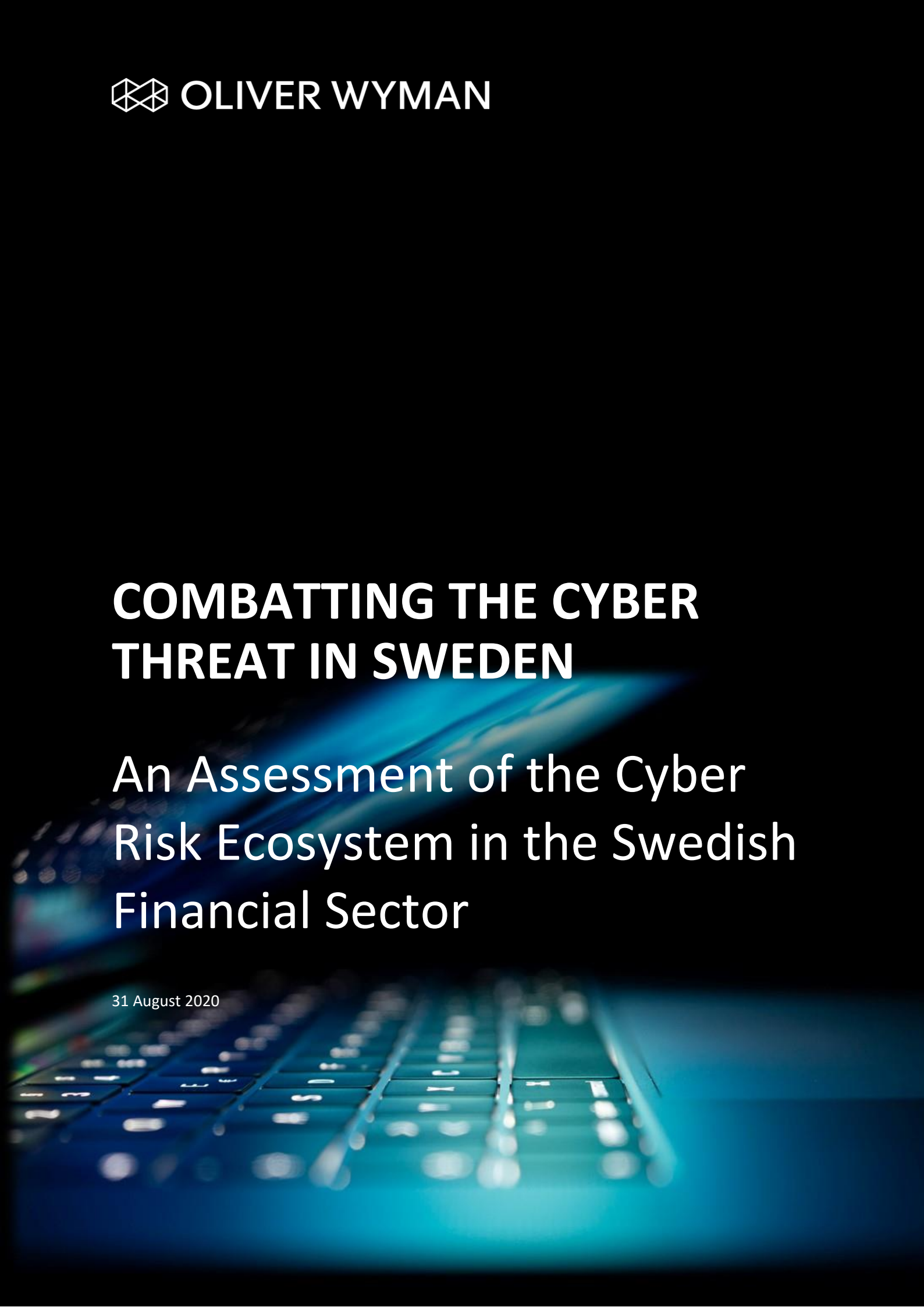
OLIVER WYMAN

COMBATTING THE CYBER THREAT IN SWEDEN

An Assessment of the Cyber Risk Ecosystem in the Swedish Financial Sector

31 August 2020



CONFIDENTIALITY

Our clients' industries are extremely competitive, and the maintenance of confidentiality with respect to our clients' plans and data is critical. Oliver Wyman rigorously applies internal confidentiality practices to protect the confidentiality of all client information.

Similarly, our industry is very competitive. We view our approaches and insights as proprietary and therefore look to our clients to protect our interests in our proposals, presentations, methodologies, and analytical techniques. Under no circumstances should this material be shared with any third party without the prior written consent of Oliver Wyman.

CONTENTS

1. INTRODUCTION

Executives rank cyber threats as the number one risk to their organisations. As many as 80% of executives consider cyber threats to be among the five most important risks they face. [1] This concern is warranted. Cyber-attacks continue to rise in volume and sophistication, are increasingly executed by state-sponsored actors, and the resulting losses tend to be significant. These types of attacks have wide-spread consequences, especially when they are perpetrated by antagonistic state-affiliated actors with the purpose of either espionage or with an explicit aim to cause panic and disturbance in another country.

This report has been written by Oliver Wyman for Finansinspektionen (the Swedish FSA) to summarise, evaluate, and provide an external perspective on the Swedish ecosystem around cyber risk in the financial sector. This encompasses an assessment of how greater collaboration can be established between the private and public spheres in order to protect Sweden's financial stability. The report draws upon experiences from other jurisdictions and sectors, as well as input from a wide range of interviews conducted across various authorities, private banks, insurers and market infrastructure providers. These insights are then leveraged to craft an understanding of the potential future role that Finansinspektionen might take in the Swedish ecosystem.

1.1. Definition and problem statement

When the industry refers to "cyber risk" a variety of scopes and definitions can be implied. For the purposes of this report, we focus on the risk arising from conscious and antagonistic actions directed at IT infrastructure, critical processes or employees in companies or authorities, with the aim of accessing information or financial funds, modifying data or rendering information unavailable. Finansinspektionen considers three types of cyber risk in its supervision:

- Attacks directed towards financial institutions' digital retail channels (for instance online banking or mobile banking)
- Denial of Service (DoS) attacks with the aim of temporarily rendering institutions' digital channels and/or backend systems inoperable
- Intrusion in financial institutions' IT systems for the purpose of fraud, blackmail, espionage or sabotage

The definition of cyber risk and cyber security may in some cases also include risk that is not antagonistic, for example risk arising from hardware, software, data and user errors related to technological infrastructure. When we in this report refer to cyber risk, we opt to define it solely as risk caused by a malicious actor or where a malicious actor is the catalyst of the risk being realised. Malicious actors may be external (for instance a hacker) or internal (data leaks from employees). IT-related risk that is not driven by a malicious actor is in this report referred to as operational IT risk to avoid confusion. While not the explicit focus of this paper, some of the below recommendations on cyber risk may also contribute to improving the ecosystem's capabilities to prevent operational resilience risks from being realised. One such example is that more extensive and formalised information sharing could be used to spread awareness of general IT issues and security holes that may impact more than one ecosystem player.

For a long time, cyber risk had mainly been considered an operational risk specific to internal IT security, namely as the risk of doing business through an internet connection or using IT software. This was mainly a problem that concerned each individual financial institution. However, as technological development has progressed, the breadth of cyber risk has grown. It has become

[1] Marsh (2019) – Global Cyber Risk Perception Survey Report 2019

increasingly apparent that cyber risk often is inextricably linked to the individual firm's employees, suppliers, infrastructure providers, counterparties and customers. For example, the International Monetary Fund (IMF), as part of its work on cyber risk surveillance, has illustrated how risk aggregation goes beyond the boundaries of each firm, and that many sources of cyber risk are outside the control of the firm, no matter how many controls and resilience measures are put in place.[2]

Cyber risk can, for instance, stem from disruptions in electricity, telecommunications or in the financial market infrastructure, which in turn creates risks for the financial sector. Furthermore, cyber attacks are more likely to happen following external shocks, whether they are natural disasters, wars or a global pandemic. Indeed, the Oliver Wyman Forum noted that the on-going COVID-19 pandemic[3] has resulted in an uptick in both e-mail scams and more high-profile cyber-attacks. The WHO reports a fivefold increase in cyber-attacks in April 2020, compared to at the start of the COVID-19 pandemic.[4] With more employees working remotely, cyber security and IT teams are subject to higher demands and more stress than ever before, creating opportunities for malevolent actors to capitalize upon.

This leaves us with an interesting question: if we agree that a significant portion of cyber risk is beyond the control of each individual firm, who is then accountable for ensuring that the risk does not materialise? Finansinspektionen is responsible for supervising financial firms and following up on implementations of controls for the risks that can be controlled by each firm. However, to what extent is Finansinspektionen also responsible for cyber risk that is shared by all actors within the whole financial sector? What considerations should be made for third parties which are not under Finansinspektionen's direct supervision but still play an important role in the financial ecosystem? What would this imply for other authorities and actors? These are all questions which we aim delineate and answer in this paper.

1.2. Why is cyber risk important?

There is growing consensus of the importance of cyber risk. In one of their latest stability reports, Sweden's central bank Riksbanken states that cyber risk has become one of the greatest threats to the modern international financial system.[5] The Danish FSA has deemed the threat level from cyber risk to be "very high".[6] The IMF states that cyber risk is a significant threat to global financial stability.[7]

This raises several important questions regarding cyber risk in the financial system and how Finansinspektionen should address it. The much-reported Wannacry ransomware (a type of attack that locks the victim's computer until a ransom is paid) infected both major banks and the central bank in Russia in 2017, as well as put ATMs out of service. Just one month later, the NotPetya malware hit the Ukrainian banking sector and rendered both ATMs and payment terminals around the country inoperable. It should be noted that these attacks were not limited to organisations active in financial services and had a wide impact across a multitude of industries.

The nature of cyber attacks has evolved at speed. The perpetrators are often no longer "script kiddies" or bored "hacktivists". According to a Verizon report, more than 30% of all breaches in 2018 were carried out by state actors. Just eight years prior, in 2010, virtually no data breaches could be

[2] IMF (2017), Cyber Risk, Market Failures and Financial Stability

[3] On-going at the time of writing in 2020

[4] WHO (2020), WHO reports fivefold increase in cyber attacks, urges vigilance

[5] Riksbanken (2019), Financial Stability Report 2019:2

[6] Finanstilsynet (2019), Strategi for den finansielle saktors cyber- og informationssikkerhed 2019-2021

[7] IMF(2018), Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

attributed to state actors.[8] The US Intelligence Community estimates that there are now more than thirty countries with "military-grade destructive attack capability".[9] Moreover, it concluded that the financial sector would be a prime target in the case that nations openly engage in cyber-warfare. By attacking the financial system, destruction and disruption of vital functions could be achieved, potentially resulting in widespread panic.

Finally, cyber risk is associated with enormous costs. The IMF estimates that losses from cyber attacks could be up to 30 percent of net revenues in the financial sector.[10] The Institute of International Finance (IIF) calculated in 2017 that cyber attacks cost the financial sector 400 billion US dollars in 2015 and that the costs will increase to 6 trillion US dollars by 2021.[11] Similarly, Lloyd's of London has estimated that the cost of a single global cyber attack could be as high as 121 billion US dollars for an extreme cloud service disruption event.[12] Given the complexity of cyber risk prevention, there exists a delicate balancing act between reducing the risk of these large-impact events and the substantial internal operational costs involved with maintaining appropriate control. This is further complicated by the fact that cyber risk is currently difficult to insure as it is challenging to parametrise.

At the same time as cyber threats to financial stability are increasing, the sector is undergoing significant change. FinTech firms are disrupting the industry, introducing more competition and innovation. This is driving efficiency gains that could support the overall financial stability. However, FinTech firms are likely to not be as prepared to defend themselves against cyber attacks by not having large cyber teams as the more established financial institutions, and their approach to market entry is often associated with greater risk taking. In addition, many FinTechs take advantage of recent regulatory initiatives to make the financial sector more integrated (for instance leveraging the PSD2 payment directive). Such integration drives higher risk concentration in the sector and may increase the likelihood of cyber risk to become systemic. As such, FinTechs and other smaller firms that have potential to still be systemically important could have significant negative impact on financial stability in Sweden. On the other hand, incumbent firms tend to have complex and cumbersome legacy IT systems, which present their own cyber risk. The illustration below highlights the types of firms that may have the greatest negative impact on financial stability in Sweden following a cyber attack, and that could be attractive targets for malicious actors.

[8] Verizon (2019), Data Breach Investigations Report

[9] US Senate (2017), Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States

[10] IMF(2018), Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

[11] IIF (2017), Cyber Security & Financial Stability

[12] https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report

Figure 1: Financial firms vulnerable to cyber risk

Participants	Importance to financial stability	Attractiveness for malicious actors	Comments
Nordic banks	**High**	**High**	• Banks typically present an attractive entry point for malicious actors • Concentration in small number of players drives high importance to financial stability
Payment providers	**High**	**High**	• Due to the direct impact on consumers and the fairly high degree of concentration, an attack on payment providers could cause loss of confidence in the financial system • With cash payments increasingly being phased out in Sweden, an attack on payment providers could have systemic impact due to the lack of substitutability
Market infrastructure providers (exchanges, central counterparties, trade repositories, clearing houses)	**High**	Medium to **High**	• The potential impact on financial stability of an attack on market infrastructure providers is vast, as these firms perform critical functions for which there are few or no substitutes • The impact on the majority of end consumers from a short-term disruption (counted in hours rather than days or weeks) may be limited, and these firms may therefore not be as attractive targets as banks or payment providers
3rd party service providers	**High**	Medium to **High**	• An attack on shared third party services can have wide-reaching consequences for financial stability by simultaneously impacting several parts of the ecosystem • Certain third-party services (for instance BankID and Swish) are also highly attractive targets as any service interruptions would have immediate impact on a large number of end customers
Insurers	Medium	Medium to **High**	• As a function of their activities, attacks against insurers present less of an immediate threat to financial stability and and insurers are therefore also less attractive targets • Nevertheless, insurers possess a plethora of information about individuals, SMEs and corporations and with IoT, the types of data collected, the number of attack vectors and the value of a successful attack is expected to increase
Branches to international banks	Medium	Medium	• While branches can be a conduit for an attack to spread across borders, they are in themselves less attractive as potential targets and an attack on them present less of a threat to financial stability

1.3. What can firms do to protect themselves?

This report mainly focuses on the collaborative actions banks, insurers and financial infrastructure firms can take to protect the overall Swedish financial sector from a financial crisis stemming from a cyber incident. However, any good defence must start at the individual firm level. There is a multitude of considerations related to establishing a robust cyber strategy for financial institutions. These considerations range from adjusting governance and the cyber operating model, to establishing a robust cyber risk management framework with associated policies, setting up risk and threat assessment capabilities, and ensuring that there is internal access to appropriate tools, people and skills. Each of these areas could be the subject of a separate report. For this reason, we have listed several key practical actions individual firms can take to protect themselves against increasingly sophisticated cyber threats in the short-term:

- Exercise and test incident-response capabilities
- Verify that internal cyber response playbooks and associated execution mechanisms are up to date, correct and understood
- Ensure that cyber response plans are also established for situations where the sector is under attack even if your institution has not been specifically attacked (yet)
- Confirm that an executive incident response team can be ready at short notice and that those on the team know their responsibilities
- Ensure that employees are aware of the potential of phishing attacks, and test their acuity in this regard
- Analyse third-party relationships for security vulnerabilities and level of preparedness for cyber events

- Review outstanding security vulnerabilities and ensure that all remediation controls are up to date and effective, such as critical patching
- Re-examine recent service outages or glitches that may have been attributed to a technical fault but upon re-examination could be tests by an external hacker regarding your defences

1.4. Cyber incidents and overall financial stability

Financial stability authorities focus on the vulnerabilities that can lead to a financial crisis (for instance through a run on the banks). Three "traditional" features of the financial system can be considered as the cause of such vulnerabilities, namely leverage; maturity and risk transformation; and procyclicality of the price of risk. Further, three additional vulnerabilities are worth highlighting. The first two – lack of substitutability and data integrity – are inherent to cyber attacks and the technological infrastructure they target. The final vulnerability relates to the loss of confidence that a large-scale cyber attack may cause and is not unique to cyber risk. Nevertheless, it is an important consideration as it may often be the main goal of a malevolent attacker to reduce confidence in the financial institutions and cause disorder.

Figure 2: Systemic cyber security vulnerabilities compared to traditional view on financial stability

TRADITIONAL VIEW

① **High leverage,** where even a small decline in the value of assets can result in financial distress and insolvency.

② **Maturity and risk transformation,** where a decrease in the price of illiquid or risky assets can lead to funding being withdrawn, forced asset sales and ultimately the failure of core institutions.

③ **Procyclicality of the price of risk,** which interacts with the leverage and maturity transformation to magnify price falls (falling asset prices decrease collateral values, which increases cost of borrowing and consequently decreases risky asset prices even further).

✚

SYSTEMIC CYBER SECURITY VULNERABILITIES

- **Lack of substitutability:** The financial sector is critically dependent on market infrastructure providers (be it stock exchanges, clearing houses, messaging systems etc.), of which there are only a few for each capability. If an attack disables any of these hubs, there would be very little possible substitution. Further, a large portion of the computing and storage in the financial sector is performed by a handful of cloud providers, and most financial institutions are dependent on similar software stacks.
- **Loss of confidence following an attack:** An attack with no systemic impact could still cause a run on the banks should it lead to a sufficiently large loss of confidence in the financial system. A wide-reaching theft of sensitive customer data could act as a catalyst, but one can also think of other causes: bank accounts being hacked, ATMs ceasing to work, or release of compromising financial information to the press.
- **Data integrity:** If a cyber attacker modifies key customer or market data to the point where it can no longer be trusted, it could cause the financial system to grind to a halt. One such example could be a malware attack on trading systems, where the malware places trades to destabilize the market. Until the cyber attack has been dealt with, trading may have to be suspended entirely with all its related consequences.

There are three key differences between cyber attacks and traditional financial shocks:

- **Timing:** Where financial crises often seem random, a successful cyber attack is carefully planned over a long period of time, in some cases including months of reconnaissance. The attack can then be launched at the most opportune time, to maximize the damage. The Systemic Risk Centre at the London School of Economics proposes that cyber risk has the largest impact when the financial system is already weakened. The impact on financial stability is even greater when attacks are timed in order to ensure simultaneous attacks on multiple firms and even sectors. An attack on several critical sectors could have significant impact on society and thus have more significant consequences on financial stability than an attack limited to just the financial sector.
- **Complexity:** The understanding of the "cyberspace risk dimensions" is still very limited compared to our understanding of financial risk, for which institutions are well versed in the development of advanced risk models for identification, quantification and management. For instance, an open question among central banks globally is how to appropriately set capital requirements for cyber risk due to the relative immaturity of modelling and more limited history of observations. This can cause a cyber incident to lead to both unpredictable events with high resulting losses. Furthermore, the next generation of attacks are likely to become even more complex, including leveraging quantum computing, AI and machine learning.
- **Adversary intent:** Unlike (most) financial risks, cyber attacks are designed by a malicious actor with the explicit goal to cause damage, disrupt legitimate business or commit fraud. This means rather than respecting the organisation structure and business processes we often work within, the attack can take advantage of gaps, interfaces and any ambiguity in responsibilities.

Whereas a financial crisis develops over time, a well-designed cyber attack can shut down the financial system overnight. Considering the consequences of the relatively controlled COVID-19 shutdown of the economy, it is not hard to imagine the major impact that an overnight crash of the whole financial system could have. And while the initial impact could be near-instantaneous, it will take much longer to restore the damage done. In 25% of cases it takes weeks to contain an attack, and for 15% of attacks containment requires months.[13]

While Sweden historically has experienced targeted attacks, several of the CIOs interviewed for this report were concerned that future cyber incidents would simultaneously hit multiple risk dimensions, infrastructures and sectors, causing systemic impact on society. Moreover, this was noted as being highly probable.

1.5. Cyber risk in the financial sector compared to other sectors

The risks and recommendations covered in this report relate directly to the financial sector. Nevertheless, at the fundamental level, the cyber threats to the financial sector are not all too different from those to other sectors that are critical to society. In other sectors, cyber attacks are also carried out with adversarial intent and are timed to maximise damage or disruption. Furthermore, the financial sector is inextricably linked to other critical sectors, as an attack on, for instance, electrical or telecommunications infrastructure would have immediate and significant implications on the activities in the financial sector as well. There are thus reasons for establishing coordination around cyber risk on a national and cross-sector level.

However, different sectors face different challenges pertaining to cyber risk. The actors, the attack vectors (the means by which an attacker gains access), their motives, the responses and the goals of an attack are different depending on the sector targeted. For example, the healthcare sector is

[13] Verizon (2019), Data Breach Investigations Report

characterised by large amounts of very sensitive personal and medical information and the transportation sector is concerned with passenger safety. The financial sector is both complex and heavily interlinked, also when compared to other sectors, which adds to the risks relative to other sectors. There is thus reason to believe that a sector-specific approach is most appropriate for financial services. The high-degree of interlinkages also contributes to the need for regulatory intervention around the work with cyber risk in the financial sector, which is further developed upon in Section 1.7.

Deep dive: The case for a sector-specific cyber risk strategy for the financial sector

THE CASE FOR A SECTOR-SPECIFIC CYBER RISK STRATEGY FOR THE FINANCIAL SECTOR

As outlined in the European Systemic Risk Board's (ESRB) recent report on systemic risks arising from cyber incidents, the financial sector is central to the functioning of the real economy.[14] The financial system performs a range of key functions, including payment services, securities trading, settlements services and deposit taking. With increasing digitalisation, these functions rely heavily on the confidentiality, integrity and availability of both data and IT infrastructure. The increasing digitalisation and interconnectedness of the financial sector coupled with the sector's high-value assets and data make it especially vulnerable to cyber attacks. This is further exacerbated by the widespread use of legacy or end-of-life IT systems in the financial sector, which may contain security vulnerabilities.

Using both real and hypothetical examples of cyber incidents, the ESRB shows how an attack can erode trust in the financial system and have systemic impact. A cyber risk turns systemic when the consequences go beyond being operational and begin having financial or confidence implications. As a result of its key functions, an attack on the financial sector may be more likely to cause significant financial losses compared to other sectors. Even the prospect of financial losses may be enough to lower the confidence in the financial sector, further increasing the risk of the event becoming systemic. This can cause a vicious circle, where the loss of confidence leads to financial losses as, for instance, markets react to the incident.

The ESRB also highlights the high degree of vulnerabilities that are shared across the sector. These range from insufficient oversight of common third-party suppliers, to legacy systems and organisational cultures not aligned with secure cybersecurity behaviours. Addressing these sector-specific vulnerabilities are key to ensure a secure cyber risk ecosystem in the financial sector.

This high degree of shared vulnerabilities combined with the interlinkages and the lack of substitutability (as described in Section 1.4) present a strong case for a sector-specific strategy for financial services. Furthermore, the financial sector is generally considered to be one of the sectors that has come the furthest in its cybersecurity efforts. With a sector-agnostic approach to cyber risk (for instance one led by the Swedish Civil Contingencies Agency, MSB), there is a risk that recommendations and proposed initiatives become too generic to accommodate for the differences between sectors. Similarly, sector-agnostic initiatives, as opposed to sector-specific ones, are not able to as efficiently leverage and build upon the already existing efforts in the financial sector and others.

As cyber risk concerns most parts of society, there is a wide range of organisations and authorities that have an interest in preventing and mitigating cyber incidents. As with any complex organisational activity, coordinating the work around cyber risk will require a certain level of delegation of responsibility. Delegating the responsibility based on sector is likely the most logical choice, given the sector differences highlighted above. Focusing on the cyber risk ecosystem for the financial sector also drives accountability in the sector. If financial authorities have a clear responsibility for preventing cyber incidents, this will raise the importance of the issues sector-wide. Further, financial institutions have more significant incentives from information sharing and knowledge transfer with other financial firms and authorities than with firms in other sectors. As such, there are likely diminishing returns from increasing the scope of cooperation to include dissimilar sectors.

A sector-specific division of responsibilities ensures that the work conducted around cyber risk considers the characteristics and maturity of different sectors. However, as cyber incidents may not be limited to a single sector, there is still need for cross-sector collaboration and central coordination. This report and its recommendations mainly relate to the ecosystem and work in the financial sector but will also touch on some of the initiatives that exist or are being undertaken at the central level.

[14] ESRB (2020): Systemic Cyber Risk

1.6. The need for cooperation around cyber risk

Over the past 5 years, many Swedish financial institutions have become victims of DoS attacks that have forced their websites to become unreachable and inoperable. Finansinspektionen estimates that the attacks in Sweden have increased in both frequency and sophistication.[15] As financial firms are exposed to attacks of a similar nature and vulnerabilities are tested by attackers across different institutions, there is a clear case for cooperation and information sharing in this area. There are clear scale economies that could be achieved from analysing threats on a common basis. Especially smaller firms may not be able to realise these scale economies on their own, despite potentially being systemically important. ENISA, the EU agency for cybersecurity, also states that "cyber risks are no longer an issue for people to deal with individually but are increasingly a social and civic responsibility that affects all sectors of the digital society".[16]

Collaboration on the topic is already ongoing in Sweden, but it is limited to bilateral communication between actors and various cooperation forums. However, in line with ENISA's statement, as cyber risk increasingly becomes a societal issue, more actors and authorities must become involved. As this evolves, keeping discussions on an ad-hoc or bilateral basis will quickly become unwieldy, inefficient, and there will be a need for a clear coordinating voice on cyber risk. Similarly, Sweden's neighbouring countries are increasing their focus on cyber risk. At the end of 2019, Riksbanken hosted the third Nordic conference on cybersecurity. During the conference, Stefan Ingves, the Governor of Riksbanken, emphasised the need for further Nordic cooperation as many of our institutions operate across the whole Nordic region.[17]

1.7. Cyber risk: a matter of public policy?

Public authorities have a fundamental responsibility (and that it is in their interest) to ensure all digital services are secured. Digitalisation provides substantial benefits to people and businesses. Ensuring secure and reliable digital services is now at the core of the modern society. A successful attack on digital infrastructure (including on the financial system), could have far reaching implications both for the work of authorities and for the lives of ordinary citizens. Mitigating cyber risk is clearly not only a concern for the private sector. Given the importance to society, some level of government intervention to mitigate cyber risk is therefore to be expected in most countries.

In addition, private entities do not have the same level of access to information as public authorities. As has been highlighted in the interviews underlying this report, access to intelligence from the military and law enforcement is a key component to an effective cyber defence and something that the private institutions have largely failed to secure.

A purely private response to cyber risk will also struggle with balancing the "greater good" with commercial values. Making the ecosystem and information sharing commercially attractive for the larger financial institutions, while still ensuring participation of smaller or specialist firms, is difficult. Without government intervention, the full social benefits from wider information sharing may not be realisable as some players may benefit more from these exchanges than others.

An additional and important factor is the presence of contagion risk. As already described, this risk can be realised as a cyber incident propagates through the financial systems. It can also be realised indirectly, through reputational impact across the whole sector following a successful attack on one firm. In the absence of public incentives or obligations, individual firms are likely to not fully internalise this risk and will therefore underinvest in security measures. This is especially true in the financial sector, given the high degree of interlinkages and shared vulnerabilities between firms and

[15] Finansinspektionen (2018), Supervision 9: Information and Cyber Security work in Banks

[16] ENISA (2013), Cybersecurity cooperation

[17] Riksbanken (2019), Opening remarks, 3rd Annual Nordic Cyber in Finance Conference

markets, as well as the lack of substitutability of critical activities in the sector. Such factors will drive substantial negative externalities from any cyber-related operational failures. Without government intervention, these externalities are likely not being sufficiently covered by investments of individual firms.

However, there are also downsides to an entirely government-run cyber defence. The cyber risk space is fast-moving and private actors tend to be more agile than government agencies in adapting in such an environment. Technical competencies are also more likely to lie with industry participants rather than with public authorities. Furthermore, cyber risk is a global concern and affects firms that are operating across borders. As such, one single state cannot guide the work in isolation.

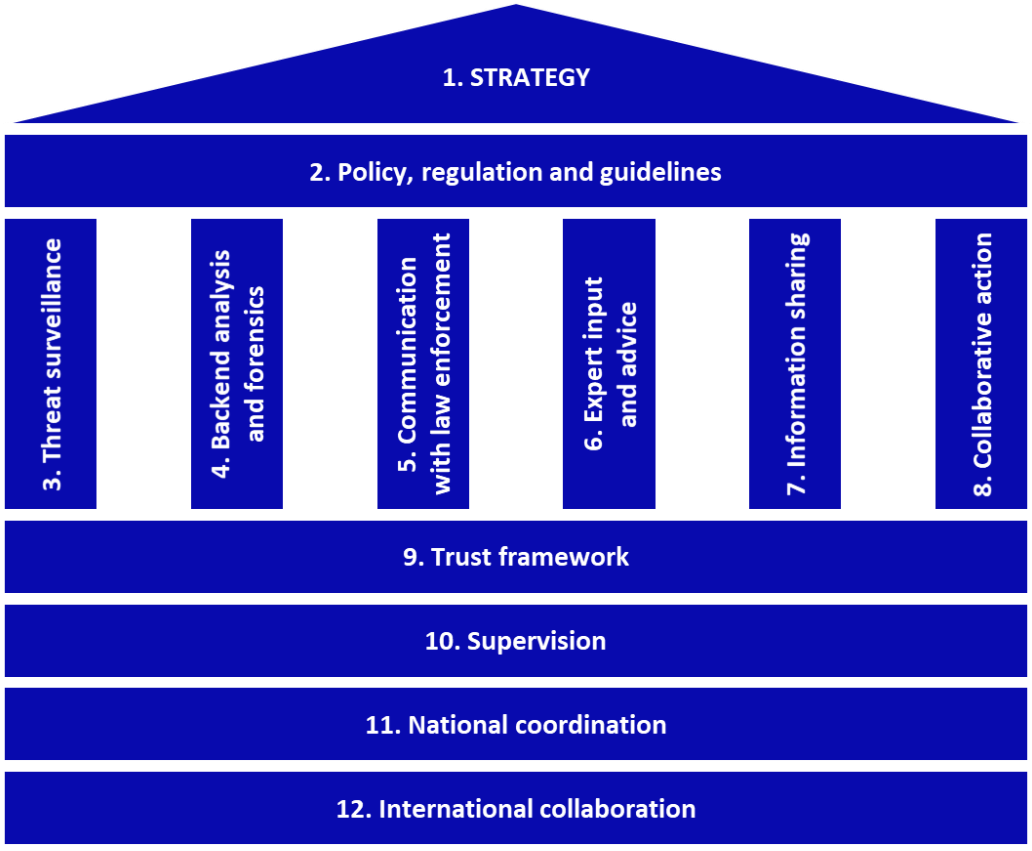
To summarise, cyber risk is clearly a matter of public policy but public authorities should work closely with the private sector to ensure that the ecosystem remains as efficient as possible. For example, rather than imposing top-down solutions, government actors can intervene in the ecosystem to provide incentives and facilitate processes with multiple stakeholders. The case for some degree of government intervention is even stronger in the financial sector due to the interlinkages and the lack of substitutability that characterise the sector.

2. THE CURRENT STATE

2.1. Functions that need to be performed for a hypothetical cyber risk ecosystem

Before we tackle how the current ecosystem operates in Sweden and the function of each actor, let us consider what functions should and could be performed in a well-prepared cyber risk ecosystem within the financial sector. These functions should be seen as building blocks in a modular ecosystem for cyber risk. While attempts in other jurisdictions have shown that it is difficult to centralise the work for cyber risk collaboration and information sharing, it could still be feasible to have one actor step in and assume the overall responsibility for facilitating the work. More likely, however, is that these functions are distributed across several actors. Indeed, this is the set-up that can be observed in most countries. The functions can be illustrated in the form of a "house". At the top of the house, you find the overarching activities involving establishing the strategy for the shared work as well as the common ground rules in the form of policies, regulation and guidelines. Then, illustrated as pillars, are the operational activities that are conducted in the ecosystem. Finally, at the bottom are the foundational components required to make the ecosystem work, including establishing trust and ensuring that the work is supervised and coordinated.

Figure 3: Functions in a hypothetical cyber risk ecosystem



1. Overarching national **strategy** for cyber risk with sector-specific strategies where additional detail is needed
2. The work around cyber risk has its foundation in **policy and regulation, with supporting guidelines**
3. **Upfront threat surveillance and relaying of information** on cyber threats to relevant actors

4. **Backend analysis and forensics** of cyber incidents for the overall ecosystem
5. **Law enforcement is involved** early when criminal activity is suspected to improve attribution abilities
6. **Expert input and advice on cyber risk** provided to actors (for instance smaller institutions) which do not hold that level of expertise or have resource constraints
7. Forums or organisational contexts in which **information can be shared** openly between actors, be it private or public
8. Collaborative forums in which **actions and preparation can be discussed and initiated jointly**
9. An agreed-upon **trust framework** between the relevant actors
10. **Supervision** of the activities and actions undertaken concerning cyber risk
11. **Coordination**, both to prepare for cyber incidents but also to coordinate a response when an incident materialises
12. **International collaboration** as cyber threats do not respect national boundaries

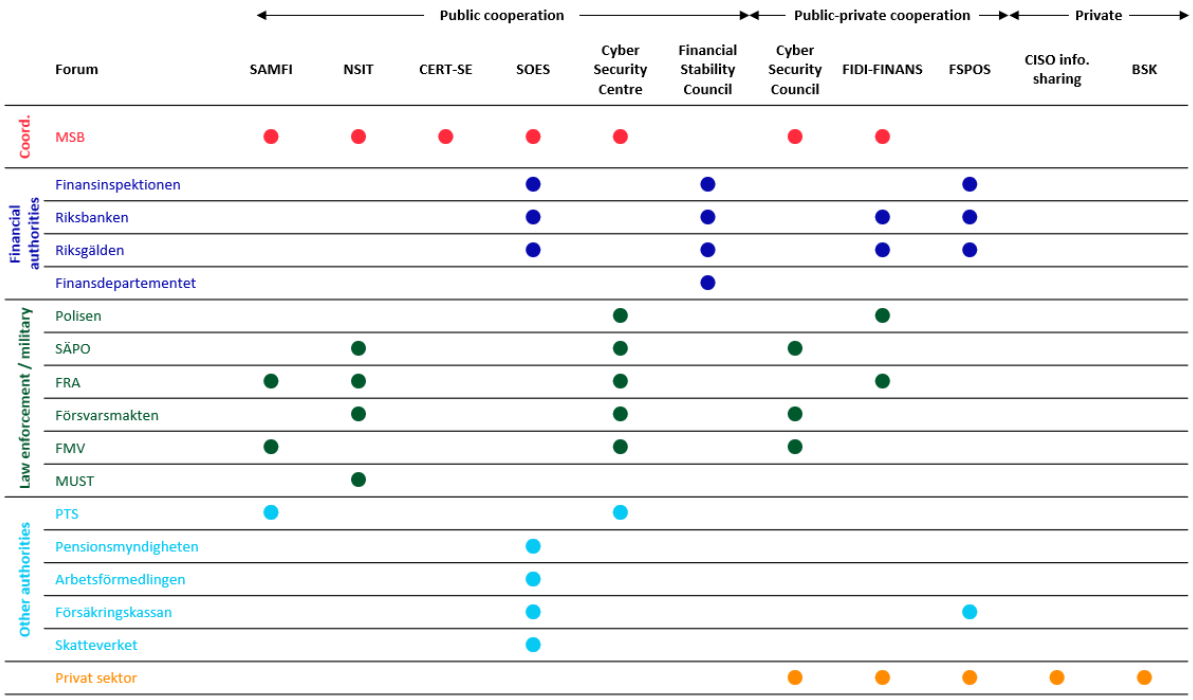
2.2. The current Swedish ecosystem

When we now turn to the current Swedish ecosystem, we will see that some uncertainty exists around how these functions are distributed, and that indeed some functions are not performed today. This also includes uncertainty around accountability, trust frameworks and information sharing.

Figure 4: Ecosystem forums in Sweden

	Forum	Led by	Description
Public cooperation forums	SAMFI (the Cooperation Group for Information Security)	MSB	Group of the four authorities defined as most critical for the national cyber security strategy – in charge of executing the strategy
	NSIT (National Cooperative Council against Serious IT Threats)	MSB	Cooperation between law enforcement and the military – analyses and evaluates threats and vulnerabilities
	CERT-SE (Swedish Computer Security Incident Response Team)	MSB	Supports authorities, firms and municipalities when cyber incidents occur and publishes warnings and advice on vulnerabilities
	SOES (the Cooperation Council for Financial Security)	MSB	Not directly focused on cyber risk, but works to ensure access and confidence in payments, especially from a societal perspective
	National Cyber Security Centre	MSB	Fully operational in 2025 and will produce analyses, spread information on threats, as well as coordinate during IT incidents and attacks
	Financial Stability Council	Ministry of Finance	Twice yearly meetings between the four authorities responsible for financial stability
Public-private	Cyber Security Council	MSB	Set up to inform, provide opinions on and quality assure MSB's work on cyber security – includes representatives from academia & private sector
	FIDI-FINANS (Forum for Information Sharing on Information Security)	MSB	One of the FIDI forums set up by MSB for information sharing in the sectors most exposed to cyber risk (focused on the financial sector)
	FSPOS (The Financial Sector's Private-Public Cooperation Group)	Riksbanken (rotating)	The main forum for public-private cooperation in the financial sector – has a working group focused on cyber risk
Private	BSK (Bankers' Association's Security Committee)	Bankers' Association	Committee for the shared security work between the banks in the Bankers' Association (including cyber security)
	CISO information sharing	N/A	Loosely organised cooperation on cyber security issues between the CISOs of the main banks

Figure 5: Ecosystem actors in Sweden



At the core of the financial ecosystem are the **financial institutions**, including banks, infrastructure players, insurance firms and payment providers. Much of the responsibility in preventing or responding to a cyber incident lies with them. The general opinion among those interviewed for this report is that at least the major institutions in Sweden have ramped up their cyber risk efforts and are generally well-prepared. However, some of the smaller institutions have been able to devote less attention to cyber risk and there is some concern that their unpreparedness could represent a vulnerability to the overall system stability.

A few clear themes have emerged during the interviews with financial institutions:

- There are several well-meaning initiatives around cyber risk, but there is a **lack of coordination**
- The attention paid to cyber risk in the financial sector from authorities in Sweden **does not match the importance of the sector** to the stability of the Swedish society
- There is a need for more **sector-specific coordination**, as the financial sector's needs and challenges related to cyber security are different from those of other sectors
- Without one clearly accountable authority, financial institutions sometimes receive **contradictory input** on their cyber risk efforts
- For collaboration to work efficiently, there should be **clearer incentives** for financial institutions to participate in collaboration
- **Information from law enforcement is limited** and almost only backward-looking on threats that have already been neutralised
- The current **private cooperation forums are somewhat limited by design** (for instance being specific to only banks, catering mainly to larger institutions)

Financial authorities

In Sweden, there are four authorities that are responsible for overall financial stability. These are **The Swedish FSA** (Finansinspektionen), **The Swedish central bank** (Riksbanken), **The Swedish National Debt Office**, (Riksgälden) and **The Swedish Ministry of Finance** (Finansdepartementet,

representing the government's interest in financial stability). These authorities meet twice annually to discuss financial stability in what is known as the **Financial Stability Council** (Finansiella stabilitetsrådet). However, the exact division of responsibility between these actors in areas pertaining to cyber risk is less well-defined.

Finansinspektionen has the responsibility to follow up on the regulatory compliance of cyber risk within financial institutions. It is participating in the EU Task Force for IT risk and has actively been part of producing the first EU legislation on cyber risk – the European Banking Authority's (EBA) guidelines on ICT risk. Finansinspektionen has also penned Swedish regulation on the topic, but the new EBA guidelines will provide more detailed directions for banks than the current principle-based Swedish regulation. Finansinspektionen has emphasised the importance of cyber security for several years (for instance writing a supervisory report on the topic in 2016) and issued the first cyber risk related sanctions as early as 2015. The authority has also highlighted the need for increased collaboration around operational incidents, including cyber incidents. However, at this point, this has remained a recommendation for banks and other actors to follow up on, for that reason Finansinspektionen has not yet taken an initiative to set-up such collaboration and is not taking part in the various collaboration forums that exist today around cyber risk.

Riksbanken and Riksgälden are operationally active in areas that in themselves could be the target of a cyber attack, with wide-reaching consequences for society. As such, these two authorities have built up internal cyber defence capabilities to a larger extent than Finansinspektionen. However, the responsibilities of Riksbanken and Riksgälden vis-à-vis the sector at large are not clearly defined. Riksbanken has until now taken a larger role in representing Sweden in the international cooperation around cyber risk, participating in various forums (including within ESRB and the Bank for International Settlements, BIS). Like many other European central banks, Riksbanken has also taken it upon themselves to implement the red-teaming cyber resilience framework TIBER-EU in the Swedish context (in the form of the TIBER-SE framework).

Cyber risk collaboration forums

The actor with the formal responsibility for coordination around cyber risk in Sweden is **The Swedish Civil Contingencies Agency** (MSB, Myndigheten för Samhällsberedskap). It is responsible for coordinating the work on cyber risk across the whole society. There are no other specialised actors or authorities to whom the responsibility for specific sectors are delegated. However, MSB has set up several information sharing forums for the sectors that are most exposed. One of these is **The Forum for Information Sharing on Information Security in the Financial Sector** (FIDI-FINANS, Forum för informationsdelning om informationssäkerhet i finanssektorn). Within this group, the major banks are represented as well as the main market infrastructure players. So are Riksbanken, Riksgälden, **The Police** (Polisen) and the military, through **The National Defence Radio Establishment** (FRA, Försvarets radioanstalt). However, Finansinspektionen has chosen not to participate in this group.

In the Swedish government's strategy for cyber security, four authorities are highlighted as being most important for the Swedish society's cyber security and preparedness. These are MSB, FRA, **The Swedish Post and Telecom Agency** (PTS, Post- och telestyrelsen) and **The Swedish Defence Materiel Administration** (FMV, Försvarets materielverk). In order to facilitate the cooperation between these authorities, **The Cooperation Group for Information Security** (SAMFI, Samverkansgruppen för informationssäkerhet) was established. Despite the national strategy acknowledging the importance of cyber security for the banking sector and financial market infrastructure, no financial authorities

are participating in this collaboration forum. Likewise, not all of the authorities responsible for the national critical infrastructure[18] are part of this group.

A **Cyber Security Council** has been set up to inform, provide opinions on and quality assure MSB's work on cyber security. This council has members from the military, law enforcement, academia and a few representatives from Swedish businesses. However, the financial sector is not represented, neither through the inclusion of financial firms, nor financial authorities.

The Swedish Computer Security Incident Response Team (CSIRT, as mandated by the EU NIS Directive), called CERT-SE**,** also sits within MSB. CERT-SE publishes warnings and advice on vulnerabilities in IT systems and collects IT incident reports from governmental agencies. Unlike in other countries (for instance Denmark, see below), where the CSIRT is working directly with financial authorities, no such formal cooperation exists in Sweden.

In addition to FIDI-FINANS, MSB heads up one additional forum related to the financial sector: the **Cooperation Council for Financial Security** (SOES, Samverkansrådet Ekonomisk Säkerhet)**.** While this group is not directly focused on cyber risk, it does work on ensuring access and confidence in payments, especially from a societal perspective. Given the threat that cyber risk may pose for payments infrastructure, these areas clearly overlap. Finansinspektionen is represented in this cooperation group, together with Riksbanken and Riksgälden. In addition, **The Employment Agency** (Arbetsförmedlingen), **The Social Insurance Agency** (Försäkringskassan), **The Tax Authority** (Skatteverket) and **The Pensions Agency** (Pensionmyndigheten) are also represented. The forum uses the traffic light protocol to facilitate sharing of information among its members, restricting disclosure of sensitive information outside the membership circle.

Law enforcement

Law enforcement is participating in several of the forums established by MSB, either represented by The Police or **The Security Police** (SÄPO, Säkerhetspolisen), or in some cases both. However, the law enforcement agencies are not participating in any of the same forums as Finansinspektionen. SÄPO, FRA and **The Swedish Military Intelligence and Security Service** (MUST, Militära underrättelse- och säkerhetstjänsten) make up the Swedish cyber defence together with **The Swedish Armed Forces** (Försvarsmakten). These organisations are all heavily involved in the cyber security activities coordinated by MSB as part of the **National Cooperative Council against Serious IT Threats** (NSIT) forum.

The private sector

In the private sector, **CISOs of the main banks in Sweden** have established a loose cooperation around cyber risk where they meet on a monthly basis to share information and knowledge. In addition, **The Swedish Bankers' Association** (Svenska Bankföreningen) has a long-standing **Security Committee** (BSK, Bankföreningens Säkerhetskommitté). Traditionally focused on areas such as physical security and fraud, the committee now also covers a working group on cyber risk. The major banks are represented in the committee by both their Head of Security and CISO, while smaller banks can choose to be represented by either the Head of Security or the CISO. Like FIDI-FINANS, the Traffic Light Protocol is used to promote information sharing in the group. The committee analyses and assesses the overall security threat level and prepares an annual report for its members on the security situation in the Swedish financial sector.

[18] Defined as energy, transportation, banking, financial market infrastructure, health care, distribution of drinking water and digital infrastructure

2.3. Public-private cooperation

The main forum for public-private cooperation in the financial sector is called **The Financial Sector's Public-Private Cooperation Group** (FSPOS, Finansiella Sektorns Privat-Offentliga Samverkan). The group was established in 2005 and includes the major banks, insurance companies and financial infrastructure firms, as well as Finansinspektionen, Riksbanken, Riksgälden and Försäkringskassan. The main goal of the group is to strengthen financial infrastructure through cooperation and information sharing. The chairmanship of the group rotates between the different members and at the time of writing is held by Riksbanken. The group primarily operates through three "working groups", one of which is focused on cyber risk. This working group includes Riksbanken and several banks and infrastructure firms but does not include Finansinspektionen or Riksgälden.

2.4. National Cyber Security Centre

In 2019, the Swedish government gave four authorities – MSB, FRA, SÄPO and Försvarsmakten – the task to evaluate the establishment of a Swedish National Cyber Security Centre. The four authorities then initiated an extended and deepened cooperation on cyber risk in October 2019, also including The Police, FMV and PTS. It did not, however, include any financial authorities. Within the context of this extended cooperation, the authorities presented a proposal for a **National Cyber Security Centre** to the government in December 2019. According to the proposal, the centre will be established over a five-year period and is planned to be fully operational in 2025. The purpose of the centre is to produce common analyses and situation reports on cyber threats and vulnerabilities, to spread information among authorities and other actors, and to coordinate the work during IT incidents and cyber attacks. The centre itself will be set up as an independent unit, but will primarily be staffed with employees from the involved authorities. A strategic steering group will be established consisting of the head of each of the involved authorities. In the short- to medium-term, a more operative steering group will be established, with managers from each of the authorities.

3. CASE STUDIES

3.1. Denmark

Unlike in Sweden, there is more formalised cooperation around cyber risk in the Danish financial sector. **The Danish FSA** (Finanstilsynet) has to a large extent taken responsibility to organise the work around cyber risk. For example, it publishes a three-year strategy for cyber security in the financial sector.

Both Finanstilsynet and the **Danish central bank** (Nationalbanken) participate in the cooperation across sectors by interacting with the **Centre for Cyber Security** (CFCS)**.** This centre is set up as a separate authority on cyber security, and one of its most critical tasks is to map interdependencies between different sectors. In addition, it serves as a situation centre and analyses cyber attacks, performs threat evaluations, participates in counter-actions against incidents and forms policy in the cyber risk area.

As part of its strategy (covering the years 2019 to 2021), Finanstilsynet also established a **Decentralised Unit for Cyber and Information Security** (DCIS, Decentral enhed for cyber- og informationssikkerhed for finanssektoren). This unit, which is operated by, and formally a part of, Finanstilsynet, is set up to coordinate the work around cyber security. It supports actors in the financial system across three main initiatives:

- Assessment of threats, vulnerabilities and risks
- Assessment of the sectors' preparedness
- Knowledge sharing

The DCIS unit is in charge of continuously ensuring that the cyber risk strategy for the financial sector is being followed and is also responsible for re-evaluating the strategy when necessary. The strategy clearly identifies Finanstilsynet as responsible for cyber security in the financial sector due to being its supervisory authority.

The Financial Sector Forum for Operational Robustness (FSOR) is a cooperation forum headed by the Nationalbanken and established in 2016 with the aim of improving operational robustness, including Danish cyber resilience. The members of the group are the key players in the Danish financial sector, including Finanstilsynet, systemically important banks, data centres and market infrastructure firms.

The group's work comprises deciding on, and ensuring execution of, common actions to protect the stability of the financial sector, including actions against cyber attacks. It is responsible for creating frameworks for cooperation and information sharing within the sector, with other sectors and internationally. As part of this work, Nationalbanken oversees testing the preparedness of the Danish financial infrastructure against cyber attacks, through the Danish implementation of the TIBER-EU framework (called TIBER-DK). Its first tests were completed during 2019. The FSOR also acts as the link between the financial sector and the national crisis response, NOST, with data collected by FSOR used to define the national situational picture.

Unlike in Sweden, the Danish financial authorities (including Finanstilsynet) and financial institutions have decided to join a Computer Emergency Response Team (CERT), specific to the Nordic financial sector which has been named **NF-CERT.** This CERT was originally a Norwegian unit, but now includes authorities and banks from both Norway and Denmark. Interest in joining this CERT has, however, been limited in Sweden, with interviewees stating that they feel that the needs are already met by other actors and forums in Sweden. It should be noted that the CERT that operates within MSB in Sweden is general to all types of cyber risk, and that no CERT specific to the financial sector exists.

In January 2020, a **Cyber Security Council** was established as a public-private group to provide advice to the government on how to protect against cyber threats and to secure knowledge sharing between authorities, businesses and academia. The group is chaired by the Cyber Security Centre. However, Finanstilsynet is not represented on the Council.

Overall, the ecosystem in Denmark has progressed slightly further than that in Sweden, as it already has an operational Cyber Security Centre. There is also more formalised cooperation within the financial sector around cyber risk, and it is Finanstilsynet that operates the DCIS that coordinates this work.

3.2. UK

In the UK, upon request from the **Bank of England** (BoE), the non-profit organisation UK Finance has designed and operationalised the **Financial Sector Cyber Collaboration Centre** (FSCCC). The FSCCC's mission is to proactively identify, analyse, assess and support coordination of activities that mitigate systemic risk and strengthen the resilience of the UK financial sector. This is achieved through collaborative activities between, and focused operations across, financial services industry partners, the UK government and international authorities.[19] Industry participants in the utility include the **private sector**; regulators such as BoE, the **Financial Conduct Authority** (FCA) and the **Prudential Regulation Authority** (PRA); T**he UK government**; and **Law enforcement**.

The utility is designed to be operational and agile in nature and acts as a national and international interface on cyber topics. The centre utilises intelligence and law enforcement partnerships to attribute acts to, and pursue, the criminals behind cyber attacks. As part of the FSCCC, operational centres for monitoring attacks have also been established, where analysts from the private sector are joined by members of intelligence agencies, law enforcement and authorities. In addition to serving as a forum for information exchange, the operations centre is also a centralised source of up-to-date information on threats which can be accessed by private institutions once sufficient security clearance has been granted.

There is also a clear tiering or layering in the information sharing model in the UK, where organisations can choose the extent of their commitment and integration. Outside the operations centre, information is anonymised to be able to be shared with other financial institutions and infrastructure firms. The information and analysis outcomes are then redacted and summarised in order to also be shared with the broader community.

3.3. Singapore

Singapore and the local financial regulator **Monetary Authority of Singapore** (MAS) are generally regarded to be at the forefront of the global work on cyber security. In 2018, the country implemented a new Cybersecurity Act which added stricter requirements on the cyber security work of financial institutions. MAS has set up multiple standing committees to collaborate with local financial industry participants on sector-wide initiatives and exchange insights into cyber threats and countermeasures. MAS has also established a **Cyber Security Advisory Panel**, which is comprised of international cyber security experts and advises both MAS and financial institutions.

Moreover, MAS oversees a **Cyber Risk Management research project** led by Nanyang Technological University in collaboration with financial services firms. The project aims to analyse risk drivers and impact quantification of cyber event scenarios, including systemic events. MAS has also invested heavily in recruiting cyber security experts, as well as training its supervisors in cybersecurity. It has

[19] https://www.ukfinance.org.uk/blogs/promoting-more-cyber-resilient-culture-across-financial-services

also appointed a member in its Board-level Risk Committee with specific background in cyber risk management and has added a Chief Cyber Security Officer to its management team.

In order to allow FinTechs to pursue innovative financial products while reducing the risk for the financial sector, MAS has established a FinTech **regulatory sandbox**. This sandbox provides FinTech actors a well-defined space to experiment within. Moreover, FinTech firms are only allowed to participate on the actual market once they have proven that they fully comply with all relevant requirements, including for cyber risk.

MAS has also collaborated with **The Financial Services Information Sharing and Analysis Centre** (FS-ISAC) to establish a regional analysis centre in Singapore, which will strengthen cyber security information sharing across South East Asia.

4. FUTURE STATE IMPROVEMENT OPPORTUNITIES

Examining the "building blocks" from our hypothetical ecosystem in section 2.1. and contrasting it with the current activities in the Swedish ecosystem, we can propose areas for improvement.

Compared to the Danish and UK ecosystems (and to a lesser extent Singapore), there is no single coordinating function for cyber risk in the financial sector in Sweden. In Denmark, Finanstilsynet operates the DCIS unit that coordinates work around cyber risk in the Danish financial services industry. In the UK, the non-profit organisation UK Finance has set-up the FSCCC. While Sweden's new National Cyber Security Centre is intended to serve some of the same goals as these units, several key areas are still unclear concerning the set-up of this new centre. There has been limited participation of financial authorities and organisations in the centre, nor has the financial sector participated during its design phase. There may thus be reason to believe that the National Cyber Security Centre in Sweden will not serve the needs of the financial sector as well as the sector-specific counterparts set up in Denmark and the UK. Nevertheless, like is the case in Denmark, there would be clear benefits from close collaboration between the National Cyber Security Centre and the financial sector (for instance through secondments).

Recommendation 1:

A financial sector-specific collaboration unit should be established in Sweden, to facilitate cooperation between the National Cyber Security Centre, the CERT and other collaboration forums.

There are existing forms of cooperation in Sweden that cover many of the characteristics described below and that could be developed upon for this purpose, including Bankföreningen's Security Committee and the FSPOS private-public cooperation. For any of these forums to be successful as the financial sector-specific collaboration unit, they would need the legitimacy of being regarded as the primary coordinating function (as the DCIS in Denmark and the FSCCC in the UK).

4.1. Potential roles for Finansinspektionen in the future state

In this section, we will highlight the roles that Finansinspektionen could play in relation to the improvement areas and to create the "building blocks" of the Swedish cyber risk ecosystem. We will, however, be less prescriptive about other actors. Instead we will only note when we believe that Finansinspektionen may not be the best suited actor to address an area for improvement.

One could envision two different paths, or archetypes, for Finansinspektionen going forward. Either Finansinspektionen becomes further involved in the collaboration around cyber security, for example by taking charge of establishing a trust framework, referred to as ***Archetype 1***. The other alternative is that the organisation remains hands-off with regard to cyber security and assumes the role of oversight and assurance. This archetype is referred to as ***Archetype 2*** below. Depending on the archetypical role for Finansinspektionen, the set-up of each of the building blocks for the ecosystem will differ.

This also relates to our first recommendation on the establishment of a collaboration unit for the financial sector. Finansinspektionen could play three different roles in relation to this unit. It could assume the main responsibility for the unit and the coordination of the work, similar to Finanstilsynet in Denmark and MAS in Singapore. Alternatively, it could participate in the work in the coordination unit, but not actively lead it, as the UK supervisor does in the FSCCC. Finally, a coordinating unit could be set up without Finansinspektionen participating. In both of the first two alternatives, Finansinspektionen would have to clearly delineate between its role within the coordination unit and its supervisory role. It would also likely not participate in information sharing sessions, to allow the financial institutions to share information openly. In the cases were Finansinspektionen does not take the leading role, an existing forum or organisation could be leveraged or repurposed as a collaboration centre for the Swedish financial sector (for instance within the FSPOS collaboration or the NFCERT organisation, as described previously).

4.2. Strategy for cyber risk

Since 2016, Sweden has established a national strategy for cyber and information security. However, this strategy is positioned as a high-level document with little to no specific guidance on how to prevent, handle or mitigate cyber attacks in the financial sector. As such, common playbooks for cyber attacks and a common understanding of potential scenarios for the financial sector have thus far not been established in the Swedish ecosystem.

There is reason to believe that efficiency suffers as more organisations from different sectors are included in a collaboration. A sector-specific strategy for Swedish financial services, similar to that in Denmark, would therefore allow for more detailed and efficient coordination and prioritisation of different initiatives. Similarly, such a strategy would provide a single source of information for how the work on cyber risk is conducted in the Swedish financial sector. Interviews have also suggested that the national cyber security strategy is too high-level to provide proper guidance on the work in financial institutions, which can partly be explained by the strategy not being sector-specific.

Recommendation 2:

A sector-specific strategy for cyber security should be published to direct the work in the Swedish financial sector.

Archetype 1:

Finansinspektionen, like the Danish FSA, assumes responsibility for publishing a cybersecurity strategy for the financial sector.

Archetype 2:

Finansinspektionen does not participate in the work on a sector-specific strategy, instead only supervising the work conducted based on it. This responsibility could instead befall one of the established cooperation forums for cyber risk, or an industry body.

4.3. Policy, regulation and guidelines

There have recently been two significant developments in regulation related to cyber security. One is the introduction of the NIS Directive in 2018, which introduces requirements on information security and incident reporting for providers of infrastructure critical to the Swedish society. This includes banking business and financial markets infrastructure, both areas under the supervision of Finansinspektionen. The other significant development was the update of the Swedish Protective Security Act in April 2019. Similar to the NIS Directive, the updated Protective Security Act tightens requirements for the security of IT systems at critical infrastructure providers, including the banks and market infrastructure firms under the supervision of Finansinspektionen. Interviews conducted for this report suggest that the appropriate manner with which to approach these two regulations have been frequent topics of discussion between financial firms in the collaboration fora. This may partly be due to limited, or insufficient, guidance from authorities on the implementation of the new regulations and their ramifications for the financial sector.

Recommendation 3:

Establish a clear format for providing guidance and Q&A on regulatory changes.

Archetype 1:

Finansinspektionen, as the lead for a collaboration centre, provides guidance on regulatory changes as well as establishes regular opportunities for discussion with financial firms on regulatory topics.

Archetype 2:

A sector-wide common interpretation of how to implement regulatory changes is agreed upon by the financial institutions, which can then be confirmed by Finansinspektionen in its supervisory role.

4.4. Threat surveillance and analysis

Threat surveillance

Up until now, most of the threat surveillance work has been handled by the financial institutions themselves, with no centralised mechanism for the purpose. As these capabilities tend to be more mature and efficient within larger organisations, this leaves smaller institutions (including online and challenger banks) less informed. Furthermore, while informal information sharing between the larger banks in Sweden takes place, the smaller ones are generally excluded from these fora. The impact on overall financial stability of an attack on a financial institution may not, however, scale linearly with the size of the institution. A severe enough attack even on a smaller institution could be sufficient to impact the public's confidence in the financial system.

Other jurisdictions have experienced success by sharing threat intelligence through a centralised secured conference call. For example, some successful public-private partnerships have established an incident phone line, where financial institutions can obtain information in real time from authorities, supervisors and peer institutions. A further development of this concept is operational centres for monitoring cyber attacks, where analysts from the private sector are joined by members of intelligence agencies, law enforcement and authorities. In addition to serving as a forum for information exchange, these centres serve as centralised sources of up-to-date information on

threats which can be accessed also by private institutions once sufficient security clearance has been granted. Bankföreningen's Security Committee performs ongoing analysis of the threat level from different security-related risks, based on the information shared by the member banks' security officers. This provides some of the benefits of a cyber risk operations centre (for instance up-to-date threat information) but is not operationalised to the same extent as the operations centres active in the UK. However, given that it is run by Bankföreningen, the information from the committee appears to be only available to the banking sector and not the wider financial sector.

The NFCERT organisation provides threat intelligence for the benefit of Norwegian and Danish financial institutions. Rather than setting up separate infrastructure for the Swedish financial sector, there may be advantages to extending this already existing pan-Nordic collaboration. However, Swedish financial institutions have to date been reluctant to join this forum due to perceived high membership fees. With adjusted membership fees, leveraging the capabilities of NFCERT for threat surveillance in Sweden may be an attractive option. As cyber threats are increasingly international and there is little reason to think that the threats to the Swedish financial sector differ from those to the Norwegian and Danish sectors, pan-Nordic shared threat surveillance capabilities appear a logical choice.

Backend analysis and forensics

Similarly, forensic analysis is performed separately by each individual financial institution. Interviews with cyber security staff at banks, insurers and market infrastructure providers have revealed that incentives to share performed analyses are currently limited. This shortcoming will grow in severity over time, as attacks become more wide-reaching and more rarely are limited to one single institution. There would be significant efficiency gains in the ecosystem from sharing the analysis work across institutions.

However, to achieve these efficiency gains, analyses must be able to be shared in a secure and, most importantly, an anonymous manner. One of the main benefits of centralised collaboration, rather than bilateral information sharing, is that the source of the data and the institution(s) involved can be anonymised. By ensuring anonymisation, financial institutions can provide information to a classified party on perpetrated attacks and the forensics lessons learned can be shared with both authorities and other institutions – without risking retribution from authorities or negative reputational consequences. Whereas this may prove an efficient venue in general, a centralised (thus, "governed") function is also at risk of politicising and weaponising specific issues or events – either by exceedingly promoting a favoured view or by outright silencing (censoring) dissent.

It should be noted that the National Cyber Security Centre that is being established over the coming five years is intended to perform analysis of cyber incidents and threats. However, to be of use for the financial services industry, it is paramount that the information does not become classified and stays with the authorities within the centre, but that it can be shared with private actors as well. If this is not achieved, it is likely that there will be duplication of work as financial institutions will continue to perform their own analysis of threats. This form of threat and mitigation assessment would also help with transparency and understanding of cyber risk. This better understanding would also be able to support the insurance sector with parametrising the risk to give firms better cover (and start a virtuous cycle of improved mitigation leading to lower cost of insurance).

Recommendation 4:

Perform threat intelligence and forensics analysis in a centralised way and ensure that the information is accessible for all institutions, for instance through a secured conference call or a cyber operational centre.

Archetype 1:

Finansinspektionen organises and coordinates the process for threat surveillance and forensics analysis, but involves analysts from domestic financial institutions through a secondment model.

Archetype 2:

The financial institutions set up a common process for threat surveillance and forensics without the involvement of Finansinspektionen, or the Swedish financial institutions decide to join NFCERT and leverage its already existing threat surveillance capabilities.

4.5. Communication in the ecosystem

Involvement of law enforcement

In the current ecosystem, there is no formalised process for the financial authorities to share information on cyber attackers with law enforcement. Likewise, communication from law enforcement (whether the Police or SÄPO) is primarily conducted on an ad-hoc basis, with law enforcement agencies reaching out when they have information to share. As highlighted in the interviews and based on learnings from other jurisdictions, there are multiple areas for potential improvement related to the communication between authorities and financial institutions.

Firstly, a clear protocol for communication with law enforcement should exist for both financial institutions and the supervisor. Without a clearly defined partnership around cyber risk, it is often too late for prevention by the time law enforcement has been engaged. Furthermore, without early and explicit involvement of law enforcement, the cyber attackers often cannot be convicted in court due to lacking attribution. As most financial firms and supervisors lack the experience and knowledge to preserve the chain of evidence until law enforcement is engaged, the evidence protocols do not stand up to scrutiny.

Secondly, a strong partnership is required to build mutual trust between financial firms, the supervisor and law enforcement. By design, law enforcement officers are reactive and rely on the financial firms and supervisor to report incidents, threats and suspicions. Without sufficient trust in the partnership, organisations may be reticent to share information they have with law enforcement and instead opt to handle the issue internally. This is similar to the issues solved by the newly established cooperation in the Swedish banking sector against financial crime, which centralises anti-money laundering analysis of transaction data and on which Oliver Wyman advised Bankföreningen.

Thirdly, as financial firms have become better at protecting against external breaches, more cyber attacks are perpetrated by internal actors. To ensure that malevolent internal actors are not able to slip between the cracks, it is important that classifications and protocols are different depending on evidence and root cause.

Finally, cyber attacks are rarely contained to a single nation state and even when they are, the perpetrator may be located in another jurisdiction. It is therefore key to understand what global authorities and law enforcement agencies (Europol, Interpol) should be engaged and how the escalation procedure works. In the UK, increased collaboration between law enforcement, public sector and financial firms have significantly contributed in efforts to identify and close down malevolent actors.

Recommendation 5:

Establish a standardised communication protocol with law enforcement and process for evidence collection.

Archetype 1:

Finansinspektionen leads the work with creating a process for collecting evidence on impending cyber attacks and sharing of this information in the financial sector.

Archetype 2:

A process is defined by another actor, for instance as part of the collaboration centre (see Recommendation 1).

Expert input and advice

The Swedish CERT is providing information and advice on cyber risk in general. There is, however, no actor providing information and advice specific to the financial sector. This type of support could be vital in the case of a cyber attack on the financial system as smaller and medium-sized financial services organisations may not have the expertise, knowledge or means to apply threat intelligence even if it is shared. The NFCERT organisation provides such sector-specific expert input to Danish and Norwegian financial institutions, but most Swedish firms have not acknowledged the value of membership thus far.

In the UK, expert input and advice has been assured through secondment of analysts from financial institutions. This secondment leads not only to concentration of knowledge that otherwise is spread across many organisations to a single point of contact, but also ensures that financial institutions will be able to upscale their own capabilities by learning from analysts seconded from other organisations. In addition, a secondment panel ensures accountability from the financial institutions as they are actively involved in the generating the expert advice.

Recommendation 6:

Ensure there is a commercially viable source of knowledge and expert advice on cyber risk for the financial sector that is accessible also for smaller firms (as NFCERT is for the Danish and Norwegian financial institutions).

Archetype 1:

Finansinspektionen establishes a collaboration centre with seconded analysts from financial institutions.

Archetype 2:

Expert input and advice are provided from another source, such as NFCERT or the National Cyber Security Centre.

Information sharing

The information sharing forums on cyber risk present in the Swedish financial sector, primarily FIDI-FINANS and FSPOS, were highly regarded in the interviews held. However, beyond making the overall system more robust, interviewees suggest that there are few "incentives" related to sharing information. Organisations of different types or sizes are capable of contributing information of varying relevance, volume and granularity, making the benefits from participation unequal.

The level of confidentiality of the information shared may also pose issues. The new National Cyber Security Centre is likely to be a valuable source of information on cyber threats. However, without providing forum members with sufficient security clearance it may be difficult to share this information in the collaboration forums.

A few interviewees have also raised the topic of not only knowledge sharing, but also data sharing on cyber incidents, for example in the form of a centralised repository. This is something that currently does not exist in Sweden, but which interviewees feel would bring substantial benefits to the internal operations at financial institutions.

Recommendation 7:

Provide infrastructure for sharing confidential data (for instance establishing secure shared technology) and ensure information sharing is commercially viable.

Archetype 1:

Finansinspektionen establishes infrastructure and information sharing forums, for instance as part of a new collaboration centre.

Archetype 2:

Centralised data technology and information sharing opportunities is ensured by another actor, either in a new format or as part of the already existing forums (for instance FIDI-FINANS and FSPOS).

4.6. Collaborative action

While the collaboration forums work well in Sweden, they are mainly limited to information sharing. The FSPOS working group has performed some additional work, mostly producing reports on relevant topics. For instance, the cyber risk group wrote a report on cyber risk awareness in December 2018, but is currently dormant. However, there are no formalised groups for taking common action against cyber threats that concern the overall industry. The CISOs of the main banks in Sweden have established a loose cooperation around cyber risk. However, interviews suggest that these types of less formalised collaboration groups are disparate and, in many cases, have no authority, hierarchy or active governance structure. This generates accountability and authority challenges. In addition, in the absence of formalised collaborative action, there have been several short-lived attempts to organise the financial sector on cyber risk (for instance an initiative started and subsequently abandoned by Fondhandlareföreningen).

Recommendation 8:

Ensure that a new collaboration centre has capacity to also proactively act and respond, in addition to sharing valuable information.

Archetype 1:

Finansinspektionen coordinates the work in the collaboration centre (but is likely not actively participating in, deciding on, or executing common actions).

Archetype 2:

The mandate of existing collaboration forums is expanded to also allow for escalation and common actions (without Finansinspektionen's direct involvement).

4.7. Trust framework

Given the sensitive nature of information concerning cyber incidents and the potential for wide-reaching reputational implications, any collaboration must be built on trust. Following the UK model, a trust framework should be established as the foundation for building trusted relationships.

A trust framework is a governance focused capability common in many countries (including the UK), which defines the set of activities and responsibilities of all entities in a joint effort. The aim of the framework is to build trust among its participating entities. This is achieved by clearly defining and agreeing on the structure of the ecosystem, the terminology used, the responsibilities of each entity and the way to ensure that those responsibilities are fulfilled. In this context, "trust" refers to the ability of the different actors to operate in a trusted way with each other, rather than the "confidence" the general public has in the financial system (which is also an important consideration when discussing cyber risk).

This framework should define an interaction and sharing model that introduces mutual trust in the ecosystem. For there to be an efficient flow of data between organisations, both data sharers (financial institutions) and data consumers (Finansinspektionen) as well as observers (industry organisations) must be comfortable that information can be shared anonymously and without repercussions. For this to work, one must implement different levels of confidentiality and clear procedures for redaction of details depending on whom the information is shared with. Participants need to be able to trust that information they share is not disseminated beyond the intended audience. In addition, the trust framework should cover the legal requirements and the governance that need to be in place for trust to be established between actors.

Recommendation 9:

Ensure a trust framework exists to facilitate the interaction and collaboration between actors and set clear governance requirements therein.

Archetype 1:

Finansinspektionen defines a trust framework for cyber risk in the financial sector.

Archetype 2:

A trust framework is defined as part of a new collaboration centre.

4.8. Supervision

There is some uncertainty around where the supervisory responsibility lies for cyber risk. On a global level, the financial supervisor may play four different roles surrounding cyber risk:

- To provide oversight of the cyber risk measures undertaken by financial institutions
- To protect financial stability in the event of a cyber incident
- Provide guidance on cyber risk considerations (usually on a higher level of abstraction)
- Share trends and/or recommendations on cyber risk based on failings discovered in conducted inspections (on an anonymised and high level)

In Sweden, Finansinspektionen certainly has the responsibility to supervise the work of the individual financial institutions around cyber risk, in line with its responsibility for other risk types. However, the responsibility is not as clear in terms of the other potential supervisory roles. Is it Finansinspektionen's role to prevent impact on the financial stability following a cyber incident? Where does the supervisory responsibility end for Finansinspektionen and where does it start for other authorities? Should Finansinspektionen, for example, have within their supervisory scope that financial institutions securely use cloud services and have secure and reliable internet connections? Could a cloud service provider be in the scope of Finansinspektionen's supervision in the case that the services provided by the company are vital to the financial ecosystem? How should Finansinspektionen position itself vis-à-vis other third party financial services that are currently not within its supervisory scope but that financial institutions are dependent on?

Finansinspektionen has also, to date, elected not to actively provide guidance on how cyber security efforts should be carried out in Sweden. Instead, it has kept any directions closely linked to current regulatory requirements and therefore only provides input as part of its existing supervision. Comments on trends and analysis around cyber risk have therefore mainly been made by other actors, limiting any views on the work in financial institutions to high-level guidance where further improvements are required.

In the context of the wider ecosystem, Finansinspektionen has largely decided to remain outside of the various collaboration forums that exist. This "at arm's length" relation to the ecosystem and the collaboration efforts allows Finansinspektionen to remain fully independent in its supervisory capacity. There may also be hesitation from the financial institutions to share information as freely with the supervisor at the table. The contrasting example would be Denmark, where Finanstilsynet has taken the role as coordinator of the various ecosystem initiatives and is participating actively. Interviews have revealed contrasting opinions on the issue. Some interviewees consider that the supervisory role of Finansinspektionen is unreconcilable with participation in the collaboration forums whereas others see benefits in Finansinspektionen also providing advice and guidance.

Recommendation 10:

Finansinspektionen should decide whether to provide ex-ante guidance in addition to its ex-post supervisory activities.

Archetype 1:

Finansinspektionen provides clear guidance and recommendations on supervisory matters related to the cyber risk work of financial institutions.

Archetype 2:

Finansinspektionen limits its role to being the supervisor and to supervising the cyber risk work in the sector "after the fact."

4.9. National coordination

MSB formally holds the coordinating role for the overall cyber security ecosystem. However, several interviewees have expressed that MSB's breadth of responsibility is wide, which may present challenges when providing the coordination required for the financial sector. Furthermore, some interviewees stated that MSB's main areas of expertise may not be within the financial field. Finally, MSB is an organisation closely tied to the Swedish military. It was formed from the previous Swedish Emergency Management Agency (Krisberedskapsmyndigheten), for which the Ministry of Defence was the principal. Consequently, multiple interviewees said that they believe that MSB may have different priorities than the financial authorities on areas pertaining to cyber risk. This includes focusing more on the actors behind attacks, trying to determine attribution, whereas the financial sector is more interested in the attack vectors, what the consequences (losses) were and what can be done to prevent it from happening again. In one interview, it was expressed that financial stability unlikely is the primary objective of MSB, unlike the goals of the financial authorities.

As a result, the cyber security ecosystem in the Swedish financial sector is fragmented and there is both duplication of effort and inconsistency in tackling security challenges. Financial institutions are receiving similar data requests from multiple authorities. With the increased attention to cyber security issues in the financial sector, more actors are keen to find ways of working together on the topic. This has led to a surge in various ad-hoc or unformalised forms of collaboration, which has further negatively impacted the degree of coordination in the sector.

Commercial considerations have also impeded some attempts to formalise collaboration. For example, the pan-Nordic NFCERT forum applies an economic model where membership fees are based on the size of each member organisation. As a consequence of this model, the major Swedish financial institutions have decided to remain outside the collaboration forum.

For collaboration to work in the Swedish ecosystem, pure altruistic motives are likely not sufficient if there are substantial associated costs. This is especially true if there is a commercial entity which may profit from fees levied. While all participants recognise the benefit for the greater good, interviews suggest that there also must be clear perceived gains for each organisation from working together in order to enable efficient collaboration. The NFCERT collaboration has proven to work well in the Danish context where most financial institutions have decided to participate. This suggests that a similar forum could work well in Sweden if the commercial considerations are resolved, recognising this may be challenging. One potential route could be to dedicate public funding for these types of activities (such as threat surveillance, backend analysis, etc.).

Recommendation 11:

Appoint an organisation that has the explicit responsibility for coordinating the work around cyber risk in the Swedish financial sector ecosystem, and for interacting with MSB (as the overall national coordinator).

Archetype 1:

Finansinspektionen assumes the coordinating role for the cyber risk ecosystem in the financial sector.

Archetype 2:

Another actor assumes the coordinating role.

4.10. International collaboration

Finansinspektionen has historically always had strong cooperation with the other supervisors in the Nordics and Baltics, partly because much of the relevant legislation is similar in the region and the major financial institutions are active across the jurisdictions. The organisation also participates in various EU bodies, but to a lesser extent in fora relating to cyber risk. Riksbanken, on the other hand, is participating in a wide range of collaboration fora on cyber risk with international central banks (arranged by ESRB, BIS, SWIFT, etc.). However, there should be a clear link between the information gathered internationally and the domestic sector, to ensure that learnings from international collaboration are being applied domestically. In the same way, there should be a clear Swedish contact point for international organisations to liaise with in the event of a cyber incident. It could be argued that this level of clarity on the responsible authority does not exist currently in Sweden.

Recommendation 12:

Appoint an organisation as the single point of contact for contact with international authorities on cyber risk.

Archetype 1:

Finansinspektionen assumes the role as the point of contact for international authorities.

Archetype 2:

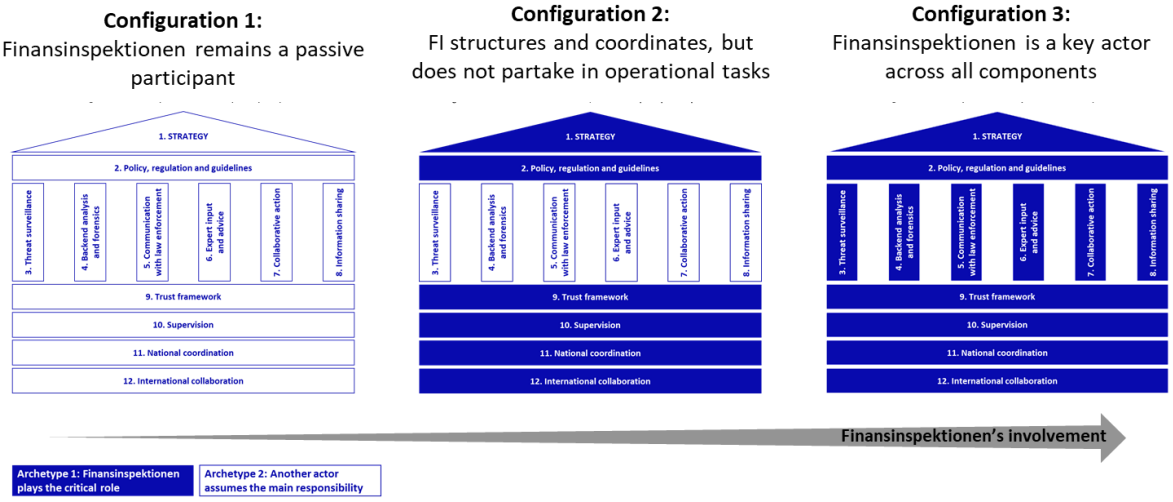
Another actor assumes the role as the point of contact for international authorities.

5. DISCUSSION OF POSSIBLE ARCHETYPE COMBINATIONS

We have defined two archetypes for each of the 13 different ecosystem components, based on the extent of Finansinspektionen's involvement. These archetypes can be characterised on a spectrum ranging from an ecosystem with limited involvement from Finansinspektionen to one where the supervisor is heavily involved across all, or most activities.

Following this logic, we can create several generalised configurations of the ecosystem along this spectrum. Two of these would be at the extremes of the spectrum, namely where Finansinspektionen has no (or a limited) role to play in the ecosystem, as well as where Finansinspektionen is the main actor in the ecosystem.

Figure 6: Generalised ecosystem configurations



In between these extremes, there is a middle ground where Finansinspektionen actively participates in some activities but leaves others to the private sector or other authorities. One could imagine that in one such middle ground, Finansinspektionen would be responsible for the coordination of the cyber risk work but would leave most of the operational work to the private sector or public-private initiatives. Linking this back to the framework, Finansinspektionen would take a larger role in the overarching structuring, involving strategy and regulation. Similarly, it would be responsible for the foundational work, entailing coordination and governance, in addition to its supervisory responsibilities. The operational activities related to cyber risk would be left to other actors.

It should be noted that the more involved Finansinspektionen is in the financial services cyber risk ecosystem, the greater the requirements will be in terms of both resourcing and skills needed. A more involved role will thus also require larger investments to build out capabilities, including, for instance, automation capabilities currently lacking within the organisation, as well as increased management attention on cyber risk. The role of Finansinspektionen in the area of cyber risk is also likely to evolve as the regulatory environment develops, driving the need for a more agile and flexible organisation.

None of these generalised configurations should be considered a recommendation for the Swedish ecosystem going forward, or as being stronger or more appropriate than the others. However, these generalisations allow us to discuss pros and cons of different roles for Finansinspektionen. With a view of the pros and cons of these configurations, Finansinspektionen can start to define where on the scale between them they can provide the most value to the ecosystem.

5.1. Configuration 1

In the first configuration, Finansinspektionen would remain on the sidelines of the cyber risk ecosystem. The configuration would allow Finansinspektionen to remain fully impartial in its role as the supervisor. Without Finansinspektionen taking a larger role in the ecosystem, it would fall upon another actor or group of actors to introduce the recommendations presented in this report.

MSB has to date taken a large responsibility for coordinating the work around cyber risk, and their responsibility could be extended to also cover the additional recommendations from this report. However, and as has been argued in the report, there are benefits to an approach which caters to the specific challenges and needs of the financial sector. MSB has generally applied a "one size fits all" approach to cyber risk, with similar information sharing forums (FIDI forums) and a shared CERT functionality. With deepened collaboration in the financial sector, the approach may have to become more bespoke. More and deeper collaboration would also likely require participants to devote more time and effort to collaborate, which increases the need for the different forms of collaboration to be as efficient and fit-for-purpose as possible.

An alternative to a non-financial authority coordinating the work around cyber risk in the financial sector is that the financial institutions themselves coordinate the work. However, as has been noted previously in this report, there are shortcomings to completely private-run collaboration. For example, private firms may not have access to information from military and law enforcement agencies and there are difficulties with creating financial incentives that ensure collaboration is beneficial and commercially viable both for larger and smaller institutions.

5.2. Configuration 2

In the second configuration, Finansinspektionen involves itself in the coordination and governance of the cyber risk ecosystem in the financial sector but remains passive on the operational work. This is similar to the approach chosen by the Danish FSA. The Danish counterpart coordinates the work in the financial sector through its decentralised cyber security unit (DCIS) and directs the work on a higher level through its cyber security strategy for the financial sector. Much of the shared operational work in Denmark is, however, driven by the local financial institutions through the NFCERT. The Danish FSA does participate in the NFCERT forum, but attempts to recuse itself from the more operational matters in the group in order to protect its impartiality as the supervisor. In Sweden, the operational role could be held by the NFCERT as well, should the Swedish financial institutions see value in joining the cooperation forum. Alternatively, an existing forum could be further built upon for this purpose, such as the Bankföreningen's Security Committee (which is, nevertheless, limited by its explicit focus on the banking sector), FSPOS or MSB's FIDI-FINANS.

This type of configuration would allow for Finansinspektionen to become more involved, while remaining at a sufficient arms-length distance from the operational work. It would also allow a financial authority with relevant sector-specific knowledge to structure and guide the work around cyber risk. Increasing involvement from Finansinspektionen in cyber risk work would also allow the regulator to learn from other participants and thus increase its own capabilities, and in the long-run perform better in its role as supervisor as well.

By being the contact point for information from international peers and organisations, disseminating that information within the Swedish financial sector and then supervising the work performed based on the information, Finansinspektionen can in this configuration ensure better continuity in the cyber risk work.

However, by not partaking in the operational work, Finansinspektionen risks that a disconnect arises between the structure that is laid out in the overarching strategy (which in this case is drafted by Finansinspektionen) and the actual work being done. If there is another authority or similar actor

leading all of, or most of, the operational work, a situation could arise where the delineation in responsibility between the other actor and Finansinspektionen becomes unclear. This would not be an improvement over the current situation and could prove detrimental in the event of a cyber attack.

5.3. Configuration 3

In the final configuration, Finansinspektionen would take the lead across all components of the ecosystem. This would have the benefit of there being one single actor, with relevant knowledge, both structuring, and participating in, the work done around cyber risk. It could also make joint efforts with other sectors and parts of society more efficient as Finansinspektionen would be the interaction partner across the range of components.

However, in interviews, several market participants have expressed hesitation about the prospect of Finansinspektionen getting involved in the operational work. It could be viewed as Finansinspektionen stepping outside of its defined area of responsibility. In Denmark, the expansion of Finanstilsynet's responsibilities for cyber risk did not come as an internal initiative but the Danish counterpart was rather mandated this role by the Government (as were several other authorities in other sectors).

Being too involved in the operational work could potentially also harm Finansinspektionen's legitimacy as the supervisor, as it may become more difficult to provide censure related to initiatives where Finansinspektionen participated. If Finansinspektionen were to take on such broad responsibilities for cyber risk, it could raise questions concerning the extent of its responsibilities for the work of preventing other risk types as well.

To alleviate these concerns, Finansinspektionen could seek mechanisms to provide advisory capacity separate to, and independent from, its supervisory mandate for cyber risk management. This could be done, for instance, by establishing two separate cyber risk arms of Finansinspektionen – one supervisory and one advisory – with clear firewalls and independence structure between the two, similar to what we have observed that certain global authorities have done. The extent to which this would be of interest for Finansinspektionen would depend on, amongst others, its current organisational set up and its ability to secure resources to expand its capabilities.

QUALIFICATIONS, ASSUMPTIONS, AND LIMITING CONDITIONS

Oliver Wyman was commissioned by Finansinspektionen (the Swedish FSA) to summarise, evaluate, and provide an external perspective on the Swedish ecosystem in the financial sector around cyber risk. This includes collaboration opportunities between the public, private and law enforcement to protect the stability of the country. The report draws upon experiences from other jurisdictions and other sectors as well as input from a wide range of interviews conducted across the various authorities and private banks, insurers and market infrastructure providers. The report finally aims to discuss potential future roles for Finansinspektionen in the Swedish ecosystem.

This report is for the exclusive use of the Oliver Wyman client named herein. This report is not intended for general circulation or publication, nor is it to be reproduced, quoted, or distributed for any purpose without the prior written permission of Oliver Wyman. There are no third-party beneficiaries with respect to this report, and Oliver Wyman does not accept any liability to any third party.

Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been independently verified, unless otherwise expressly indicated. Public information and industry and statistical data are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information. The findings contained in this report may contain predictions based on current data and historical trends. Any such predictions are subject to inherent risks and uncertainties. Oliver Wyman accepts no responsibility for actual results or future events.

The opinions expressed in this report are valid only for the purpose stated herein and as of the date of this report. No obligation is assumed to revise this report to reflect changes, events, or conditions, which occur subsequent to the date hereof.

All decisions in connection with the implementation or use of advice or recommendations contained in this report are the sole responsibility of the client. This report does not represent investment advice nor does it provide an opinion regarding the fairness of any transaction to any and all parties. In addition, this report does not represent legal, medical, accounting, safety, or other specialized advice. For any such advice, Oliver Wyman recommends seeking and obtaining advice from a qualified professional.

Martin Andersson
Partner
Email: martin.andersson@oliverwyman.com
Tel: +46 73 317 27 06

Carl Raning
Partner
Email: carl.raning@oliverwyman.com
Tel: +46 70 984 95 88

Michael Heaney
Principal
Email: michael.heaney@oliverwyman.com
Tel: +44 77 48 10 56 79

Paul Lewis
Partner
Email: paul.lewis@oliverwyman.com
Tel: +44 75 84 14 42 22