collaboration with relevant third parties, for the reasons explained in adoption. This means that the time such implementations take is not always completely in control of the organization, being dependent on standards or the decision of other parties.

The time this process takes is dependent on more aspects, such as the size of the firm and the number of operations that need to be adapted. In cryptology such transitions are referred to as migrations, and they can be very complex. The solutions chosen by the firm will have different implications for the migration time, but also the type of changes that need to be made. Some involve hardware changes and others only software changes, the costs also vary per solution. These aspects have to be considered in the strategy the organization adopts.

4.3.4 Post implementation

Once the technology has been implemented the process is not over, there always remains need to monitor both the external and internal situation in case changes need to be made to guarantee full readiness. This could be problematic as it means that it is not possible to ever be fully ready. To solve this, we take full readiness as the state of having implemented the technology that was decided upon in the adoption phase. It then becomes possible to fall back in your level of readiness when there are changes in the situation. These could be changes such as a better solution for the organization's situation, or an increased threat from better quantum computers.

Next to monitoring the external situation the internal situation also needs to be monitored. This is similar to Schreier's phase of assessment of outcomes. Depending on the impact and effectiveness of the implemented solution changes might need to be made. In both the external and internal change case a decision to have to adapt puts the organization into an earlier stage of readiness. Specifically the adoption phase, as the firm has to reassess its processes and the solutions that are available.

It is also possible for the organization to go back to the first phase of initiation. This would happen if the need of the organization changes, in which case a new awareness has to be developed. This means that in the post-implementation phase need also has to be monitored.

The post implementation phase is different to the previous phases in that it is an evaluating phase, where it is possible for the organization to fall back to a lower level of readiness.

4.4 Readiness scale

Having defined the different phases it is now necessary to operationalize the theory so that an organization can be pinpointed in the right phase through measurement. To do this more concrete milestones are needed than are defined in the model above. This is similar to what TRL does, and is quite linear. However, in order to make concrete measurement points such milestones do have to be defined, so a linear approach is a pragmatic choice. Nonetheless, it is important to keep in mind that the actual process in organizations may not be so linear. To make this scale every phase can be characterized by a certain requirement, this is discussed per phase below.

4.4.1 Initiation

In initiation there is one milestone to be reached, which has to do with the awareness of need. The question is how to determine whether an organization is aware of the need. To get the right definition the intended result has to be referred to. This result is there being a decision to further investigate the internal processes and the available solutions, to enter the adoption phase. Such a decision is made by managers, which means that the awareness of need has to be at that level as well. So, the milestone is:

1. **Managers are aware of the need for quantum safe communication of their organization.**

The question is then how to make this more concrete. A manager having heard of the problem is not the same as them actively discussing it internally and having meetings about the possible need they have. The issue here is finding a universal measure, as each organization might do it differently at this stage. It could be that an organization has an internal report about need, or it could have all been discussed informally. The best way to do it involves asking top management in interview form.

4.4.2 Adoption

The adoption phase begins when the decision to gather information about processes and possible solutions has been made. This immediately presents a relatively easy to define milestone:

2. **Decision to gather information about processes and possible solution fit has been made.**

Again, the issue here is making this concrete, although this it is not as big of an issue as with awareness. Depending on the situation and the organization such a decision could take a different form. It could be that a project team has been set-up, that external consultants have been hired or a number of other things. Whether or not such a decision is formally recorded is the question, it could be in the form of an email or even verbal. Again, the best way to test this is through an interview.

The next milestone indicates the transition to the implementation phase. This can be done when sufficient knowledge on processes and solutions has been gathered to make the decision to implement. The knowledge of processes are two parts of the same phase that are done in parallel, as you need both to make the right decision. For that reason, they are grouped into one milestone:

3. **Sufficient knowledge of processes and solutions has been gathered to implement.**

To make this milestone more concrete the decision to implement is appropriate to look at. This is something that will have occurred formally inside the organization, as a project has to be started to do so.

4.4.3 Implementation

This phase can be a very complex with a lot of steps in it, depending on the solution the organization wants to implement and other factors. Ideally, you subdivide this phase into smaller milestones for this reason. This is challenging to do as each organization will have very different implementation situations. One milestone that is universally required can be defined, whether or not the resources required have been assembled. Next to resources, the team has to be assembled that is responsible for the implementation. This leads to the fourth milestone:

4. **The necessary resources and team have been assembled to implement the solution.**

This is likely still quite early on in the implementation phase. After this it is hard to say what other milestone there might be before the end, as it is highly dependent on the organisation's situation. The final milestone is:

5. **The solution has been implemented; monitoring has started.**

Monitoring here refers to the post-implementation phase, which falls out of the readiness scale itself. As explained, it is still of importance and a requirement to go out of the implementation phase completely. Both milestone four and five are quite concrete milestones as these things will be formally on paper in organizations.

Between milestones four and five the model can mislead; the model indicates that the organization is near full readiness since it is in the last phase. However, in terms of time to reaching full readiness the organization could be a lot further off. In other words, the model is not proportional to the time taken between phases. Organisations need to be aware of this and take it into account. More specifically, the organisation has to estimate for itself how long getting from milestone four to five will take.

4.5 Theoretical contribution readiness

This chapter adds to theory by clearly separating different approaches to readiness. It explains how it can be interpreted in two main ways, namely:

1. A desired end state, meaning that a change or solution has been fully implemented.
2. The ability to change or implement a solution, meaning the ability to implement a change or solution. In other words, the ability to reach a desired end state.

The first interpretation is in line with the readiness progress definition of this thesis, the second with readiness adaptability. The next addition to theory is the bringing of implementation and change management literature into the quantum threat context. From this the readiness progress model is defined.

5 Case selection and data collection

As explained in the earlier method chapter, this thesis is built up through a mixture of literature, own contribution and interviews. A large first part of the thesis was done with literature and own contribution. From this the need model and the readiness model where made almost completely. A first shot at potential strategies was also made. To further develop the models and strategies, as well as validate to a certain extent, case studies where the next step. First literature is consulted to correctly design the case study.

Yin 2012 is an authoritative source on case study design and was mainly consulted. According to Yin case study design is most appropriate for research where (1) the main research questions are “why” and “how” questions; (2) a researcher has little to no control over behavioural events; and (3) the focus of the study is a contemporary phenomenon.(Yin, 2012, pg. 2). Criteria 2 and 3 are clearly met with the research being done here, however criteria 1 seems not to be. The research questions being dealt with here are formulated as “what” questions. However there is an important difference in this research to more standard forms of case study research, as a mixed method research design is used. The first method used is literature study with own contribution, in this part of the study the what is first answered. In the case study part the goal is to validate what has been found and to add to the developed models from new insights. As a result, even though no “why” or “how” questions are being answered the method is still appropriate as it is not the sole method being used to answer the “what” question.

A holistic multiple case study design is used here, meaning that each case has a single unit of analysis, the organization. An advantage of multiple case study design is that replication can be used to compare results between different cases. To a certain extent this will be applied here, with a number of questions remaining constant. However, (Yin, 2012, pg. 65) also states that case study designs can be adjusted between cases as a result of new information or discovery. This adaptive approach makes sense for this research, as it is quite exploratory in nature and is building theory. New insights are bound to come, incorporating these into the successive cases improves the quality of the research.

The method of data collection used in the first two cases is the semi-structured interview, and in the third case grey literature is used. Ideally, the same method of the semi-structured interview is used in all three cases, this improves internal validity and reliability. However, due to circumstances the interview was not possible to plan, so the alternative grey literature study had to be used. Nonetheless, in this case the grey literature was quite strong and able to answer many of the same questions from the interviews. Next to this it was a contrasting case, which further increased the usefulness.

The choice for a multiple case study design is now based on literature, Figure 20 gives an overview of the entire design.

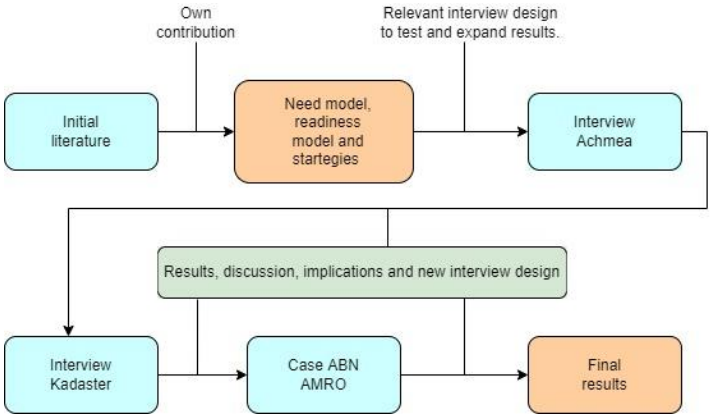

Figure 20: Overview of the data collection process

After the initial study interview question where made for the first case, the results of this interview then discussed. These where used to adapt the interview questions for the next case for more useful results.

This was repeated again in the second round. The third and final round was slightly different, as instead of an interview case the case was described using grey literature. Meaning, publicly available news posts, press releases and other internet sources. The case that was dealt with in the third round was suited for this, as they have a lot of relevant information to the subject in grey literature.

Before getting to the interviews themselves, the case selection is discussed. This begins with a discussion on the categorization of organizations, where it is argued which types of organizations would be most interesting to study for the purposes of the thesis.

5.2 Case selection

The need model gives three categorizations of need: low medium and high. Here, the case selection for the interviews and case is discussed. As explained in section 3.3.4 communication pattern will not be weighed heavily here. Also, there is a different level of sensitivity for different information streams within an organization. In that sense, to get a full overview an organization would need to map all of them and rank them. This will not be done here. It is also the case that organizations within certain industries will share similar data sensitivity levels and similar communication patterns. For this reason, sensitivity and communication pattern will be discussed at the industry level. Based on this discussion, a selection of organizations from different industries can be selected.

To begin with there is a certain baseline need that all organizations have. All organizations deal with financial data, personal information about employees, strategy documents and many other potentially sensitive information. Here, this base line will be considered as low need.

On top of this baseline certain organizations deal with more sensitive information. For example, and industry that deals with client data that must adhere to privacy laws. This could be a hospital or a health insurance company. There are also industries that deal with financial data, such as banks. The industries just mentioned fall within the medium to high need category. These are interesting to study further for a number of reasons. Firstly, having higher need means they are more likely to be focused on cyber security and possibly the quantum threat also. This means they have thought about it more, might be in a higher state of readiness and have considered their strategy more. Two organizations from this category are chosen to do interview cases on, as will be explained further later on.

Another interesting category of organizations to study are governmental ones. These can vary quite a lot in their need, from the secret service having extremely high need to agencies dealing in publicly available information having lower need. The different type of responsibility government organizations have are interesting to bring into the study as well. An organization with low to medium need is also interesting to study to a certain extent. Likely, such an organization is lower in readiness and has less developed strategies. Either way, this is what is interesting to test. For this reason one organization from this category is used as a case.

5.2.1 Organization 1: Achmea

The first organization of interest falls into the medium/high need category, as it fits in the insurance category described in the categorization of organizations section. First, a description of the organization is given. Achmea is one of the largest financial services and insurance companies in the Netherlands, with a revenue of 20.2 billion euros in 2020 and 13,300 employees. It is the parent company of a number of large organizations. For example Het Zilveren Kruis, a large health insurance provider. Also, Centraal Beheer is one of the large companies it owns, which is a general insurance company.

As it is a large insurance organization it has a large attack surface, it communicates with many parties, also using PKI infrastructure. Next to that, it deals with quite sensitive information, insurance data is privacy sensitive. For these reasons it is considered as a medium to high need categorization. As the perspective of managers is taken in this thesis interviewing an employee in such a position is most useful. Also, as this is an IT issue an employee in this department of the organization is likely to know most about the situation of the organization regarding the quantum threat.

Contact was made with the organization and an interview was planned with the manager of IT security and data governance of Achmea. The interview questions used are described next.

5.2.2 Organization 2: Het Kadaster

Het Kadaster is a government agency that registers all land use in the Netherlands, the agency falls under the ministry of internal affairs and kingdom relations. They register all the property rights, and the actual geographical data of all properties in the Netherlands. This includes exact descriptions of property boarders, information about pipeline and other public infrastructure location (for construction purposes for instance). For a low price the information that you might need about a property can be bought, meaning anyone can access it. So it is public information, which is an interesting case with respect to the need of quantum safe communication technologies.

This makes the information less sensitive in the sense of confidentiality, it is not at all confidential. In the sense of data integrity and availability it can be a different story, especially integrity. Manipulating the data to suit your needs could be a risk for Het Kadaster. Given these considerations Het Kadaster was placed in a medium need categorization.

Again, managers were sought out and an interview was planned with the director of IT and the chief information security officer.

5.2.3 Organization 3: ABN AMRO

ABN AMRO is a large Dutch bank, it is an organization that falls in the high need category. It employs 19,000 employees and has a market capitalization of 5.7 billion euros. They are a significant player in the financial services sector and handle a lot of financial transactions. The financial information they deal with is very sensitive in nature, next to this they have a large attack surface as they process a lot of transactions with many different parties. Financial information is sensitive in multiple ways. In the sense of confidentiality organizations and consumers do not always want it to be public what transactions they are making. From an integrity standpoint it also needs to be safeguarded, otherwise balances can be changed.

Managers were sought out to interview in this case without success. Fortunately, ABN AMRO has quite a lot of relevant information about the topics discussed here open to the public. This is used in the data collection chapter later on.

5.3 Interview questions description Achmea

Here the reasoning behind the interview design is given. The goal of the interview is to validate the need assessment, validate the readiness model and to explore strategies further. To do this a semi-structured interview approach is taken, allowing space for follow up questions and discussion. The organization was already placed in a need category, checking if the interviewee agrees is then is a good way to validate the reasoning.

Then, the readiness model is tested using three steps. These steps test the model in different ways, allowing for comparison of the results between steps. If they overlap, then the model is validated. The first step involves briefly showing the different stages in the readiness model to the interviewee and having them place the organization in the stage they think they are in. The second step involves asking questions from the operationalized readiness scale, to use the answers to these to again place the organization in the model. The comparison of steps one and two is then a form of validation. The third step then involves open discussion with the interviewee over any discrepancies between steps one and two. Here new insights can be found to improve the model.

The last part of the interview involves a discussion of strategy, whether they have a particular strategy and what it then entails. This part starts open, after which follow up questions can be asked based on own thinking about strategy. The full interview questions used can be found in appendix A.

5.4 Summary report interview Achmea

Here a summary report of the interview is given, the raw data can be found in appendix A. The summary report briefly presents the most important points of the interview, the implications are discussed separately afterwards. Table 8 gives an overview of the results.

Table 8: Main interview results Achmea

Need	Readiness	Strategy
High need: • In areas such as health insurance information more sensitive than banks. • Fulfils a different role than banks though, not on the critical infrastructure.	**Initiation:** • Aware but have not done anything yet, time horizon for quantum threat still unclear. • Will not develop technology themselves, will buy commercial quantum safe products when available. So being more ready not urgent.	**Reactive:** • Observes what current cyber security standards and makes sure to keep up with those.

5.4.1 Information interviewee

First the interviewee was asked about their role, after which he described the functions of the teams he manages. There are four main teams, a defence centre, an ethical hacking team, a security scanning and engineering team, finally a data governance component:

- The defence centre monitors cyber security threats and responds to incidents when necessary.
- The ethical hacking team tests its systems for vulnerabilities by attempting to hack it themselves.
- The security scanning and engineering team is also scanning for vulnerabilities, and they make sure the right technologies are available for all other teams.
- Data governance is also a large part of his responsibilities, which has to do with compliance to rules and general organization of data.

5.4.2 Need categorization (RQ1)

In discussion of need the interviewee emphasised that Achmea deals with some very sensitive information. They deal with a lot of personal information, especially health related information is sensitive.

"We deal with sensitive enough information to want to use up to date encryption".

Also, in the discussion the interviewee was asked how they think they stand with respect to banks in their need. The answer was that Achmea is right behind the banks.

"Sometimes we have even more sensitive information than banks, if you look at health and life insurers"

However, he also pointed out that banks have a different role. For example, ABN Amro manages critical financial infrastructure. He referred to an employee of ABN Amro who is in a similar position to him.

"He has a whole team on quantum, and 500 people on cyber security under him (edit: the 500 not all on quantum specifically). I have 12, it's a different order of magnitude."

5.4.3 Readiness model (RQ2)

After presenting the model and asking in which phase Achmea is the answer was quite decisive, placing them in the initiation phase.

"We are aware of the quantum threat, we know that it will pose a threat to our encryption at some point. The crux is, when? We haven't actually defined this for ourselves, so we are aware but aren't doing anything with it yet."

The interviewee also emphasised that they do not develop technologies themselves, so they are not a party that is going to make a PQC algorithm for example. The point here is that they just buy what is on the market, implying that they will buy the quantum safe technologies once they are available. Basically, they expect not to have to actively do so much and can wait until products are on the market and then implement them.

The second stage of questioning about readiness involved some more specific questions about indicators of readiness. To the question whether top management is aware of the quantum threat the answer was that they are. However, not much more than that, so no ideas of what to do about it exactly. The rest of the specific questions prepared for this part were easily answered, they were all no as Achmea is in the initiation phase. These specific questions were indicators of later phases (adoption, implementation and post-implementation).

5.4.4 Strategy (RQ3)

The last part of the interview discussed strategy. Achmea does not have a specific strategy for the quantum threat.

"We do not know much about the problem at all, I already heard you throw around terms that I cannot place".

Again, the point about using commercial quantum safe products when they are available came up. As a follow up the more general cyber security strategy was asked about. Here the interviewee used an analogy:

"If you think of it as a bike race we like to be in the front of the peloton. We are not in the breakaway group, but we do make sure we are in the front to stay out of crashes and be in a safe position."

Achmea follows a what can be described as an observe the others strategy. They look around to see what the standard is other organizations are adhering to and make sure they are up to date with this.

5.5 Discussion Achmea interview

The information of the interviewee part indicates what responsibilities a cyber security manager has. These are quite numerous, and is a reminder of the wide nature of cyber security. This also means that the perspective such a manager takes is wide, and that they are considering many threats to

cyber security. The quantum threat is then one of many, this adds an extra complication to the problem from a managers perspective. They then need to assess how the quantum threat compares relative to all other possible threats, to then decide where to prioritize. This can lead to over or underestimation of the threat, especially if there is not a proper understanding of how they will be impacted by it. Also, the fact that the term of the threat is unknown(which the interviewee emphasises), can make the priority lower.

5.5.1 Need (RQ1)

In discussing the need of Achmea it is interesting to see that they place themselves quite high, close to the banks in terms of need. This being a result of the sensitive information they deal with, such as health and life insurance data. This shows that the need estimation made before the interview was fairly accurate, but possibly a bit on the low side. Maybe more accurately, the estimation relative to the estimation of the need of banks was too low, and that they may in fact be closer together. That being said, the interviewee also pointed out that banks have a different role than insurance companies and that they control more critical financial infrastructure. This is an interesting point that adds to the estimation of need. It points out that the infrastructure the bank runs is also essential for the flow of money in society, on which the entire economy is largely dependent. This makes it even more sensitive, validating the very high categorization of banks in terms of need.

5.5.2 Readiness (RQ 2)

The interviewee placed Achmea in the initiation phase, giving one main reason. That being that the time horizon of the quantum threat is unknown, and that the they do not have a sense of urgency yet. The question is whether this lack of urgency is justified. The fact that the need of Achmea is quite high makes this lack of urgency potentially more problematic. It is also an indication that more organizations may be in the initiation phase, especially if you expect a firm with high need to be in a more advanced stage and they turn out not to be(as is the case here). The fact that so little is known within Achmea about the problem is of concern.

The point made by the interviewee about Achmea buying commercial products and not developing technologies themselves is important to consider. Firstly it is good to realize that this was not assumed in the readiness model made here, this was excluded in the model. Specifically, phases 1 and 2 from Schreire's model were left out for this reason. The implication of this point is that Achmea does not need to be as involved with the problem as they can just wait for a solution to come on the market. Whether this is true or not depends on how hard implementing these commercial products is (for instance PQC encryption). This is not something that the interviewee discussed, it could be that this is underestimated. At the very least, there should be a good understanding within Achmea of how implementing these technologies would work. Without that, just waiting for commercial products to come on the market could be risky.

What is also interesting is that there are already solutions on the market (albeit early phase, and in the case of PQC not standardized). Either they are not aware of them, or they do not deem them ready to be bought. As they are also a party that communicates with many other organizations they might not be able to implement a solution without collaborating with others. In such a case waiting for a standard might be necessary. The problem here might be that this takes too long, the NIST standardization process has been taking quite long and is only expected to reach a standard in 2024.

The second method of testing readiness was short and did not lead to validation of later phases of the readiness model. The initiation phase question was accurate though. This might be a problem for testing this model in later interviews also, if a lot of organizations are in fact in the initiation phase. (Might be the case if a high need organization like Achmea still is). It could also be that there is not a very strong correlation between need and readiness in this respect, this seems like a logical assumption but has not been tested.

5.5.3 Strategy (RQ 3)

The interviewee indicated that Achmea does not have a specific strategy for the quantum threat. Given that the organization is still in the initiation phase this is not very strange, they are only aware of the problem and not much more. This is useful insight for the strategy chapter. The adoption phase, where the organization is doing research into the problem and solutions, is where you would expect an explicit strategy to be developed. Again, the interviewee mentioned that they wait on the availability of commercial products, which could be considered a strategy.

The general cyber security answer given is also interesting and seems to be in line with the wait for commercial products approach. Essentially, the strategy is to observe what organizations around them are doing and keeping up with them. This could be indicative of how a lot of organizations operate in terms of cybersecurity. It is a rather reactive approach, on the one hand it makes a lot of sense. Instead of expending resources being very proactive, observing what the rest does saves resources and increases the chances that your security is ok. At least it will be as good as the rest. This does not exclude the possibility of the rest being too far behind in their encryption standards, in which case there is a significant problem. Also, given the possible long migration time it could lead to a serious problem. Potentially this general cyber security strategy Achmea has needs to be adjusted for the quantum threat.

5.5.4 Conclusion Achmea interview

The first interesting result from the interview was the high self-categorization of need, slightly higher than thought of beforehand. Also interesting was that despite having high need, Achmea is still in the initiation phase with limited knowledge of the problem. Achmea's current position on the quantum threat is reactive, they are waiting for commercial products that solve the problem to come on the market. They also do not have a separate quantum strategy yet, their strategy to it then falls under their more general cyber security strategy. This more general strategy involves keeping up with current standards other organizations follow, in the case of the quantum threat this could be problematic.

5.5.5 Questions to change in next interview

The next step of the data collection process involves taking lessons from this first interview to refine and expand the questions for the second interview. Here the changes to be made for the next interview are discussed.

The interviewee referred to the fact that Achmea would buy commercial quantum safe technologies when they are available. What would be interesting to know is whether or not such commercial products would be easy to integrate into the IT infrastructure of a large organization. The testing of the readiness model will be kept the same, even though it is possible that many of the question will again be quickly answered if the next organization is also in the initiation phase.

Next to these changes, some other changes will have to be made in order to make the questions better suited for the type of organization interviewed next. The final changes made to the interview design are discussed in the next section.

5.6 Interview question description Het Kadaster

The interview structure and many of the questions are kept the same for the second interview. The changes made are based on some of the insights from the previous interview, but also as a result of Het Kadaster being a different type of organization.

The opening question is changed and does not ask about their responsibilities anymore, rather it focuses on their perception of the quantum threat and how they would describe the need of their organization. Then the same questions are posed on readiness and strategy. The fact that it is a government agency will make the strategy questions interesting, likely they will follow government wide policy. The full interview questions used can be found in appendix B.

5.7 Summary report Het Kadaster interview

Here a summary report of the interview is given, the raw data can be found in appendix B. The summary report briefly presents the most important points of the interview, the implications are discussed separately afterwards.

The interviewee was the chief information security officer (CISO) of Het Kadaster, with extensive experience in cybersecurity in the government, for instance at the police. Table 9 gives an overview of the interview results.

Table 9: Main interview results Het Kadaster

Need	Readiness	Strategy
Medium/high: • Higher than estimated in thesis, as a result of how databases are allowed to be accessed.	**Initiation:** • Says to know enough. • Will buy commercial quantum safe products when available.	**Reactive:** • Will buy commercially available products when available. • Can follow government guidelines but do not have to.

5.7.1 Need categorization (RQ1)

In asking about the sensitivity of the data Het Kadaster manages the answer highlighted that the sensitivity may be higher than anticipated here beforehand. Although the information Het Kadaster manages has to be public there are rules about how the database can be used. The crucial point is how information can be searched in the database. Everyone is allowed to request information about a property, which will give details about the surface area, property type and also about the owner. However, the search function cannot be used the other way around. Meaning, you cannot search an individual's name and find out where they live. This is a security concern that makes the data more sensitive. A hacker could steal the database and then do such a reverse search.

Also, the interviewee that they, just like all organizations, have sensitive employee data, financial data and other data forms that are standard in an organization.

5.7.2 Readiness model (RQ2)

The opening question of the interview asked about the knowledge of Het Kadaster about the quantum threat. The answer was decisive:

"Enough, we know that we will need new protection in the future."

This is already an indication of the readiness stage the organization is in, they know about the quantum threat, and that they will need to implement a solution in the future. This means they are not yet in the implementation phase and does not give enough information to distinguish between the initiation and adoption phase.

Later, the readiness model was presented and the interviewee was asked to place Het Kadaster in one of the stages. The answer started with a critique of the question, stating that it is not the right question. The explanation began by stating that we do not know how the quantum threat will unfold and that Het Kadaster is not the party that needs to be thinking about this. They do not have the resources to, and the interviewee pointed out they do not develop technology themselves and will just buy quantum safe encryption technology when it comes on the market. Nonetheless, the interviewee would place Het Kadaster in the initiation phase of the readiness model presented here.

5.7.3 Strategy (RQ3)

The answer to this research question was already more or less answered. They do not have a specific strategy other than being reactive to how the market develops, and then buying quantum safe encryption products. Furthermore, when asked about whether they follow government wide cyber security policy or develop their own the answer was it depends. They are an independently run organization, they can chose to follow the government wide security policy or go their own way. Often they do follow the government policy.

5.8 Discussion Het Kadaster Interview

In discussing the interview reference will be made to the result of the Achmea interview, as it is interesting to compare what the similarities and differences are in the results. To begin with, Het Kadaster is different in that it is a governmental organization that has a different function than Achmea. However, in terms of cybersecurity needs, and then especially encryption, the perspective of the CISO does not seem to be that different. In both cases the CISO was interviewed, so the comparison was easily made. This will be clear in the discussion per research question below, where similar results are found.

5.8.1 Need (RQ1)

As was the case with the Achmea interview, the need turned out higher than initially estimated. Initial estimation too low as a result of not understanding how they have to manage data, as explained in the summary report above. These kinds of complications may be applicable to a lot of publicly available information, there are still many security requirements to these kinds of data sets, so simply saying it is public information so the need is lower is inaccurate. Still interesting to see how need is so far been estimated high by CISO's themselves. Can also be a result of the function they are in, their job is to be concerned with cybersecurity so for them the need always seems high. However, they did give good reasons for their higher estimation of need.

So it could also be that need is not normally distributed over low, medium and high in the model handled here, it could be more skewed towards high. This can be the result of a number of things, such as the increased data dependence in modern organizations.

5.8.2 Readiness (RQ2)

Interesting here is the confidence with which the answer was given to the question about what they know about the quantum threat. The word 'enough' being used, indicating that they do not need to no more at this point in time. The argumentation used for this again referred to the point about buying commercial products that protect against the quantum threat when they come on the market. The common perception seems to be that these products will easily be integrated into the IT systems that they use. As will be explained further later, this does not mean that they will not need to go through the phases of the readiness model described. Also, there might be a slight misinterpretation on the interviewee side, where they interpret the model describing a process of internal technology development. The question is again how easily these new products will be integrated into the organization. This also depends on which solution is to be integrated, QKD has different implementation requirements than PQC. The interviewee's were only referring to PQC solutions, which would mainly require a software migration.

The interviewee also critiques the question about which stage they are in with the rational that they are not the party that needs to be thinking about this. This again ties in with the theme of not having to develop any products themselves and that they simply will be able to buy the products. This will be discussed in more detail in the overall conclusions of the data collection. Nonetheless, the interviewee placed themselves in the initiation stage.

5.8.3 Strategy (RQ 3)

As with Achmea they do not have a specific strategy for the quantum threat. They are reactive to how the market develops and buy commercial quantum safe products when they are available. They differ to Achmea in that they also tend to follow government wide security policy. There are a lot of government parties (such as the AIVD and the police) that are more proactive in their quantum safe strategy. In that sense, the government has a good amount of knowledge on the issue and is in a position to develop a good strategy. On the other hand, the government is a large bureaucratic organization in which these kinds of strategies are hard to implement. Also, not all branches of government have the same requirements for their IT systems, the differences might be big enough that Het Kadaster still needs to tailor the strategy to their situation

The question is again whether or not this reactive strategy is justified. Is the problem being underestimated and could the migration be more of a challenge than they think, or are they correct and will it be solved externally after which they can just buy the products. Other factors also weigh into the decision, there are many threats to cybersecurity that they have to deal with. They have limited resources, they have to make a decision on where to spend them. This is cyber risk management, it is apparent that the current estimation of the risk of the quantum threat is low. This will change in the future (this the interviewee's acknowledge), depending on the development of the quantum threat. Once this is high enough, they may decide to spend more resources on the issue and develop a strategy.

5.8.4 Conclusion Het Kadaster interview

Again, the need here was higher than estimated beforehand. This time due to a lack of understanding of how publicly available data is still sensitive if accessed in certain ways. The

possibility that need is not normally distributed over the three categorizations was also raised here, with the main reason being the dependence on data of modern organizations. This insight, if true, would imply that the quantum threat will have a greater impact. In terms of readiness and strategy Het Kadaster is in a similar position to Achmea, in the initiation phase and having a reactive strategy. That while the need is relatively high. In the next case it would be interesting to see an organization in a different readiness phase and with a different strategy.

5.9 ABN Case

The case is structured in a similar way to the interviews, it being split up into the three sub research questions. Here, instead of having interview answers, they will be collected from online sources. Following this a discussion will be had of the implications of the findings. The case selection and the description of the organization can be found in the categorization of organizations section.

An important part of the case involved ABN AMRO's CISO's website (http://martijndekker.eu/), this contained a number of his publications and other information. He has 20 years of experience driving security strategy of organizations. These sources allowed for a good insight into his positions with regard to the quantum threat. They are referenced a number of times in the case, along with other relevant sources such as the ABN AMRO website. Table 10 gives an overview of the main findings.

Table 10: Main results ABN AMRO case

Need	Readiness	Strategy
High: • No change to earlier categorization	**Implementation:** • Testing quantum safe technologies with partners • Dedicated team on the quantum threat	**Proactive:** • Emphasizes importance of preparing for quantum • Crypto agility of importance

5.9.1 Need (RQ 1)

As this categorization has already been done on the basis of online sources there is not anything to add here. It is a categorization with a high degree of confidence, and also something they say themselves about their need. Unlike Achmea and Het Kadaster, as ABN AMRO has already been put in the highest need categorization it is not possible that it turns out higher.

5.9.2 Readiness (RQ 2)

This is an interesting one to discuss as the high need categorization could imply a higher state of readiness. In the Achmea interview it was mentioned that the CISO of ABN AMRO has a whole team on the quantum threat.

> *"He has a whole team on quantum, and 500 people on cyber security under him. I have 12, it's a different order of magnitude." (Interview Achmea)*

Also, they are already doing projects with other organizations to develop solutions. They have partnered up with Qutech to develop QKD for secure banking(Qutech, 2019).

These two things alone puts them at least in the adoption phase, having passed milestone 2 of the readiness model developed here: **Decision to gather information about processes and possible solution fit has been made.**

The third milestone is: **Sufficient knowledge of processes and solutions has been gathered to implement.** It is not clear whether they are this stage yet, this information is not readily available. It can be safely said that no solution has been implemented yet, as this would likely have been disclosed openly. The fact that they are partnering up to develop QKD solutions says they are testing out potential solutions. The question is whether this should already be considered implementation or not. This is expanded on further in the discussion.

5.9.3 Strategy (RQ 3)

As can already be concluded from the readiness findings above, ABN AMRO has a more proactive strategy than Achmea and Het Kadaster. It is even known what technology they are developing, namely QKD. This does not mean they are solely focusing on this technology, most likely they are also exploring PQC solutions. From a technical perspective alone this is necessary, as QKD cannot authenticate and requires additional asymmetric cryptography to do so. For this PQC has to be used to be completely quantum safe. Martijn Dekker's article in Financial Services Information Sharing and Analysis Center(FS-ISAC), called " Why All CISOs Need to Prioritize Quantum Tech Today" also gives insight into ABN-AMRO's perspective on the quantum threat (Dekker, 2022).

Next to advocating for the importance of learning about the quantum threat, he also makes suggestions for strategy, naming four points:

- Familiarize yourself with the spectrum of quantum technologies now in use
- Leverage quantum in your own security measures
- Learn how to protect quantum technology
- Get access to quantum talent

He also emphasizes the importance of crypto agility, and that this should be prioritized to be ready for the quantum threat. Crypto agility refers to the ability for the IT systems to switch to different cryptographic algorithms easily. This is of importance when switching to PQC for instance.

It should be noted that these are strategies articulated by the CISO of ABN AMBRO, not necessarily the strategies that are also implemented at ABN AMRO. It is reasonable however to assume that they are at least similar, which is what will be assumed here.

5.10 Discussion ABN AMRO case

First of all, the fact that the method for this case is different than the other two needs to be discussed. Although an interview would have allowed for more directed questions and follow up questions, giving more details about the positions of ABN AMRO, the method used here is still adequate as there was sufficient information online to answer the research questions. The method is also appropriate from a process perspective as the data collection method is iterative and not meant for strict comparison, and because the same research questions were the subject of all the interviews and cases.

Another point that makes this case comparable to the other two is that the CISO was again a source of a lot of information. Due to the fact that he has a lot of his opinions in online sources allows for comparison with the other two interviewee's.

This case stands in contrast to the other two cases, especially in terms of the readiness and the strategy that they employ. The CISO of ABN AMRO also has a different opinion on how organizations

should prepare for the quantum threat, which is an interesting difference to see. In the discussion here the need categorization will be brief, mainly the readiness and strategy are of interest.

5.10.1 Need (RQ 1)

The high need categorization remains justified, unlike Achmea and Het Kadaster it did not change. In the cases of Achmea and Het Kadaster the relatively high need did not go paired with a more advanced stage of readiness, in this case it does. This at least indicates that they are more proactive, whether it is enough is not necessarily true. These thing tie into the next two research questions discussions.

5.10.2 Readiness (RQ 2)

ABN AMRO is in either the adoption or implementation phase of the readiness model, putting them ahead of Het Kadaster and Achmea. Whether they are in the adoption or implementation phases depends on where you place the current activities ABN AMRO are undertaking. In 2019 they started partnering with organizations like Qutech to look into QKD, where they also started testing. The question then becomes, is testing part of the implementation phase. The implementation phase starts when a decision has been made to implement a technology. This would involve the implementation of a technology that is then used in real operations. A test could develop into that eventually, but not necessarily. As a test has the potential to become an implementation, putting testing in the implementation phase makes sense. There is still the possibility that the test fails, in which case the organization would be put back into the adoption phase. This suggests that the model is less linear and more iterative in nature, this will be further discussed in the adjustment of models section. Another aspect that points at ABN AMRO being in the implementation phase is that a team has been assembled especially for this problem.

As explained earlier in the model description, this phase can be very long time wise and it differs per organization. As ABN is a large bank with high security requirements it might be especially long. This is a limitation of the model, getting an indication of where in the implementation phase you are would help. One thing that was not tested was whether they would place themselves there as well. This would have been useful information to test the model, which is one of the main limitations of doing a case rather than an interview.

5.10.3 Strategy (RQ 3)

The more proactive strategy ABN AMRO has is in line with their high need and higher state of readiness. Being in higher readiness implies that a more proactive strategy has been adopted because action is being taken. This is something to take away for the strategy part discussed later on.

It is interesting that Dekker say's all CISO's should prioritize quantum, which stands in contrast of what the CISO's of Achmea and Het Kadaster where doing. Interestingly, the focus seems to be on QKD and not so much on PQC. A discussion of this is not so relevant for the focus of this study, so the pro's end con's of the technologies will not be discussed further. What is interesting is the proactive strategy, suggesting to hire quantum talent, leverage quantum in your IT and to prioritize crypto agility.

Crypto agility is an interesting concept as it ties in with the issue that has already come up, about how easy it is to integrate commercial quantum safe products into an organizations IT infrastructure. The fact that the concept exists indicates that is not always as easy, in the cases of Achmea and Het Kadaster they should at least know their crypto agility in order to estimate whether their reactive strategy will work. It was not asked whether they had considered this, but is an important concept. In

the adoption phase there is a sub category of knowledge of processes, in here it is of importance to get a good estimation of your crypto agility.

The fact that there is more concern in ABN AMRO about the quantum threat, and that it is emphasized that it may not be so easy to solve, is an interesting contrast with the other two interviews. It may be typical for the phase they are in, where actual steps are being made to solve the problem and where an actual understanding of the problem is developed. In the initiation stage the problem is still a black box, where organizations may be prone to underestimating the problem.

5.10.4 Conclusion ABN case

Although a different method was used, useful comparison was still possible to do between the different cases. There were interesting differences, in readiness ABN AMRO is more advanced, being in the implementation stage. Given the high need this is somewhat expected. The strategy of ABN AMRO is much more proactive as a result, actively testing and collaborating on solutions. The difficulty of solving the problem is also perceived as higher. This may also be the result of the responsibilities ABN AMRO has, which is discussed further in the readiness model discussion.

5.11 Adjustment of models

In this section the findings from the interviews and cases are discussed further, and used to make some adjustments of the need and readiness models made in the thesis. The insights from the data collection have already been discussed to a certain extent after each case, here they will be brought together. Table 11 gives an overview of the main findings of the interviews.

Table 11: Overview of the interviews and case results

	Achmea	**Het Kadaster**	**ABN AMRO**
Need	High	Medium/high	High
Readiness	Initiation	Initiation	Implementation
Strategy	Reactive: Buy products when available	Reactive: Buy products when available	Proactive: Test and contribute in developing.

5.11.1 Adjusted need model

The need model was not tested in its details of workings in the cases, but in the accuracy of its categorizations of the organization. Although the detailed need model was not asked about specifically, in the discussions with the interviewee's one important aspect that is missing was brought up twice. This shed light on an aspect of need that was actually already known but not included. As it was mentioned twice here it shows that it is important to add. That aspect is the attack threat level, in other words, when the quantum threat will actually be able to break encryption. This aspect increases the operation vulnerability over time.

> **Attack threat level:** The capability of an attacker, in the case of the quantum threat this is tied to the development level of the quantum computer.

The threat of store-now-decrypt later was also mentioned in the interview with Het Kadaster. This is a concern for organizations that have information that can be saved now by hackers (still encrypted) and still be sensitive when it can be decrypted by a quantum computer. This has an effect on the need by making the time aspect even more urgent, it forces organizations to act as if the quantum threat is already here for certain information types. Any information that is threatened by store-now decrypt later suffers from forward sensitivity.

> **Forward sensitivity:** How long information remains sensitive, making it vulnerable to store-now-decrypt later attacks.

This variable has an effect on the attacker threat level, as it increases it depending on how long the forward secrecy requirements are. It essentially forces an organization to consider the attack threat level of the future on current information being used. The two changes discussed above, adding attacker capability and forward secrecy, have been integrated into the model in Figure 21.

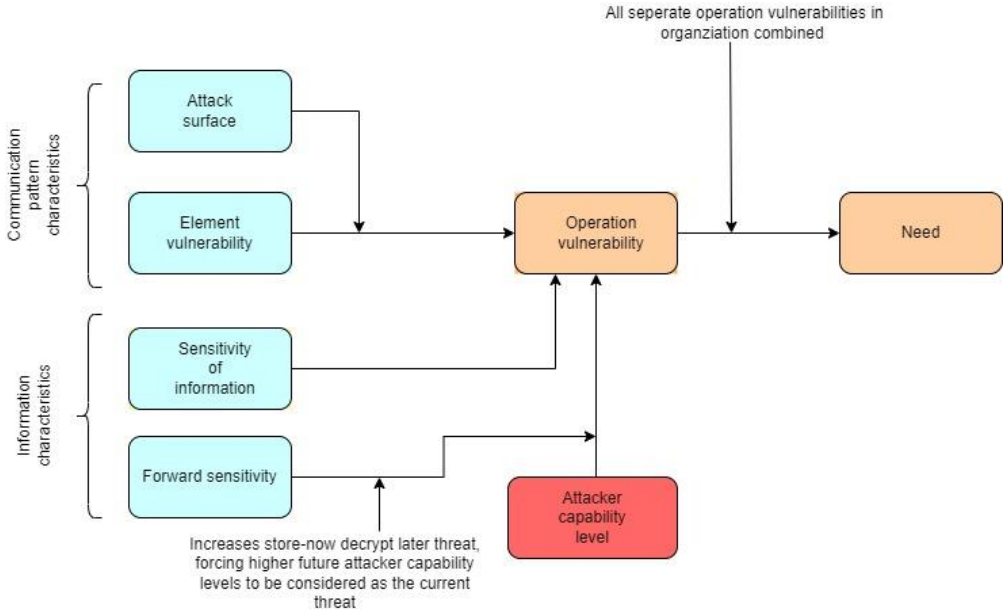

Figure 21: Adjusted need model

As mentioned, this has not been tested, but interesting framework to think about the problem. The addition of these new sub elements does add to the complexity of the model. In section 3.4 it is explained that the need approach taken here is different to the general need as it takes the gaps of sub elements rather than the gap between the total end state and current state. In Figure 21, each element in blue has a gap between a current and desired state. In the original model it was not explicitly specified that the gap of each sub element is dependent on the attacker capability level. Now that has been made explicit, even taken to a slightly different level. As the attacker capability is a variable that effects every gap in the sub elements, it can be taken out of each element as one variable. Now, it has been placed next to the total operation vulnerability, which has shifted where the need gap is placed in the model. Now, the need is the gap between the operation vulnerability and the attacker capability level.

Note, when considering attacker capability it is crucial to take migration or implementation time into account. If you do not then it would imply that the need of all organizations at this moment is zero, as there is not powerful quantum computer right now. Rather it has to consider what the attacker

capability will be by the time the organization is able to secure its current operation vulnerabilities. Put differently, currently an organization has a certain element vulnerability, and it would take 5 years to migrate and remove the vulnerability. That means that the attacker capability of 5 years from now has to be considered. This is an unknown level, so it has to be considered from a risk assessment perspective, probability of occurring multiplied by the potential impact. These are some important details in operationalizing the model described here.

5.11.2 Adjusted readiness model

As opposed to the need model the readiness model was tested for the actual validity of the model, by using the three step approach discussed in the interview design. As a reminder, this involved first asking the interviewee to place their organization in the phase they thought they were in. After this specific questions were asked based on indicators of the model, to have a different way of placing the organization in the readiness model. These two can then be compared and discussed in the third step with the interviewee. This approach gave a number of useful insights that can be used to adjust the model. Again, Table 11 gives an overview of the main results.

One of the most interesting results from the two interviews was that both Achmea and Het Kadaster do not seem to concerned with the quantum threat. They realize it will require a change in their encryption at some point in time, but they will simply be able to purchase commercially available quantum safe technologies when they are available. This approach raises a number of questions, namely whether or not it is justified to think integrating these commercial products will be so easy that preparation is not yet required. It is clear that they are not really preparing a lot from the fact that they are still in the initiation stage of the model. In this stage still very little is known about the problem, which might contribute to the easy thinking about the problem.

The two interviews stand in contrast with the ABN AMRO case in two ways, firstly that ABN AMRO is in the more advanced readiness stage of implementation(more on this in a bit). Also, they have a more proactive approach to the problem, and do not see it as just buying commercially available products when they come on the market. They are actually involved in testing and developing the technology in collaboration with partners.

The fact that a different attitude is adopted to the problem could also be a result of the type of organization they are or the responsibilities they have. As was mentioned in the interview with Achmea, ABN AMRO is a system bank that has more responsibility on the infrastructure of the Dutch financial system. Although they do not develop quantum safe technologies by themselves, they are much more involved with the parties that are doing that. This makes the process they are going through different than an organization that is much less involved with technology creating organizations, like Achmea and Het Kadaster. This is a variable that can be added to the readiness model, but it first needs to be defined properly.

A concept that is relevant to this from literature is Pavitt's taxonomoy (Pavitt, 1984), which classifies innovation models according to different types of organizations. Pavitt looks at industrial firms, which the organizations here are not. Nonetheless, the general concept is still relevant. The taxonomy gives four different categories of industrial firms: supplier-dominated, scale-intensive, specialized suppliers and science based. Similar categorizations could be conceived of in the context of IT. Investigating this further could be interesting, and it will be suggested in the further research chapter.

One aspect of Pavitt's taxonomy that can be used here is the supplier-dominated categorization. Here it can be adapted to the IT context, as a measure of how involved an organization is in the actual development of quantum safe technologies. So here we define:

Degree of R&D: The level of involvement in development of quantum safe technologies.

Rather than a categorization this can be used as a variable, which ranges from organizations that are developing the technologies(eg. IBM, Microsoft), to organizations that will only implement them(such as Achmea and Het Kadaster). ABN AMRO would fall somewhere in between those two extremes. The degree of R&D would affect the readiness process by changing what the organization has to do. It has an effect on the amount of time it needs, the amount of resources it needs to invest and involves a different strategy. Using this in the model gives organizations a more accurate idea of what kind of readiness process they will be going through.

There still is a discussion to be had about how much the degree of R&D influences the readiness process in terms of complexity and how difficult the transition will be for the organization. Firms with low degrees of R&D, like Achmea and Het Kadaster, could still face complex implementation of technologies that they did not develop themselves. The fact that they have low levels of R&D resources might make it an even bigger problem, as they lack knowledge about the technologies. So it will definitely have an effect on what the readiness process will look like, but not necessarily as much on the complexity of the migration process. Also important to note, the degree of R&D is likely positively correlated at least to a certain extent to need. Although, this might not be a strong correlation, for example in the case of Achmea the need is high but the degree of R&D is low. These might be the organizations at the greatest risk.

The complexity of integrating products into the organization ties into the concept discussed in the ABN AMRO case, crypto agility. This is another aspect that has to be added and emphasized in the readiness model, determining the crypto agility of your organization is an important part of knowledge of processes, in the adoption phase.

Crypto agility: How easily an organizations IT systems can change underlying encryption.

Without this knowledge the organization can not estimate how difficult implementation of the new technologies will be. Next to this, in the initiation phase organizations should be aware that they could have an issue with crypto agility, which might make them decide to enter the adoption phase sooner.

In the discussion about whether or not ABN AMRO is in the adoption or implementation phase it was clear that there is some ambiguity. Eventually it was argued that they are in the implementation phase, due to the fact that they have a team actively working on the problem. One of the reasons for ambiguity was whether or not the tests ABN AMRO are running with QKD are an implementation or not. Not all test end up being successful, in which case they are not an implementation. This points at the iterative nature of how such readiness processes actually unfold in real organizations. The model here suggest this is a linear process, while in reality it is much more nuanced. There can be steps back if certain test turn out to fail, there can also be differences in readiness among different branches of an organization. The iterative aspect had already been included to a certain extent in the original model, in the post-implementation phase it was emphasized that developments in threats and solution could bring the organization back in readiness.

Now it is clear that the iterative concept has to be expanded to more areas of the model, specifically between the implementation and adoption phase. There could be a number of iterations between

the phases, and aspects of the phases may actually happen in parallel. For instance, the knowledge of solutions aspects of the adoption phase is something that will keep expanding when the implementation phase has been entered. Especially as problems are encountered when implementing, which will require expansion of knowledge on the process. Figure 22 shows the adjusted readiness model.

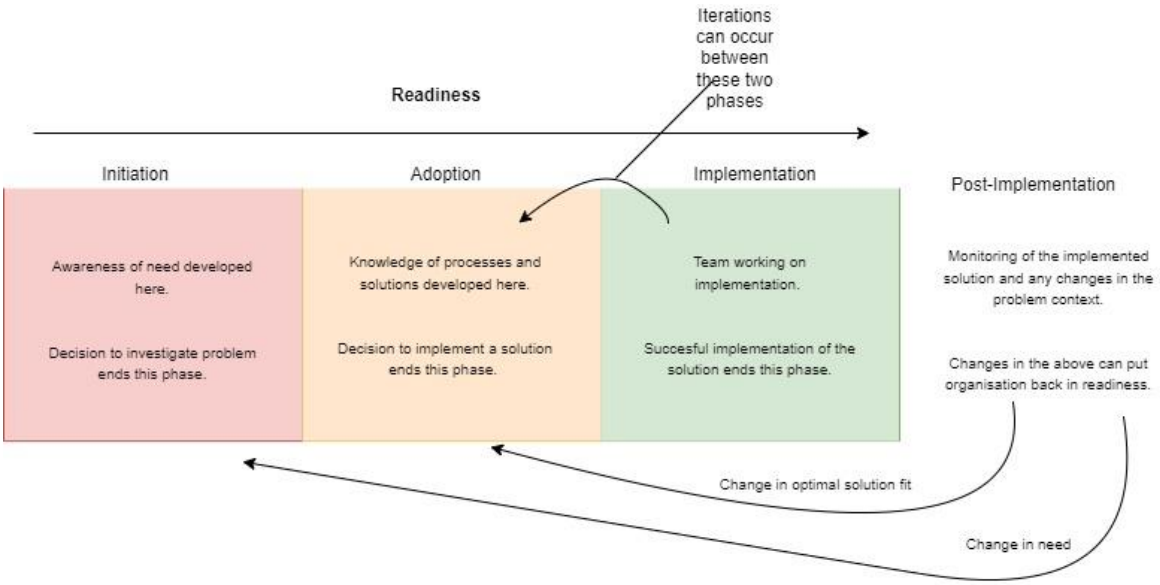

Figure 22: Adjusted readiness model

The question is whether or not such a linear model is even at all appropriate anymore. It is still a useful way to categorize your organization, but it has to go with the understanding that certain aspects will be iterative or run in parallel. That way the model informs a manager of what activities need to be done and where they are at approximately. This has important implications for the strategies that the organization must adopt, as will be explained in the next section.

5.12 Strategy implications

This chapter approaches strategy in such a way that it is most useful for the target audience of the research, namely managers of organizations. Specifically what a manager must do within the organization to be ready for the quantum threat. Internal strategy is therefore the focus, however, as will be seen in more detail later, internal strategy is tied to external strategy in the case of this problem. For that reason external strategy has to be considered, along with other external factors such as the problem characteristics of the quantum threat. These two things are discussed first in the chapter, but only to a limited extent. It is explained mainly in relation to internal strategy, which is the subject this research can say much more about.

After this the internal strategy is discussed, which is split up into two parts. First, the impact of need on internal strategy and secondly the impact of readiness on internal strategy. Why this approach makes sense and works is explained in the beginning of the internal strategy section. First, the problem characteristics and external strategy.

When discussing strategy it is important to have a good understanding of the problem characteristics, as this heavily influences strategies. The problem characteristics have been discussed in chapter 2. Some of the main points where:

- Uncertain development of quantum computer, leading to lack of urgency.
- It is a multi-actor problem
- It is technically complex, involving the entire internet.

Furthermore, before diving into the strategy implications it has to be clarified at what level strategy will be discussed here. There are two categories of strategy, external and internal strategy.

> **External strategy:** This looks at how the organization acts in the multi actor network they are in. It involves how they collaborate with partners, how to deal with standards being developed, but even things like geopolitical considerations.
>
> **Internal strategy:** This is focused on how the organization manages the implementation of quantum safe technologies the most effectively according to the organization's needs.

These two are not completely independent. For example, if an organization is looking to find the best technological solution to implement for its organization(internal strategy), it needs to consider what its partners are doing with whom they share data (external). With this in mind, the two will still be discussed separately.

The problem characteristics mentioned above mainly influence the external strategy, but also influences internal strategy indirectly. The models developed in this thesis regarding need and readiness are focused on internal characteristics of organizations (especially the readiness model). These tools are useful for discussing strategy, and will be used as the framework to discuss internal strategy in. As a result of that internal strategy will be the focus. Some of the external strategy considerations will be discussed first, especially the ones that influence internal strategy.

5.12.1 External strategy

The multi actor problem aspect significantly influences how an organization must act. In most cases the organization cannot act alone, they are dependent on other parties in a number of ways. Also, the uncertainty of the development of the quantum threat makes it that there can be a lack of urgency in many actors. This makes the fact that an organization is dependent on other actors a potential problem.

Partners they share data with will need to have compatible systems, influencing what technology solution an organization must chose. In cases where organizations manage the entire end to end communication chain, the organization can act alone. In many cases collaboration with partners will be necessary to come to shared solutions. Due to the technically complex problem, and the large multi actor network, this could be a significant challenge. Also, it could be a bottle neck in your internal strategy. Where you are willing to advance readiness, but you have not been able to determine standards for shared solutions with partners yet. For this reason, this collaboration is something that needs to be prioritized. Developing aspects that are not dependent on external parties should be done, such as crypto agility. That way, once the external bottleneck has been solved the solution can be implemented quicker.

Also, organizations are more or less dependent on other parties for the development of the technology depending on the degree of R&D they have. This influences internal strategy and is expanded on in the readiness part of internal strategy. In certain internet applications there is also a level of dependence on standardization, for instance the NIST standard for PQC algorithms that is still being developed. This can also be a bottleneck for your internal readiness, an organization with high need could then consider not to wait for NIST where possible.

5.12.2 Internal strategy

In discussing internal strategy the models made in the thesis are used as a framework. They are both used in slightly different ways, the need model influences more general aspects of the strategy. The readiness model goes more into detail, and uses each phase to describe what strategy to use in that phase. There is some cross dependency, meaning that an organization with a different need will act differently per readiness phase. Where this occurs it is highlighted.

This approach to internal strategy is effective as it begins by considering a dimension in which organizations vary, the need. This is the first thing a manager should consider as it impacts strategy across the entire process of becoming a quantum safe organization. It impacts urgency, the resources that should be deployed and the technological solution that best fit the organization. From there the manager can start looking more into the actual process and what strategy to apply per phase. These phases are not to be taken rigidly, as explained earlier the readiness model seems linear but in reality these processes never are, there will be iterations between phases. This also means that strategies will overlap into different phases, these are also not to be taken rigidly in each phase. Rather, they are strategies that should be emphasized on at that point in the process. An alternative way to present these strategies would be to just provide all the strategies without an indication of the phase of the process. This is less effective as it gives less sense of what to prioritize, and it does not provide a structured approach in time. Table 12 shows an overview of the strategy implications.

Need impact on strategy

Need influences a number of things in terms of strategy. Urgency, amount of resources to invest, what to do with data being communicated now and what technology solution best fits the organization.

> **Urgency:** This impacts how far in the readiness process the organization should aim to be. It impacts whether or not they can wait for more standards to be made and for other parties to develop the technology further, allowing them to 'free ride' more. It also allows for more time to coordinate solutions properly with other parties. If urgency is very high, less time to wait for standards and other parties, have to take more initiative yourself.
>
> **Resources:** Higher need requires more spending of resources in all stages of the readiness model. This is due to the fact that there are more vulnerabilities in your organization(see need model), so more problems need to be solved. Also, the impact of the quantum threat will be greater on the business model of the organization.
>
> **Current communication:** The data being communicated now may need to be adjusted based on whether the organization has store-now-decrypt later vulnerable information. Should stop sharing that information as much as possible on digital channels if that is the case(reduce the attack surface).
>
> **Technology fit:** The need you have also influences the technology solution that best fits your organization. Especially the component of communication pattern influences this. Which technologies fit best is dependent on a lot of variables and is different per case. This is something that is out of the scope of this thesis, but is important to consider when formulating a strategy.

These are general strategies related to your need level that do not really change per readiness phase.

Readiness impact on strategy

The readiness model made in this thesis serves as the frame work for all the strategy discussion. It lends itself very well for this purpose, as it has already strategic goals defined within each phase. Per readiness phase there are different strategies, but there also some general differences that will change an organizations strategies across the phases. One of those has already been discussed above, the need. The second comes out of the readiness model and is the degree of R&D concept, this is discussed first.

> **High degree of R&D:** If this is high, you will be more involved in testing and developing the technology, this influences what kind of knowledge you need to acquire in the adoption phase, and it influences the implementation phase as you will be more involved in testing. It will involve more resources also, requiring more iterations to successfully implement. A larger team is required to implement.
>
> **Low degree of R&D:** If the degree of R&D of the organization is low, less resources, less testing and less iterations will be involved. However, the organization should not underestimate how difficult integrating new cryptology or other quantum safe technologies into IT infrastructure is. The process of understanding how to implement the technology and to make it all work will still requires iterations and significant resources. One way to estimate how hard it will be is to have a good understanding of the organizations crypto agility.

Now the strategy will be discussed per phase, where the implications of degree of R&D are relevant it is mentioned. Table 12 gives an overview of the strategies per phase.

Table 12: Overview of strategy implications per readiness phase

Initiation	Adoption	Implementation	Post-implementation
Understand need Understand complexity Involve people Learn from others Understand external dependence	Understand and develop crypto agility Inventorize operations Prioritize operations Collaborate	Plan for long process Manage iterative nature	Monitor changing technological context Monitor implemented solution

Initiation phase

In this phase there is no implementation strategy yet, here the organization must learn about the problem.

> **Understanding of need:** Even before learning about the problem, the organization must have a good understanding of its need. It likely already has idea of its general cybersecurity needs, this is a good starting point. Using the need model described here they can get a good understanding of their need. Especially if they are able to identify their main vulnerabilities in their cryptography.

Understand complexity: After this the organization must get to grips with how complex the problem is, and understand that implementing these technologies could have significant impact on their IT systems.

Involve people: To do this many people in the organization have to get involved, especially the people who work with IT and would have to implement solutions if it came to it. Here the organization can get the first idea of what it is going to be like. Having a good understanding of the crypto agility of the organization will also help estimate how hard implementing new encryption is going to be.

Learn from others: Also important here already is to learn from others, and to start communicating with partners with whom you will need to coordinate your solutions. Learning what other organizations are doing can save having to research the same things. It is worth considering hiring consultants who specialize in this area, who can give tailored advice to tackling the problem (this can be done in the adoption phase as well).

Understand external dependence: Developing a good understanding of how dependent your organization is on external parties for the implementation of the solution will give a better understanding of the complexity of the problem also.

At this point it is also important to assign resources and define responsibilities for the next two phases.

Adoption phase

This is the most strategic phase of the whole readiness model, here is where the solution selection is made for the organization. This phase has two parts two it, knowledge of processes and knowledge of solutions. Knowledge of processes involves understanding the organizations operations, how vulnerable they are and what cryptographic algorithms are underneath. Knowledge of solutions then looks at the technologies which need to be implemented, understanding how they work so that they can be integrated into the organizations IT. Both areas should be explored simultaneously, as you need information transfer between both to get the understanding that you need. Strategies regarding knowledge processes are discussed first:

Crypto agility: This has already been highlighted a number of times as an important concept. In the initiation phase it was already suggested that an understanding of the crypto agility of the organization is useful for understanding how difficult integrating new cryptography will be. If this understanding of crypto agility was not there yet, then in this phase it should be developed. This is especially important if the degree of R&D of the organization is low, as that means that an externally developed technology will have to be integrated into the IT. Even though the organization is not yet in the implementation phase, improving crypto agility already here is a strategic priority. This can be done before there is complete knowledge of all the solutions, so waiting for the implementation phase is not necessary.

Inventorize operations: A complete inventory of the operations in the organization is need with accompanying understanding of how they need to be adjusted cryptographically. With this the right solution fit can be found, and operations can be prioritized.

Prioritize operations: Given the complexity and potential long duration of implementing solutions, identifying the operations with the highest vulnerability(as defined in the need

model) to prioritize is wise. Focusing resources here will help accelerate the process of finding the right solution fit, so that solutions can be implemented here quicker.

Collaborate: As explained before in external strategy, this is a multi-actor problem and in many cases the organization cannot act independently. This external aspect has significant consequences for the internal strategy s it is discussed here again. Collaboration is necessary to understand where shared solutions need to be developed with business partners. This also involves following standardization activities. If external parties are slow and the organization has high need, then looking where independent action is possible may be necessary.

While developing a good understanding of the own process the solutions that are available can be explored. This consists of finding the technology that best fits the communication patterns of the organization and the overall need. It will again be dependent on what other parties do in many cases. What technologies exactly is dependent on a lot of factors, and is not in the scope of the project here. In technology solutions there is an overview of different technological solutions and hybrid combinations of those. This is an indication of how many options there are and how complex finding a solution can be. Once this is completed a complete implementation strategy can be finalized.

Implementation phase

Strategically there is less to be said about this phase as it involves executing the strategy that has been developed in the adoption phase. Here it is about the practical steps that mainly the IT department has to execute to successfully implement the technology. From a managers perspective there are a couple of points that are important to realize about this phase:

Long process: It is important to realize that this phase can be very long due to the complexity of implementing these technologies. This has to be managed accordingly.

Iterative nature: Also, the iterative nature of the problem is important to consider. Once this phase has been entered activities from the previous adoption phase will still be necessary at times. As explained before the model is iterative and activities from different phases can run in parallel, the organization has to be aware of this and manage accordingly.

Post-implementation phase

Again, there is not much to be said about this phase from a strategic perspective. In the model description the main activity described is monitoring. This is the strategy to follow here, monitoring market developments on both the threat and solutions side. A significant advance in quantum computing could force the organization to adapt again, putting the organization back to the adoption phase. A development in quantum safe technologies could also prove to provide a better solution fit for the organization. Next to the external monitoring described above, internally the solutions should also be monitored. They should be tested regularly, to see if they function as they should.

5.12.3 Wait and see strategy

Having explained the approach to strategy this thesis takes a step back is now taken to a result that came back multiple times in the cases. Both Achmea and Het Kadaster stated that they are using a wait and see strategy, in which they wait for the market to develop a technological solution which they can buy and integrate into their organizations.

As already mentioned there are some issues with this approach, the first being the underestimation of integrating new technology into the organizations IT. Without knowledge of how the integration process works the organization will not be able to estimate how long it will take. In the case of this problem this can have severe consequences, as it could mean longer operation with unsafe communication. Another issue is that it assumes that the organization cannot already start preparing for the integration of new solutions. For example, even though the organization might still abstain from developing or looking into quantum safe communication technologies they could start improving crypto agility, or hiring better IT staff.

Yet another pitfall of this strategy is that it assumes that the market will be able to bring the correct solution in time. It is very much possible that the quantum computer develops faster than the market can develop a widely implementable solution. There is also a wider issue, if a lot of organizations adopt this strategy it hamper a market even forming around the technological solutions. It will reduce apparent demand for it, and it will decrease the amount of actors collaborating and pushing for a solution.

Nonetheless, there are some potentially positive aspects to the strategy. It reduces the amount of resources spent significantly, at least initially. If it turns out that integration of the technologies provided by the market is not such a big issue, then it would be a cost effective strategy. This is likely not the case though. Also, If the development of the quantum computer turns out to be slow(or doesn't happen at all), then the strategy pays of a lot by avoiding sunk costs. Also, there are different degrees of how passive an organization is when deploying this strategy. If an organization still actively follows trends and listens to advice of experts, the strategy could be less risky.

Overall the strategy is risky to use and not advisable. This does not mean that every organization has to completely commit to developing quantum safe technologies in house, but that they should at least be a proactive actor in the developments of these technologies.

6 Discussion and Conclusions

Having adjusted the models the overall discussion can now be had. This will be done per research question, and it will combine the discussions of the different stages of the research used to answer that research questions. As there was already discussion at all the different stages, a lot of the points will be repeated. There was discussion of the literature, there was discussion of how the models should be constructed and there was discussion of the results from the interviews and case. The latter discussion was integrated into the adjusted models to a certain extent. So, the discussion here will be slightly summative in nature, next to having some additional discussion points.

6.1 Discussion research question 1

As a reminder, the first research question was:

What determines organizations need for quantum secure communication?

The first issue encountered with this problem is the vagueness of need in literature, and its broadly applicable nature. The fact that it is broadly applicable makes it so that researchers often define it in the context of their own research. This literature did not contribute much to the development of the need model. Instead the model was built up from two sub constructs that make up need in the context of this problem, communication pattern and sensitivity of information. Given that communication pattern can refer to a lot of characteristics that are unique to every organization, going into details was not in the scope. Rather than doing that more general concepts of attack surface and element vulnerability were used. This allows for a conceptual framework to think about communication pattern, but has limited practical applicability as the concepts are very general. To make it practically applicable there has to be further work done, an idea of what that could look like is given in further research.

After this the second aspect of sensitivity of information was discussed to be used in the model. This was more straightforward, ended up being the main aspect that was used to determine need for organizations in this thesis. That this plays a crucial role in need is fairly obvious, making it straightforward. The choice was made to use sensitivity as the main criteria to classify organizations in different need categories in this thesis. This was a reasonable choice given the scope of the thesis, communication pattern criteria are far more complex and case specific.

Although using sensitivity of information as the main criteria to determine need seemed straightforward at first, in the interviews it turned out to be less evident. Need estimations were too low in the case of Achema and Het Kadaster. In the case of Het Kadaster the reason for the need estimation being too low was that sensitivity of information was estimated inaccurately. This had to do with the fact that although it is publicly available information, it is not supposed to be accessible in all ways(see summary report Het Kadaster for detailed explanation). This showed that taking a zoomed out view, seeing that the information being dealt with is public and labelling it as low sensitivity(in the NIST standard this would make it low in sensitivity), is not accurate. In a way this was already stated in the discussions of need, that determining need is very case dependent and is difficult to do very accurately without good understanding of the processes of an organization.

Now, this does not mean that the need model developed her is low quality and not useful. It means that in order to have an accurate result the model has to be applied in its entirety(communication pattern and sensitivity of information), and it must be applied more in depth per individual case. As

mentioned before, this would require some additional work in developing operationalized tests based on the model, especially in determining communication pattern characteristics(see further research).

Next to theses insights the data collection part gave some other insights that helped improve the model. One insight is not directly related to the research question but does have interesting implications. In making the three categorizations of need in the model construction, there was no discussion about how organizations may be distributed across the three categories. It might be logical to assume an even or normal distribution(if it were made a continuous scale) across the categories. However, all the cases investigated here were more in the high range, which might be indicative of how all organizations are distributed. This would have to be tested further, but seems very plausible. Given the high digital dependence of the modern organization, with a lot of operations running over the internet. If true, this would imply that many organizations would need to increase their readiness more quickly.

Furthermore, the insights from the data collection helped add two things to the need model that are specific to the quantum threat. The first was the attacker threat level, is an uncertain criteria but still important to include at least in the model. It was an aspect that was already discussed, just not included in the need model. This was also the case for the forward sensitivity addition, discussed but not included. It is an addition that is relevant as it is a unique characteristic of this problem, and something that might be overlooked if not included explicitly. Overall a fairly complete model resulted from the research, one that is also more broadly applicable to cyber security than just the quantum threat. To make it quantum specific the encryption has to be looked at, but it could be applied for other vulnerabilities as well.

In section 3.4 the theoretical contribution of the need approach taken here was discussed. With the additions made to the need model from the data collection this theoretical contribution has become stronger. This because the gap has been made more explicit rather than being embedded only in the sub elements of the model.

6.2 Conclusion research question 1

The research question was answered at a fairly general level, giving a good first shot at what determines need. As the scope was very general it is a zoomed out answer, giving a good starting point for diving into a specific organization and figuring it out in detail for that organization. As the goal of the thesis was more theory building, the zoomed out general nature is justified, it was successful in developing a framework in thinking about need. The data collection part, especially the two interviews, helped in improving the overall model, which is shown in Figure 23.

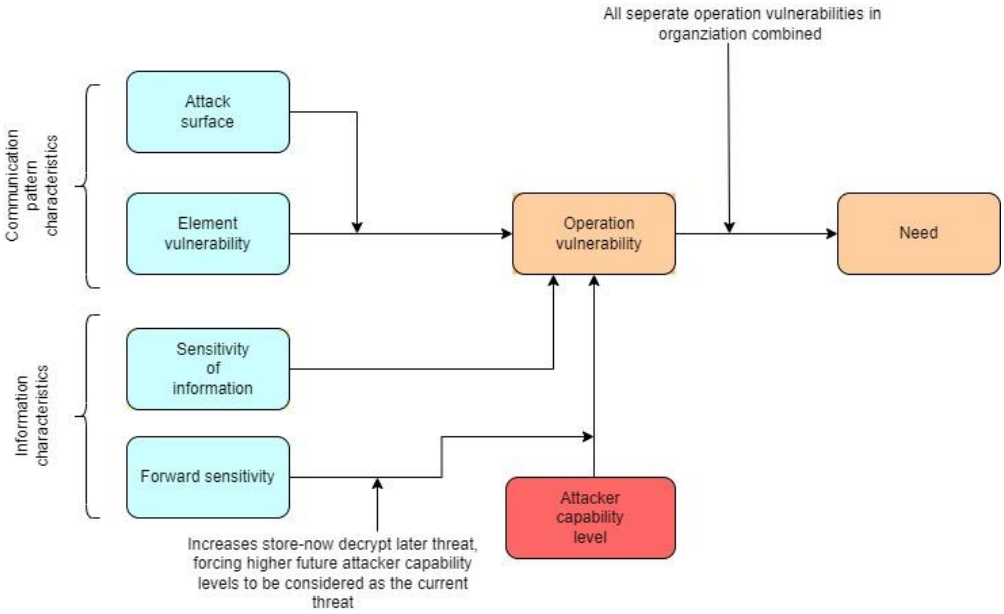

Figure 23: Adjusted need model

There are two main sub constructs that determine need, communication pattern and sensitivity of information. Communication pattern affects need by describing how large the attack surface of the organization is, and how vulnerable the elements on the surface are. The vulnerability being affected by the type of encryption being used in the case of this problem context. Sensitivity of information affects need by indicating how large the impact would be on the organization if data is hacked.

Next to the two main sub constructs there are two additional variables that affect need that are quite specific to the quantum threat. Those are the forward sensitivity and the attacker threat level. The latter is dependent on the advancement of the quantum threat, the more powerful it becomes the more acute need becomes for organizations. The forward sensitivity part has to do with the store-now-decrypt later threat, which is when an attacker stores current encrypted information to decrypt it in the future.

The way the context specific need has been approached here is a useful theoretical contribution. It highlights the problem with the general need approach, which looks at the gap between the complete desired state and the current state. Also, the issue of the end state not being fixed is highlighted, which is an important factor that makes a different approach to need necessary. Then, need is approached by taking the gap between the current and desired end state of sub elements that make up the need(see Figure 14). In the first model this was embedded in each sub element, in the improved model the attacker capability level was taken separately, as it effects each sub element. The result is a context specific need gap, between two changing variables, the operation vulnerability and the attacker capability.

To apply the model all these aspects need to be determined per operation in an organization. An operation refers to a business operation which uses some form of digital communication, for instance transactions with clients, or information sharing with suppliers. Each operation then has a certain need for quantum safe communication, all of the operations of the entire organization combined then gives the overall need.

What can be done to make the model more applicable in real scenarios is discussed in further research.

6.3 Discussion research question 2

Now a discussion in the same structure as above about research question two. As a reminder, the second research question was:

What determines the readiness for the quantum threat?

The literature study on the concept of readiness was challenging due to varying interpretations of the concepts in different streams of readiness literature. In the process of the research this led to some changes in direction and steps back to make sense of the literature. Eventually the confusion was cleared out, using the concepts of readiness progress and readiness adaptability to do so.

This in itself is a useful theoretical contribution, as it made clear what the different approaches are of the different literature streams. Also within the separate streams some potentially confusing aspects were cleared up, as in the case of the organizational readiness literature. Here it was shown what the different approaches are, the structural and the psychological approach. In this problem context the here the structural approach would be more relevant. This has to do with the 'under the hood' nature of the problem. Most employees would not see any change when quantum safe technologies ae implemented, it would mainly affect the IT department. A psychological approach then becomes less relevant, as this looks at how employees must adapt psychologically to changes the organization, which they will not really see in this case. Organizational readiness fell within the readiness adaptability categorization, which ended up not being investigate much.

The research went more towards the readiness progress interpretation, looking at the chronological process of becoming ready. This was the result of the intention with which the research was started (oriented to readiness progress) and incomplete understanding of what organizational readiness really entailed. This leaves the readiness adaptability aspect of the research question fairly unanswered. Answering this part would have been a significant amount of extra research, and was not feasible to do. This reflects on incorrectly estimated scoping, which was the result of the initial misunderstanding of the readiness concept. There was more in there than initially thought.

Nonetheless, the research question was still answered from the readiness progress perspective. The two readiness progress streams consulted were TRL and technology implementation literature. The latter ended up being the main basis of the readiness model constructed here. The TRL literature was not very applicable to an organization as it takes a project approach to readiness. This is a linear perspective with very concrete milestones, which is applicable to a technology but not easily converted to an organization. This is because an organization is much more dynamic, with many different departments, people and aspects that can be at different stages of readiness. The technology implementation literature was more suited to the thesis here as it was looking at the level of an organization. It still took a relatively linear approach by looking at different phases, but these are more general and leave space for iterative aspects typical of an organization in it. However, in the data collection part one of the reflections was that it did not account enough for the iterative nature of the organization.

This became evident from the ABN AMRO case, where it was not clear whether they were in the adoption or implementation phase. This because they were already running test with quantum safe technologies, which could become an implementation, but could also fail and not be implemented. This is evidence of iteration, implementation initiatives being taken, putting the organization into the implementation phase, those initiatives failing and putting the organization back into the adoption phase. This discussion was had in the adjusted model section, where the iterative nature was further included. That it does not account completely for the iterative nature still remains a limitation to a

certain extent, but that is the compromise that must be made to have a model that is actually useful. Managers can use the model delivered here much more practically, as long as they also keep the iterative nature of the reality in mind.

In the adjustment of the readiness models two more important insights were used form the data collection part, which significantly improved the models. The first came out of the responses form the interviewees, representing Achmea and Het Kadaster. They argued that they do not need to be so involved in the process of becoming quantum safe, as they will simply buy the quantum safe technologies when they come on the market. This is a reactive approach to the problem, which stands in contrast with ABN AMRO, who are being much proactive and involved in testing quantum safe technologies.

In the adjustment of the readiness model part a more detailed discussion is had on this, but it came down to the inclusion of the concept of degree of R&D. This is a measure of how involved an organization is in technology development, ranging from developing it in house to being completely dependent on third parties. This was inspired from literature about Pavitt's taxonomy. This addition is significant as it indicates how different types of organizations have to deal with the threat, based on the capabilities they have.

This ties in to the second important addition to the readiness model, the concept of crypto agility. This is a measure of how easy integrating new encryption technologies into an organizations IT infrastructure is. This is an important aspect to consider especially for firms with a low degree of R&D, as they need to integrate externally made products into their IT. This is an area where Achmea and Het Kadaster could be underestimating the problem. A good understanding of their crypto agility could significantly help them here, it would indicate whether their reactive approach is appropriate.

6.4 Conclusion research question 2

The goal of this part of the research was to give managers a model to understand the path towards becoming a quantum safe organization. Different readiness literature streams were explored, technology readiness, organizational readiness and technology implementation literature. The latter provide the main basis for the model constructed.

The model divides the process into four phases, the initiation, adoption, implementation and post-implementation phase. Figure 24 gives an overview of the model.

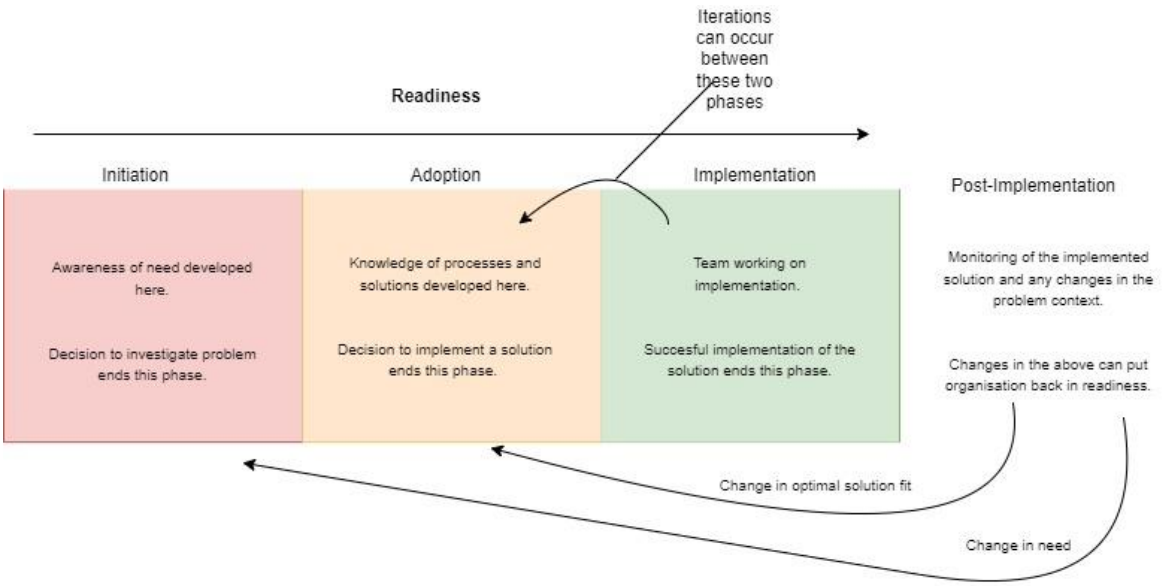

Figure 24: Adjusted readiness progress model

The model was adjusted as a result of the data collection part of the research, adding three important aspects:

Degree of R&D: The level of involvement in development of quantum safe technologies.

This is a measure to differentiate on the type of organization, which has implications for how they will deal with the quantum threat. Specifically, some organizations will not be able to develop quantum safe technologies themselves and are dependent on external parties for the development of the technology. This will mean they have to prioritize differently to an organization that can develop technologies in house.

Crypto agility: How easily an organizations IT systems can change underlying encryption.

This is an addition that is especially important for organizations with low degrees of R&D. They will need to be able to adapt their IT to technological solutions that external parties provide.

Iterative nature: The process of becoming ready in an organization is not linear, it involves different parts of the organization being at different stages, and iterations between attempted implementations and earlier phases.

The final model provides managers with a path towards becoming quantum safe, and it provides a framework for thinking about strategy. This sets up answering the third research question nicely, which is discussed next.

There are two main contributions to theory in regards to research question 2. The first is the clarification of the different readiness interpretations and what literature falls within each category. Then, there is the addition of bringing change process and technology implementation literature into the quantum threat context. This includes a number of very case specific factors, such as the three added just above.

6.5 Discussion research question 3

Now a discussion in the same structure as above, apart from one difference. That being that strategy was approached differently, there not being a separate literature part and the strategy implications coming out of the data collection part. As a reminder, the third research question was:

What strategy best fits the need and readiness of the organization?

Although there was not a dedicated literature part on strategy, different parts of the literature study still played a role in the formulation of the strategies. Firstly, the problem context chapter gave insights into characteristics of the quantum threat problem that have significant implications for the strategy. This is used as the starting point of the strategy implications section, and these characteristics come back in other places in the thesis, such as in the interviews.

Another part of the literature study that gave insight into strategy was the readiness literature. As was seen in the strategy implications part, the readiness model provided a good frame for thinking about strategy. Also, a lot of the milestones or actions described in the readiness model are quite related to strategy, it indicates what must be done to reach higher readiness.

Next to readiness providing a good frame for strategy, the need concept also proved to help in the thinking about strategy, in a different way to readiness as will be explained in a it. Together with interview and case results a number of strategy implications were formulated, first a distinction had to be made between external and internal strategy. This is an important distinction to make, but it turned out that they are quite linked to each other. This is often the case, but in this problem context even more so. The main reason for this was the fact that organizations are involved in a complex multi actor system, with whom they need to coordinate technical solutions to the quantum threat. This was considered where necessary, especially on the parts where external factors had impact on the internal strategy.

Internal strategy was the focus as that is what the need and readiness model lent itself to. The goal is to get the organization ready for the quantum threat, this is mostly an internal affair. Both models played a different role in how they influence strategy, need played a role in overall strategy that had affects over all phases of readiness. Readiness on the other hand zoomed in more, going into more details per phase. Using need as the starting point for strategy makes sense as this is influences the entire strategy, a manager first wants to know this before going into more detail on the strategy.

The readiness model lent itself well to discussing strategy per phase, as it implicitly defined strategic goals, them being how to get to the next phase. All that was then left was to fill in the strategies to reach the strategic goals. Initially, the idea of a matrix with need and readiness on both sides was the goal, however this turned out not to be the best way to illustrate the strategies. This because the strategy per readiness phases does not differ a lot if the organization has a different level or need. Need influences the level of priority given, the amount of resources to spend and which technology to choose. The steps that need to be taken in the different phases are not effected that much by it, just how those steps are taken. With which urgency, resources and technology. Instead they were looked at separately, and this worked quite well. A manager would now have to go through two steps to get their strategy, looking at both the need and the readiness strategy implications.

In the strategies per readiness phase the last two phases, implementation and post-implementation, did not have many useful insights. At this point the most important strategic choices have really been made, now it is a question of the technology being implemented practically.

6.6 Conclusion

In answering the third research question the main research question is also answered, as it is the last part of the three sub question the main research question is made up of. As a reminder the main research question was:

> *What strategies can be formulated from knowledge of an organizations need and readiness for quantum secure communication technology implementation?*

The need and readiness parts of this question were just discussed and answered above. This provides a good basis for strategy implications as mentioned in the discussion just had.

The strategy implications were divided into two aspects, internal and external strategy. The nature of the problem makes these two aspects closely related, as the problem is multi actor with many parties having to coordinate to come to shared solutions. This is the case for most organizations, as use the internet for a lot of their operations. The external impact had to be weighed appropriately when discussing internal strategy.

Internal strategy is the focus here, the need and readiness model lend themselves best for thinking about the internal strategy. The need and readiness model have different effects on the strategy, need impacts strategy in four ways:

> **Urgency:** How much priority the organization should give
>
> **Resources:** How many resources they should expend to advance readiness
>
> **Current communication**: Do current communication practices need to be adjusted due to the threat of store-now decrypt later.
>
> **Technology fit**: Which technological solution fits their organization best.

These aspects have an effect on strategy across all readiness phases. The readiness model gives strategies per phase, and are in that sense less general than the need implications on strategy, they are shorter term. Table 13 gives an overview.

Table 13: Overview of strategies per readiness phase

Initiation	Adoption	Implementation	Post-implementation
Understand need Understand complexity Involve people Learn from others Understand external dependence	Understand and develop crypto agility Inventorize operations Prioritize operations Collaborate	Plan for long process Manage iterative nature	Monitor changing technological context Monitor implemented solution

Next to the above implications the degree of R&D influences the strategy across all readiness phases. Higher degrees of R&D means an organization is more involved in testing and developing technologies themselves. Organizations with low levels of R&D need to prioritize crypto agility more, as they will need to implement externally developed technologies. The combination of need and readiness provides a manager with a useful tool to prepare themselves for the quantum threat. There are still aspects on which further research can be done to help mangers even more, these are discussed in further research.

The approach taken to strategy here is a theoretical contribution, as it uses the need and readiness models as a frame for strategic thinking. Beginning with need is a useful way to do this, as it gives a clear understanding of general strategy. Following this the use of readiness helps in splitting strategy up in phases, even though the strategies described per phase do not strictly only have be used in each phase. It allows for prioritization depending on how far in the process the organization is.

6.7 Managerial implications

Although often intuitively understood, the work here gives a more structured outlook on what need is. A manager can then more precisely estimate their organizations need, and pinpoint more accurately which operations in the organization are most vulnerable. Not only does the manager then have a good understanding of need, they already have the first indication of where to focus efforts.

The need model in the thesis is still limited mostly to theory, a way to measure all the components of the model has not been devised. This means a manager has to either devise a way to do this within their organization, or look for further research on the topic. Often, a manager is in a good position to devise their own way of measuring the components within their organization. Even without accurate measurement, the model provides a frame for thinking about the problem and can aid a manager in estimating where the organization is at. Next to this, it provides useful insights in thinking about strategy. The thesis gives a number of strategy implications from this perspective, a good starting point for a manager to develop the strategy that fits their organization best.

The work then continues by looking at readiness, the process of becoming a quantum safe organization. This helps a manager by giving an overview of the process, and allows the manager to pinpoint where their organization is in the process. This can be done by looking at the milestones defined in the model. Importantly the manager must be aware of the iterative nature of the model, although it is linearly structured the real life process rarely only goes linearly. The model also adds an important influencing factor managers must be aware of, the degree of R&D. This variable indicates the level of involvement of the organization in the development of quantum safe technologies. An organization that does not have any capability to develop these technologies internally needs to prepare for the difficulty of integrating externally developed products. One way this can be done is by prioritizing crypto agility. The readiness process for an organization with a high degree of R&D is different in a number of ways. The amount of resources to be invested is much higher, and the process is likely much longer.

With these two tools at hand a manager is now in a position to formulate an effective strategy for their organization. This is done by first determining the best general strategy according to need. This influences the amount of resources to allocate, but also what type of solution to go for. Once this is known the manager can look more into the details of the strategy by using the phases of the

readiness model. This allows them to prioritize certain strategies depending on where the organization is in the process.

Also, from the results it was apparent that a wait and see strategy is being adopted by certain organizations. This is a strategy managers have to be careful of for a number of reasons, the main one being that integrated externally made quantum safe products could be more difficult than expected. It is wise for managers to at least have a good understanding of how difficult such integrating would be before adopting such a wait and see strategy. In most cases, it would be even better to take a more proactive approach.

6.8 Limitations

The research conducted here is quite exploratory and general in nature. It builds theory by constructing models around need and readiness. As the focus was on this, there was less space for operationalization and validation of the models in real situations. This is a limitation of the research, the models have been argued for from literature and own contribution, with validation from only three cases. This makes it non generalizable, and keeps it limited to theory contribution mainly.

The need model developed here suffers from this limitation, in its current form it is not very practically applicable. The three need categorizations given here are not super reliable since they could not make use of an effectively operationalized need model. A proposal for research on an operationalized need model is suggested in further research.

The next limitation is that the research focuses mainly on one stream of readiness, readiness progress. The other aspect of readiness, readiness adaptability, is also very important to understand for managers. For that reason a proposal for further research on this topic is given in the further research section. Another limitation is the small sample of cases. This makes any insights found not statistically relevant. Nonetheless it provides evidence of some potentially interesting findings, such as the discrepancy between need and readiness in organizations. Also this could be an interesting area of further research.

6.9 Further research

Throughout the thesis a number of ideas for further research where already alluded to, here they are recapped. A number of the further research suggestions come from the fact that the thesis here took quite a wide scope, limiting research into details in some areas.

6.9.1 Need model

The need model developed here is theoretical and has not been applied to an organization. Interesting further research would involve applying the model to organizations to get more detailed analysis of the need of an organization. The goal of such further research would be to develop a method to accurately measure the need of an organization. This would be done by operationalizing the need model and testing it with real organizations. Potential formulations of the research questions are:

> Main research question: *How can an organizations need for quantum safe technology be measured?*
>
> Sub research question 1: *How can the need model be operationalized?*
>
> Sub research question 2: *How accurately does the model measure an organizations need?*

Here a first shot is given at what to consider in operationalizing the need model. As a reminder Figure 25 is given below.

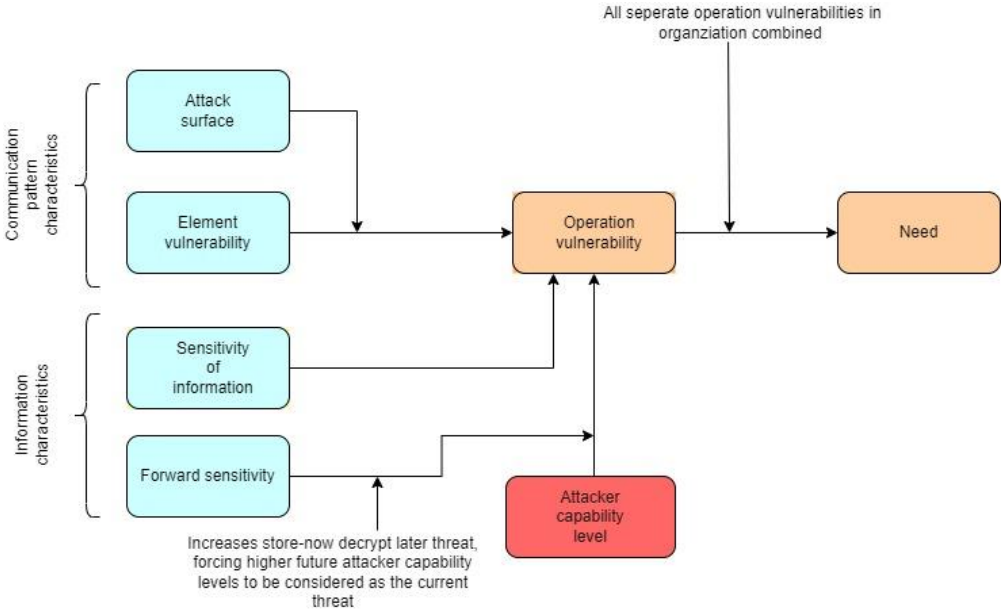

Figure 25: Final need model

To begin with the communication pattern characteristics of an organization have to be analysed. Doing this involves going into the details of the applications that are being run in the organization, and would have to be done with a good understanding of computer science. It would involve a step by step process where the following need to be taken:

1. All operations (or applications) need to be identified and inventorized. An application could for instance be an inventory control system or accounting software.

2. Per application an attack surface analysis needs to be done. This is done by analysing the source code and identifying all points of entry and exit(in the model referred to as elements). These points can be a range of things such as login entry points, admin interfaces, data entry forms and many other points.

3. Once the attack surface has been mapped the vulnerability of the elements on the attack surface has to be assessed. In the context of the quantum threat this involves looking at the encryption underlying the element. All elements involving asymmetric encryption are vulnerable, certain symmetric encryption as well.

This is a general description of the steps, a way to quantify the attack surface and its vulnerabilities would add usefulness. This could allow for comparison between organizations and make the assessment more useful. Quantifying could be done by counting the amount of entry points, and having a rating of the vulnerability of each element, depending on the security level of the underlying encryption.

The second part of the operationalization of the need model is more subjective. The information characteristics of all the operations in the organization need to be analysed. The criteria from Table 5 given in section 3.3 form the basis for need model assessment questions that a manager must answer. This assessment requires estimating the impact data leakage would have on the organization. Assessing the forward sensitivity would involve a similar subjective assessment.

Having developed a method to apply the need model it would then be interesting to use it to collect data on organizations. This can have two goals, to test and validate the method developed and to compare the need of different organizations.

6.9.2 Readiness adaptability

The concept of readiness was split up into two aspects in this thesis; readiness progress and readiness adaptability. The first was the focus here, leaving readiness adaptability largely uninvestigated. As a reminder readiness adaptability is defined as:

> **Readiness adaptability**: Capacity to implement quantum safe communication technology.

This looks at the characteristics of an organization that make it able to implement quantum safe communication technologies effectively. As opposed to how far they are in the process of implementing the technology as studied in this work. An example of such a characteristic is the absorptive capacity of an organization. A higher absorptive capacity would lead to easier integration of technological innovations, such as quantum safe technologies.

In further research this concept can be explored, the research questions can be something like:

> Main research question: *What determines the readiness adaptability of an organization for quantum safe communication technology?*
>
> Sub research question 1: *What are the factors that determine readiness adaptability of an organization for quantum safe communication technology?*
>
> Sub research question 2: *How do these factors affect readiness adaptability?*

Some of the literature concerning this concept has already been explored in the organizational readiness section 4.2.3. Organizational readiness as defined in literature is much in line with readiness adaptability defined her, this is explained in more detail in section 4.2. Section 4.2.3 outlines the different streams within organizational readiness, distinguishing between the psychological and structural approach. In that section it is also explained that the structural approach is more relevant for the quantum threat.

The structural approach also consist of various sub concepts, as can be seen in Figure 18. These sub concepts are the kinds of characteristics that would need to be investigated to get a sense of the organizational readiness of an organization. For instance, financial readiness will give an indication whether an organization has the financial resources required to successfully implement quantum safe technologies. The research would require weighing the different sub readiness constructs, to get a sense of what is important in making an organization able to implement quantum safe technology effectively.

Here some example questions of what to consider in determining financial and staffing readiness of an organization:

Financial readiness:

- What is the allocated budget at this moment?
- How does the organizations need affect how much to invest?
- What budget would be needed?

Staffing readiness:

- Does the organization have the right talent?
- Does the organization have enough staff?
- Does the staff need to be trained?

Next to these two readiness sub types there are also others such as process and operations readiness, cultural readiness and business readiness.

A potentially interesting link could be made to the readiness phases outlined in the work here. Possibly sub readiness constructs weigh differently in terms of importance during different phases. For instance, staffing readiness may not weigh that heavily yet in the initiation phase. It would become more important in the implementation phase. Such research would provide managers with even more detail of the readiness of their organization, allowing them to make more targeted decision of where to improve readiness.

6.9.3 Other

Next to these two main further research topics there are two more areas of potentially interesting research. These are not as closely related to the research that was done here, but did come up in the work. As they are less closely related less relevant insight came out of the thesis as to how to set-up these two areas of further research. For that reason, they are only dealt with in brief here. The first of these has to do with the degree of R&D concept and Pavitt's taxonomy. The second suggested further research concerns the use of the models in a cross organization analysis to identify statistically relevant trends in need and readiness.

Degree of R&D

As a reminder, the degree of R&D is defined as:

> **Degree of R&D:** The level of involvement in development of quantum safe technologies.

This aspect has impact on how able an organization is to integrate quantum safe technologies into their organization, for both internally and externally developed technologies. This idea is related to the concepts discussed in Pavitt's taxonomy (Pavitt,1984). This taxonomy was focused on manufacturing industries, in the thesis here it was shown that similar taxonomies play a role in IT aspects of organizations as well. This can be investigated much more extensively, giving insights in how different types of organizations implement IT innovations.

Statistically relevant analysis:

The final suggested further research involves a different application of the need and readiness models. They can form the basis of a cross organizational study to see where organizations fall in need and readiness. This could give insights into trends around the quantum threat, how need is distributed among organizations and how ready they then are. Although not conclusive evidence, the organizations investigated here showed to have high need and relatively low levels of readiness. If proven for a larger data set this would have significant implications.

Doing this would involve operationalizing the models in a way that data can be collected in a consistent manner from many organizations, the research would likely be interview or survey intensive.

6.10 Reflection

The thesis process was a challenge in a fashion I had not encountered before. It is a unique challenge as you chose your own area of interest, look for what has not been researched on the subject and dive into the unknown. In the beginning this caused me to be lost in the possible directions you could go in. You have a goal in mind in the beginning but quickly you start seeing so many issue with what you had in mind in the first place. Before you know it you are completely lost and do not know where to start anymore. This is the point where patience and perseverance are key, and where the help of an involved mentor helps tremendously. This part of the process was a good learning experience. Here I was surprised at my creative abilities in thinking of new models for a complex problem, but I also learnt that I need to improve decisiveness and remaining focused on the most important goals.

After getting though that part of the process the next is more characterised by time pressure and feeling overwhelmed by how much needs to be done. So much so that postponement of the deadlines was necessary. Given the ambitious planning this was not a huge surprise, it also allowed for the final product to be less rushed. In the end I feel satisfied with the models I was able to create, but less satisfied with how I communicated my findings. I found it difficult to put the ideas that are clear in my head on paper, especially as the thesis document got longer and longer. Nonetheless I learnt a lot in this regard, especially when trying to improve the communication of my results after my greenlight meeting.

Overall it was a unique opportunity to have half a year to spend on your own research, and a very learn some experience.

-

7 Bibliography

1. Bement, A. L. (2004). *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems*.

2. Dekker, M. (2022, March). *Why All CISOs Need to Prioritize Quantum Tech Today*. FS-ISAC.

3. Dyakonov, M. (2019). When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing. *IEEE Spectrum*, *56*(3), 24–29. https://doi.org/10.1109/MSPEC.2019.8651931

4. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96*, 212–219. https://doi.org/10.1145/237814.237866

5. Howard, M., Pincus, J., & Wing, J. M. (2005). Measuring Relative Attack Surfaces. In *Computer Security in the 21st Century* (pp. 109–137). Springer-Verlag. https://doi.org/10.1007/0-387-24006-3_8

6. Innovatie Spotter. (2020, October 6). *Opkomst van dark fiber in Nederland*. Innovatie Spotter.

7. Intellipaat. (2022, April). *What is the CIA triad?* Intellipaat.

8. Jeran Renz. (2021). Kerberos protocol. In *Creative Commons*.

9. K, J. (2014). *Sai Om Journal of Commerce & Management CONSUMER BEHAVIOUR MODELS: AN OVERVIEW* (Vol. 1, Issue 5). www.saiompublications.com

10. Karit, Z. (2016). *Applying Encryption Algorithms for Data Security in Cloud Storage, Kartit, et al"*.

11. Lai S, V., & Mahapatra, R. K. (1997). Exploring the research in information technology implementation. *Information & Management*, *32*(4), 187–201. https://doi.org/10.1016/S0378-7206(97)00022-0

12. Lehman, W. E. K., Greener, J. M., & Simpson, D. D. (2002). Assessing organizational readiness for change. *Journal of Substance Abuse Treatment*, *22*(4), 197–209. https://doi.org/10.1016/S0740-5472(02)00233-7

13. Leigh, D., Watkins, R., Platt, W., & Kaufman, R. (2000). Alternate models of needs assesment: Selecting the right one for your organization. *Human Resource Development Quarterly*, *11*(1), 87–93.

14. Lunenburg, F. C. (2010). Approaches to Managing Organizational Change. In *INTERNATIONAL JOURNAL OF SCHOLARLY ACADEMIC INTELLECTUAL DIVERSITY* (Vol. 12).

15. Manadhata, P. K., & Wing, J. M. (2011). *A Formal Model for a System's Attack Surface* (pp. 1–28). https://doi.org/10.1007/978-1-4614-0977-9_1

16. Mankins, J. C. (2009). Technology readiness assessments: A retrospective. *Acta Astronautica*, *65*(9–10), 1216–1223. https://doi.org/10.1016/j.actaastro.2009.03.058

17. Mankins, J. C. (1995). *TECHNOLOGY READINESS LEVELS A White Paper*.

18. Mashatan, A., & Heintzman, D. (2021). The Complex Path to Quantum Resistance. *Queue*, *19*(2), 65–92. https://doi.org/10.1145/3466132.3466779

19. Matt Swayne. (2021, May 10). TQD Exclusive: Quantum Delta NL Plans to Put 615 Million Euro Investment in Quantum to Good Use. *The Quantum Insider*.

20. Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., & Voznak, M. (2020). Quantum Key Distribution. *ACM Computing Surveys*, *53*(5), 1–41. https://doi.org/10.1145/3402192

21. Muller, F., & van Heesch, M. (2020). Migration to Quantum-Safe Cryptography. *TNO Position Papaer*.

22. Nguyen, P. Q. (2017). Quantum-safe cryptography. *ASM Science Journal*, 41–42.

23. NIST. (2020, July 22). *PQC Standardization Process: Third Round Candidate Announcement*.

24. Ortt, R., van Veen, B., van der Burg, S., & ter Haar, M. (2022). *How to create a quantum safe internet and beyond?*

25. Parker, D. B. (1998). *Fighting Computer Crime*. John Wiley & Sons.

26. Pavitt, K. (1984). Sectoral patterns of technical change: Towards a taxonomy and a theory. *Research Policy*, *13*(6), 343–373. https://doi.org/10.1016/0048-7333(84)90018-0

27. QED-C. (2021). *A Guide to a Quantum-Safe Organization Transitioning from today's cybersecurity to a quantum-resilient environment*.

28. Qutech. (2019, June). *Quantum technology for secure banking: QuTech teams up with ABN AMRO*. Qutech.

29. Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations*. https://doi.org/10.6028/NIST.SP.800-171r2

30. Scheirer, M. A. (1983). APPROACHES TO THE STUDY OF IMPLEMENTATION. *IEEE Transactions on Engineering Management*, *EM-30*(2), 76–82. https://doi.org/10.1109/TEM.1983.6447505

31. Schwenk, J., & Stebila, D. (2019). *A Reduction-Based Proof for Authentication and Session Key Security in 3-Party Kerberos*.

32. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700

33. Stallings, W. (1990). *Cryptography and Network Security: Principles and Practice.* . Prentice Hall.

34. Stam, B. (2020). *Comparative case study into the barriers that prevent QKD and Tokamak nuclear fusion power plants from large scale diffusion MSc Management of Technology*.

35. Thompson, V. A. (1965). Bureaucracy and Innovation. In *Quarterly* (Vol. 10, Issue 1).

36. Toekomstbeeld Der Techniek, S., & Ortt, R. (2021). *Commissioned by The Netherlands Study Centre for Technology Trends Quantum Technology*. www.stt.nl

37. van Ingen, R., Peters, P., de Ruiter, M., & Robben, H. (2021). Exploring the Meaning of Organizational Purpose at a New Dawn: The Development of a Conceptual Model Through Expert Interviews. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.675543

38. Vashistha, B., Panwar, N., Reddy, R. N., & Jabeena, A. (2014). *Implementation of Spread-Spectrum Techniques in Optical Comunication* (Vol. 9, Issue 3). Ver. III. www.iosrjournals.orgwww.iosrjournals.org44|

39. Weiner, B. J. (2009). A theory of organizational readiness for change. *Implementation Science*, *4*(1), 67. https://doi.org/10.1186/1748-5908-4-67

40. Yin, K. (2012). *Case Study Research* (3rd ed.). Sage.

41. Yoon, A. (2019). *Organizational Readiness for Machine Learning Exploring the key readiness factors for business adoption of machine learning*.

8 Appendix

8.1 Appendix A: Interview Achmea

Interview Centraal Beheer Achmea

Interviewee information:

- Paul Geurts
- Function: Manager IT security and data governance.

Opening:

- Bedankt voor het meewerken
- Introductie
- Scritpie management of technology
- Kijk naar het effect van de kwantum dreiging op organizaties. Iets meer uitleggen…
- Ik wil uitzoek in hoe vere organizaties hier al mee bezig zijn, en wat voor een strategie ze het beste kunnen toe passen.
- Ik zou graag het interview opnemen, ik ga ook mijn scherm delen zodat we samen door de vragen heen kunnen.
- Het interview is een half uur

Start screen share

Introductie

Het interview is opgedeeld in twee delen, een gaat over readiness en de ander over strategieën. Eerst een openings vraag:

1. U bent manager IT security and data governance. Wat houdt deze functie in?

- Technische afdeling van de informatie beveiliging
    - Zit een defence centre team onder mij:
        - Die doen monitoring van cyber security, en incident response als nodig
    - Ethical hacking team:
        - Die testen eigen omgeving en van derden die zij gebruiken
    - Security scanning and enginering team:
        - Zit vulnerability scanning in
        - Zorgen dat techniek beschikbaar is voor security teams
    - Data governenance is ook een onderdeel:
        - Van heel Achmea
        - Ook zorgen dat alle accounting data veilig is
        - Data policy ook, om te zorgen dat al je dat op orde is(ook volgens de wet)
        - Behoorlijk lastig vakgebied

Readiness vragen

Readiness: De mate waarin een organisatie kwantum veilig is.

In het model wat ik heb ontwikkeld kan een organisatie in vier fases zijn met betrekking tot readiness. Die zijn:

Initiatie: De organisatie wordt bewust dat er een kwantum dreiging is en dat dit mogelijk effect heeft op de organisatie.

Adaptatie: De organisatie zoekt actief uit wat de mogelijk oplossingen zijn en welke het beste past.

Implementatie: De organisatie heeft een oplossing gekozen en is actief het aan het implementeren.

Post-implementatie: De organisatie heeft een oplossing geïmplementeerd en let op ontwikkelingen die een andere oplossing zou vragen.

2. Waar zou u Centraal Beheer Achmea momenteel plaatsen en waarom?

Initiaitie:

- Zijn ons bewust van kwantum dreiging, hebben door dat op termijn dit onze encryptie onveilig maakt.
    - Crux zit in op termijn, wanneer dan?
- Wij hebben nog geen termijn voor ons zelf gedefinieerd, zijn dus eigenlijk bewust maar doen er nog niks mee.
- Wij passen ook alleen technologie toe, wij gaan nooit onze eigen kwantum afdeling maken.

Ik vraag door over store-now-decrypt later:

- Daar zijn we nog niet mee bezig
- Variant die jij noemt hebben we nog niet gehoord

3. Is top management bewust van het probleem?

- Zijn er van bewust
- CIO redelijk dicht bij RVB
    - Hij is er van bewust, maar weet ook niet wat te doen.
    - Ook initiatie
- Martijn van ABN, heeft een heel team op quantum, en 500 mensen onder hem. Ik heb er 12, is een andere orde van grote.
    - Banken zitten ook in de kritieke infrastructuur, dus andere rol.

Ik vraag door: Maar hoe zie je de behoeft voor beveiliging dan, bijvoorbeeld vergeleken met een bank?

- Persoon gegevens en medische gegevens zijn gevoelig.
- Er is in ieder geval genoeg gevoelige informatie om het op een up to date manier te encrypten.
- Soms zelfs meer bijzondere gegevens dan banken, als je kijkt naar ziekte en levens verzekeraars.

Ik vraag door: Zouden de prioriteiten niet meer zoals die van de banken moeten zijn?

- Nogmaals, de vraag is wanneer gaat het impact hebben?
    - Hebben we overigens niet een heel goed antwoord op voor onszelf…

Is ook het lastige aan het probleem, en aan de andere kant heb je ook dat migreren heel lang duurt:

- Maar wij passen technologie toe, niet ontwikkelen of bedenken.
- Op het moment dat het beschikbaar komt gaan we het echt wel gebruiken.

Software en applicaties worden vooral extern gekocht?

- Ja meestal wel, soms zelf gemaakt.
- Encryptie gaan we niet zelf maken, kopen we gewoon commerciële producten voor.
-

    a. In welke mate?

    b. Zo niet, wie wel?

4. Wordt er intern onderzoek gedaan naar het probleem?

5. Wordt er met andere partijen samengewerkt op dit vlak?

6. Is er een team verantwoordelijk/ bezig met dit probleem?

7. Worden er test/ pilots gedaan met PQC algoritmes, QKD of andere kwantum veilige communicatie vormen?

8.2 Appendix B: Interview Het Kadaster

This interviewee asked not to be recorded, so the answers to the question were mainly filled in right after the interview in the summary report in the main body of text.

Interview Het Kadaster

Interviewee information:

- Andrei Klein, CISO

Opening:

- Bedankt voor het meewerken
- Introductie
- Scritpie management of technology
- Kijk naar het effect van de kwantum dreiging op organizaties. Iets meer uitleggen…
- Ik wil uitzoek in hoe vere organizaties hier al mee bezig zijn, en wat voor een strategie ze het beste kunnen toe passen.
- Ik zou graag het interview opnemen, ik ga ook mijn scherm delen zodat we samen door de vragen heen kunnen.
- Het interview is een half uur

Start screen share

Introductie

Het interview is opgedeeld in twee delen, een gaat over readiness en de ander over strategieën. Eerst wat openings vragen:

1. Wat weten jullie over de quantum dreiging?
- Genoeg, we weten dat er neiwue beschermings middelen nodig zijn.

2. Hoe gevoelig is de data die het Kadaster hanteert?
- Wettelijk openbare taak, informatie is in principe openbaar
- Zoek sleutel en zoek ingang altijd de kaart is en niet de persoon, je izet niet wie der woont, het gaat alleen om eigendom.
- Als iemand onze database zou hebben zouden ze wel op persoon kunnen zoeken.
- Het gaat om de zoek functie, je kan allen op adres zoeken.

Readiness vragen

Readiness: De mate waarin een organisatie kwantum veilig is.

In het model wat ik heb ontwikkeld kan een organisatie in vier fases zijn met betrekking tot readiness. Die zijn:

Initiatie: De organisatie wordt bewust dat er een kwantum dreiging is en dat dit mogelijk effect heeft op de organisatie.

Adaptatie: De organisatie zoekt actief uit wat de mogelijk oplossingen zijn en welke het beste past.

Implementatie: De organisatie heeft een oplossing gekozen en is actief het aan het implementeren.

Post-implementatie: De organisatie heeft een oplossing geïmplementeerd en let op ontwikkelingen die een andere oplossing zou vragen.

8. Waar zou u het Kadaster momenteel plaatsen en waarom?

- We weten nog niet hoe het precies gaat werken de quantum dreiging.
- Er zijn staten die alle communicatie vast zetten, store now decrypt later.
    - Als je dit niet hebt, dan moet de organisatie hier aan denken.
- Migratie process:
    - Omdat wij standard producten gebruiken implementeren we die
- Zelfstandig bestuursorgaan, kan kiezen tussen zelfstandig en overheid beleid.
- Wij zijn niet proactief hierin, hebben we de middelen niet voor.

9. Is top management bewust van het probleem?

    a. In welke mate?

    b. Zo niet, wie wel?

10. Wordt er intern onderzoek gedaan naar het probleem?

11. Wordt er met andere partijen samengewerkt op dit vlak?

12. Is er een team verantwoordelijk/ bezig met dit probleem?

13. Worden er test/ pilots gedaan met PQC algoritmes, QKD of andere kwantum veilige communicatie vormen?

Strategie vragen

Strategie in deze thesis: Lange termijn plan van aanpak met betrekking tot de kwantum dreiging

14. Heeft het Kadaster een strategie geformuleerd die specifiek met de kwantum dreiging te maken heeft?

15. Wat heeft of zou het Kadaster doen om tot de juiste technologische oplossing te komen voor het bedrijf?

16. Hoe ziet het Kadaster de rol van samenwerking met andere partijen in strategie met betrekking tot de kwantum dreiging?

17. Hoe lastig verwacht het Kadaster dat implementatie van kwantum veilige technologieën gaat zijn?

Stop screen share

Afsluiting

- Heel erg bedankt uw tijd en het meewerken aan het interview

Strategie vragen

Strategie in deze thesis: Lange termijn plan van aanpak met betrekking tot de kwantum dreiging

18. Heeft Centraal Beheer Achmea een strategie geformuleerd die specifiek met de kwantum dreiging te maken heeft?

Schot voor de boeg, wat zou de aanpak zijn?

- Denk dat we het niet zo goed weten
- Jij noemde net termen die ik niet kon plaatsen, dus we weten nog vrij weinig lijkt me.
- Pas als het in commerciële producten beschikbaar is gaan wij het gebruiken

Waar kijken jullie dan naar, overheid, grote tech bedrijven?

- Zie niks vanuit de overheid…
- Misschien gezamenlijk onderzoek(met banken en andere verzekeraars) vanuit een TNO bijvoorbeeld. Daar zouden we naar kijken.

Algemeen strategie met cyber vraag.

- Dat is wel erg breed
- Maar ik zal in algemene termene beantworden.
    - Zitten in de kop van het peleton, niet in de kop groep maar wel vooran in het peleton.
    - Willen bijblijven, up to date zijn
- Da tweet een architect in het team, wat de huidige standaard is.
- Die standaar wordt een keer per jaar vastgesteld, en dan zorgen we dat alles binnen het bedrijf daar weer aan voldoet.

Dus eigenlijk een volg wat de rest doet strategie?

- Negatieve manier om hetzelfde te zeggen.

19. Wat heeft of zou Centraal Beheer Achmea doen om tot de juiste technologische oplossing te komen voor het bedrijf?

20. Hoe ziet Centraal Beheer Achmea de rol van samenwerking met andere partijen in strategie met betrekking tot de kwantum dreiging?

Stop screen share

Afsluiting

- Weet u toevallig andere relevante informatie die relevant zou kunnen zijn voor mij?
- Heeft u misschien tips van mensen in andere bedrijven die ik hierover zou kunnen interviewen?
- Heel erg bedankt uw tijd en het meewerken aan het interview