Chapter 4.

Digital security policy

This chapter provides an overarching description and analysis of digital security policy in Sweden. Sweden's 2017 National Cybersecurity Strategy aims to better integrate digital security policy within the broader digital transformation agenda and marks a positive turning point towards a more holistic approach to digital security.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

This chapter provides an overarching description of digital security policy in Sweden and discusses its strengths and limitations from the perspective of the OECD 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* ("Security Risk Recommendation"). Unless specified otherwise, "digital security" refers to the management of economic and social risks resulting from breaches of availability, integrity and confidentiality (AIC) of information and communication technologies (ICTs) and data. As explained in the first section, some Swedish policy documents are using this expression in a broader manner; other policy documents use other terms such as "cybersecurity" and "information security".

This chapter does not cover policies directly related to criminal law enforcement (i.e. cybercrime) or national security.

Digital security within the Swedish digital strategy

Digital security is not a new policy area in Sweden, but it took a long time to reach a strategic level. The Swedish government expressed interest in digital security policy as early as 2003 by asking a commission of enquiry to make a proposal for an "information security" policy, including recommendations as to how Sweden should implement the 2002 OECD *Guidelines on the Security of Information Systems and Networks*. On the basis of the commission's 2005 report, the Swedish Emergency Management Agency adopted an action plan in 2008 covering information security in organisations, skills, information-sharing collaboration and response, and communication security and security in products and systems (Swedish Emergency Management Agency, 2008). In 2010, the successor of the Emergency Management Agency, the Swedish Civil Contingencies Agency (MSB) developed a Strategy for Information Security 2010-2015 (MSB, 2010) followed by a new action plan in 2012 (MSB, 2012a). Both documents were developed in consultation with the agencies of the Cooperation Group for Information Security (SAMFI) formed in 2003 (further described below). The strategy recognised that "information security is everyone's business" and aimed to provide a common understanding of digital security in the society. However, neither the strategy nor the action plans were adopted by the government: they reflected the views of independent[1] agencies with the highest stakes on digital security.

It was only in 2017 that the first high-level strategic policy documents addressing digital security were adopted by the government: the Digital Strategy for Sustainable Digital Transformation ("Digital Strategy"), which includes a section on digital security, and the National Cybersecurity Strategy, adopted a few weeks later.

The Digital Strategy is a first step towards approaching digital security as a strategic economic and social policy challenge

The overarching objective of the Digital Strategy released in May 2017 is to make Sweden the world leader in harnessing the opportunities of the digital transformation. Digital security is one of the five strategic goals for achieving this objective, together with digital skills, digital innovation, digital leadership and digital infrastructure.

According to the "digital security" strategic goal, Sweden should provide "the best conditions for everyone to safely take part, take responsibility for and trust in digital society". This strategic goal is broken down into six "important areas":

1. **Digital identity**. Although a large part of the Swedish population has an electronic identity (e-ID) (see below), the strategy aims to ensure that everyone in Sweden can use simple and secure digital credentials, including across borders.

2. **High security requirements** to identify and prevent vulnerabilities and handle incidents. This requires awareness of information and cybersecurity and of how to protect information systems. This area, covered by the Network and Information Security Directive (NIS Directive) (European Union, 2016), is addressed in Sweden's 2017 National Cybersecurity Strategy.
3. **Privacy in the digital society**. The use of personal data is often crucial to streamline and develop both public and the private services. However, the right to privacy is essential to maintain confidence, security and trust in the digital environment. Sweden has the potential to lead with respect to privacy-friendly technologies.
4. **Preserving democracy in digital environments**. Opportunities to spread threats, hatred, extremist propaganda and deliberate dissemination of false information increase. Freedom of expression must be given very wide limits. However, strong action is required against criminal acts, whether online or offline.
5. **A secure and mobile labour market**. Digitalisation fundamentally changes the labour market, including the nature of the work and working environment. Close dialogue between the government and social partners to ensure continuous adaptation to social development, in line with the Swedish model, is essential.
6. **Functioning digital markets and secure consumers**. Digital markets must always be a safe and legal place for consumers, businesses and rights owners. Regulatory and supervisory authorities should maintain effective consumer protection and competition on equal terms.

The Digital Strategy uses the term "digital security" differently from the OECD. The "digital security" strategic goal brings together under one umbrella the policy domains that Sweden views as requiring some protection for digital transformation to be sustainable: identities, systems and networks, privacy, democracy, workers, and consumers. Thus the term "security" in this context can be understood as "social security", that is, the part of the social contract that addresses the need for collective protection against uncertainty, such as loss of job (secure workers), scam (secure consumers) or misinformation by foreign influence (secure citizens). In contrast, the OECD defines "digital security" as the management of economic and social risks resulting from breaches of AIC of ICTs and data. Therefore, only two of the six "important areas" listed above relate directly to AIC and the others have a lower degree of relationship with it, from relatively high (privacy protection) to relatively low (secure and mobile labour market).

In fact, the Swedish term used in the strategy for the expression "digital security" is not "*säkerhet*", such as in "*informationssäkerhet*" (information security) or "*cybersäkerhet*" (cybersecurity), but "*trygghet*".[2] The distinction between *säkerhet* and *trygghet* is subtle: English-Swedish dictionaries translate *trygghet* into "security" but the meaning of *trygghet* might be closer to "safety" than "security", in the sense of relating to people, as suggested by the use of "social *trygghet*" to mean "social security".

Despite the unusual use of the term "digital security", which might be a translation artefact, the Swedish strategy's grouping of issues has the merit of considering digital security (in the OECD sense of AIC-related risk) as an economic and social challenge related to the digital transformation. However, it may suggest that the uncertainty created by potential breaches of AIC requires primarily collective solutions analogous to the collective protection provided by the welfare state. In other words, it may imply that digital security does not require action at the individual level because society, through some form of collective protection, will take care of it. This would be inconsistent with the principle that all stakeholders should take responsibility for the management of digital security risk, according to their role, ability to act and the context, formulated in the OECD 2015 Security Risk Recommendation.

The fact that these documents do not use the terms "digital security" in the same manner as the OECD is not an issue: many countries use different terms to refer to this area. However, the apparent terminological inconsistencies across Swedish policy documents are more troubling. In particular, the differences between the overall "digital security" goal ("digital *trygghet*"), the notions of "high security requirements" ("*Höga krav på säkerhet*") as one of this goal's important areas, and of "information and cyber security" ("*informations- och cybersäkerhet*") as used in the title of the national cybersecurity strategy (see below) are indeed relatively unclear to the non-expert.

One way to clarify the "digital security" strategic goal of Sweden's Digital Strategy would be to call it "digital trust", which would be consistent with all the "important areas" it covers. The title "higher security requirements" important area could be aligned with the title of the National Cybersecurity Strategy, i.e. "information and cybersecurity", or it could be changed to "digital security", if consistency with the OECD is sought.

The "high security requirement" important area of the "digital security" strategic goal is addressed in more detail in Sweden's "National Strategy for the Society's Information and Cyber Security", translated as the "National Cybersecurity Strategy", which was adopted one month after the Digital Strategy, suggesting that both strategies have been developed in parallel and through relatively separate tracks rather than in full synergy, which may explain terminological misalignments.

In sum, the inclusion of digital security (as understood by the OECD) in the Digital Strategy seems to indicate that Sweden has made a first step towards approaching digital security as an economic and social issue. Sweden has, however, not yet developed a clear vision of what this means and implies, nor of how digital security fits within the broader framework of the digital transformation. Terminological inconsistencies reveal more than branding issues. They suggest that Sweden understands many aspects of digital security but addresses them as separate pieces rather than through an integrated and holistic approach (Box 4.1). The Digital Strategy represents a first step towards bringing together the different dimensions of digital security, but further work is needed to devise a truly holistic and unified vision.

Nevertheless, with this first effort to bring digital security to the strategic level, Sweden is likely to be in a situation similar to that of other countries whose first strategy was a necessary first step to develop a real high-level holistic vision a few years later (e.g. Australia, Canada, France, the Netherlands and the United Kingdom). The Netherlands, for example, adopted a "National Cyber Security Strategy 2" in 2013 only two years after the first version. It took other countries a few more years to update their frameworks. In all cases, the second strategy was always much more sophisticated, visionary and holistic than the initial one which, *a posteriori*, looked like a necessary stage in a learning curve towards more strategic thinking.

While Sweden started late in this process, it aims at integrating digital security within a strategy for the digital transformation of Sweden. This is more challenging conceptually and from a governmental co-ordination perspective, but it also has more potential for effectively integrating the economic and social dimension of digital security into the fabric of the digital transformation.

Box 4.1. **Digital security, cybersecurity, information security, cyberdefence, cybercrime: The need to simplify terminology**

The multiplication of terms related to digital security in Swedish policy documents is an illustration of a maturing policy-making process. Sweden is not the only country in this situation as, unfortunately, there is no universally agreed terminology to capture the different facets of digital security in every context.

In its 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity*, the OECD uses the term "digital security" rather than "cybersecurity". OECD countries considered that "cybersecurity" was already used by different actors as a broad concept that did not reflect the multifaceted nature of this area. More generally, they favoured "digital" over "cyber" as the latter was used in certain circles as a synonym of "cyberwarfare", "cyberdefence" or "cyberinfluence". Furthermore, "cyber" is absent from economic circles, which more generally stick to the digital semantic: digital economy, digital transformation, digitalisation, etc. "Digital" facilitates the recognition of "digital security" as an economic issue by policy makers and business leaders. "Information security" was left aside as a technical management primarily reflecting the view of the technical community (e.g. ISO/IEC 27000 "Information Security Management Systems" standards) rather than business leadership's perspective. It also carries ambiguity in an international context as it has a different scope in countries such as the People's Republic of China and the Russian Federation, which use it also to capture policies against disinformation, influence and information manipulation.

The National Cybersecurity Strategy is focused on information systems and networks rather than economic and social activities

The development and adoption of the National Cybersecurity Strategy follow a series of audit reports by the National Audit Office, which concluded that digital security efforts in several government agencies "fell considerably short of being adequate" (NAO, 2016a; 2016b). The strategy also follows the development of a report by a commission of enquiry which developed proposals for a new digital security strategy focusing on government activities (Government Offices of Sweden, 2015). However, the strategy is broader and aims to: i) "create the long-term conditions for all stakeholders in society to work effectively on digital security"; ii) "raise the level of awareness and knowledge throughout society".

The National Cybersecurity Strategy is based on both the National Security Strategy's objectives of protecting the lives and health of the population, the functioning of society, and the capacity to uphold fundamental values and the Digital Strategy's objectives of becoming the world leader in harnessing the opportunities of the digital transformation. It covers six strategic priorities: i) ensuring a systematic and comprehensive approach in cybersecurity efforts; ii) enhancing network, product and system security; iii) enhancing capability to prevent, detect, and manage cyberattacks and other information technology (IT) incidents; iv) increasing the possibility of preventing and combating cybercrime; v) increasing knowledge and promoting expertise; and vi) enhancing international co-operation.

The scope of the National Cybersecurity Strategy carries some ambiguity. The strategy defines cybersecurity as the set of security measures to preserve the availability, integrity[3] and confidentiality of information. However, the strategy also addresses disinformation and influence campaigns, including to "intentionally disseminate untrue or misleading details in order to influence people's attitudes, standpoints and actions in a certain direction". Disinformation and influence are important issues exacerbated by the digital transformation and can sometimes overlap with digital security, for example when digital security attacks are used to manipulate public opinion. They are, however, different from the management of the economic and social consequences of breaches of AIC, as they involve different policy tools and raise different legal considerations related to freedom of speech, media regulation, etc. Furthermore, the fact that they are addressed in the National Cybersecurity Strategy seems inconsistent with the Digital Strategy, in which disinformation is addressed within the digital security ("*trygghet*") strategic goal, but as a different "important area" related to the "preservation of democracy in digital environments". These inconsistencies suggest that both strategies are not entirely integrated.

Analysis of the National Cybersecurity Strategy confirms that Sweden has not yet developed a clear vision of how digital security fits within the broader economic and social policy framework of the digital transformation. Indeed, the National Cybersecurity Strategy primarily considers digital security from the perspective of ICTs, i.e. focusing on a risk to information systems and networks rather than the economic and social activities that rely on them. This approach is consistent with the 2002 OECD *Guidelines for the Security of Information Systems and Networks* ("Security Guidelines") but not with the *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* that replaced them in 2015. It is essential to understand the difference between these two approaches.

Since the early days of computing and until relatively recently, most stakeholders, including policy makers, approached digital security primarily as a technical issue: they focused on security risk to systems and networks, and so did the OECD with its 2002 *Guidelines for the Security of Information Systems and Networks*. This approach to digital security, which includes technical, human and management aspects, led governments and organisations to increase digital security efforts. In public policy, for example, governments established and strengthened the capacity to respond to digital security incidents through computer emergency response teams (CERTs). They also increased stakeholders' awareness about technical digital security risks (phishing, malware, hackers, identity theft, etc.) and encouraged organisations to adopt standards such as the ISO/IEC 27000 family, a path followed by Sweden.

Progressively however, most economic and social activities have become digital or digital-dependent "by design" and, in parallel, risks continue to increase, elevating the importance of digital security within organisations and at the public policy level. As losses from digital security incidents have become more common, stakeholders' attention has shifted from the technical incidents such as denial of service attacks, ransomware, or personal data breaches to their economic and social consequences to financial and reputational losses, loss of business opportunities and reduced competitiveness resulting from theft of innovation and trade secrets, privacy impact and loss of trust, as well as in some cases, physical assets destruction and, tomorrow, possibly loss of lives (Box 4.2).

In addition, stakeholders have also realised that the security measures put in place to reduce digital security risk can have negative effects on the economic and social activities they are expected to protect: in addition to their financial cost, they can close the digital environment and reduce its dynamism, limiting the opportunities to use ICTs for innovation; they can also increase time-to-market, lower performance and user-friendliness, etc.

While recognising the continued importance of the security of information systems and networks, organisations realised that digital security risk management should primarily focus on economic and social activities rather than on the digital environment that supports them, and that, as a result, it should be led by organisations' business leadership with the support of technical experts rather than the reverse. Managers in charge of realising the economic and social benefits of the digital environment are better placed than technical experts to set the acceptable level of economic and social risk for the organisation (i.e. its "risk appetite") and to assess the consequences of digital security risk on economic and social objectives they have the responsibility to achieve. They are also in a better position to ensure that security measures do not reduce the potential of ICTs to innovate and contribute to competitiveness. But these managers rely on technical experts to understand the risk factors (possible threats, vulnerabilities and incidents) and the options to reduce the risk (i.e. technical security and business continuity measures). Both have to work together, but risk-related decisions and responsibility should be owned by business decision makers and not delegated to technical experts. In fact, risk management should be an integral part of business decision making rather than a separate area. Digital security risk management is no exception.

Box 4.2. **Examples of economic and social consequences of digital security incidents**

Since robust quantitative data on the cost of digital security incidents are unavailable, policy makers most often rely on anecdotal evidence, which is also rare as most companies do not communicate on the business impact of digital security attacks so as to protect their image. However, the damages from the June 2017 Wannacry and NotPetya ransomware attacks which hit many public and private organisations globally were so high that several publicly traded companies had to disclose financial information as part of their financial transparency obligations requirement. In most cases, the economic consequences were much more important than the technical ICT damages:

- Danish transports and logistics company AP Moller-Maersk: estimated USD 200-300 million losses from business interruption (Palmer, 2017).
- French industrial company Saint-Gobain: EUR 250 million net sales losses and EUR 80 million operating income losses for 2017 (Saint-Gobain, 2017).
- US pharmaceutical company Merck: USD 135 million sales losses and USD 175 million operational expenses for the 3rd quarter 2017, and a similar impact to revenue and expenses expected for the 4th quarter. The temporary production shutdown caused by the attack and higher-than-expected demand at that time forced the company to borrow doses of its Gardasil 9 vaccine from US Centers for Disease Control and Prevention stockpile to fulfil customer orders, reducing the company's 3rd quarter sales by USD 240 million (Merck, 2017; Hufford, 2017).

These examples could be completed by others such as the dismissal of the US retail company Target Store's chief executive officer following a digital security attack in 2014 (Rushe, 2014), or the December 2015 temporary blackout in Ukraine following a sophisticated attack on the country's power grid (Zetter, 2016b). In 2015, an attack reported by the German Federal Office for Security in Information Technology caused "massive" physical damages in a German steel mill (Zetter, 2016a).

Sources: Hufford (2017), "Merck swings to loss as cyberattack hurts sales", MarketWatch, 27 October, www.marketwatch.com/story/merck-swings-to-loss-as-cyberattack-hurts-sales-2017-10-27-134853159; Merck (2017), "Merck announces second-quarter 2017 financial results", www.mrknewsroom.com/news-release/corporate-news/merck-announces-second-quarter-2017-financial-results; Palmer (2017), "Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk", www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk; Rushe (2014), "Target CEO Gregg Steinhafel resigns in wake of customer data breach", www.theguardian.com/business/2014/may/05/target-chief-executive-steps-down-data-breach; Saint-Gobain (2017), "Résultats du 1er semestre 2017", www.saint-gobain.com/sites/sgcom.master/files/cp_vf_resultats_s1_2017_t.pdf; Zetter (2016a), "A cyberattack has caused confirmed physical damage for the second time ever", https://www.wired.com/2015/01/german-steel-mill-hack-destruction; Zetter (2016b), "Inside the cunning, unprecedented hack of Ukraine's power grid", www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

Digital security, which used to be primarily owned by technical experts, should therefore become a business management responsibility. The replacement of the OECD 2002 *Guidelines for the Security of Information Systems and Networks* by the 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* reflects this evolution at the policy level. This evolution from the security of information systems to the management of digital security risk to economic and social activities is a shift in responsibility which aims to ensure that the assessment and management of opportunities and risks are in the same hands, because they are two sides of the same coin. It implies that organisations' leaders should be responsible for managing digital security risk as much as they are responsible for managing the opportunities offered by the digital technologies. Ultimately, digital security risk is simply one risk among many that business decision makers must own and manage and cannot entirely delegate to technical experts.

An incident in 2017 illustrated the shortcomings of the current approach (Box 4.3). This incident followed others which contributed to raising digital security awareness among the population and the political leadership, such as large co-ordinated denial of service attacks on 20 March 2016 which shut down several national and regional media outlets' websites for at least one hour (Sverige Radio, 2016).

Box 4.3. **A digital security risk management failure at the Transport Agency**

In July 2017, a newspaper revealed that unauthorised personnel at IBM subsidiaries in Eastern Europe had access to a very large amount of sensitive data as a result of a 2015 outsourcing agreement with the Swedish Transport Agency for the management of vehicle registration and driver's license databases.

A large amount of personal data about Swedish people including the identities of persons working undercover for the police, the security service and the special intelligence unit of the Swedish armed forces, along with details about bridges, roads, ports, the Stockholm subway system and other infrastructures had been exposed (Anderson, 2017). This incident was reported by the press as one of the largest government data breaches in Sweden (The Local, 2017).

Following investigations by the parliament, it appeared that the Director General of the Transports Agency had knowingly bypassed the legal security compliance requirements in an attempt to speed up the outsourcing process. After the publication of this information by the press, this digital security incident turned into a political crisis as the prime minister reshuffled the Cabinet, dismissing the Minister for Infrastructures, responsible for the Transport Agency, and receiving the resignation of the Minister of the Interior, who apparently had been informed about the issue but did not inform the prime minister.

Over the summer parliamentary break, an opposition alliance threatened to launch a no-confidence motion in the parliament against the Minister of Defence, potentially leading to a serious government crisis. Ultimately, the motion failed, but parliamentary investigations were still ongoing at the time of writing.

These incidents followed the 2014 and 2016 National Audit Office reviews of many public sector institutions which underlined "extensive shortcomings" (NAO, 2014) and a level of digital security efforts that "fell considerably short of being adequate", and was "not acceptable" (NAO, 2016a).

Sources: Anderson (2017), "Swedish government scrambles to contain damage from data breach", www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html; NAO (2014), "Information security in the civil public administration", https://www.riksrevisionen.se/en/audit-reports/audit-reports/2014/information-security-in-the-civil-public-administration.html; NAO (2016a), "Information security work at nine agencies", www.riksrevisionen.se/en/audit-reports/audit-reports/2016/information-security-work-at-nine-agencies.html; The Local (2017), "Swedish government battles political fallout from transport data leak", www.thelocal.se/20170725/swedish-government-battles-political-fallout-from-transport-data-leak.

Instead of chief executive officers, director generals, board members and business line managers, the approach followed by the 2002 OECD Guidelines and by the 2017 Swedish National Cybersecurity Strategy leads to responsibility for managing digital security risk being owned by those who maintain and operate the digital environment, i.e. chief information officers, chief technology officers, etc. To realise the benefits of the digital transformation, business leaders and decision makers need to undertake a double-sided cultural shift: i) rethink all aspects of their business activities to understand the innovation opportunities that data and digital technologies can unleash to increase their competitiveness, improve their service and grow; and at the same time ii) understand and manage the risk inherently related to digitalising their activities. A leader who does not own, understand and manage the risk related to his/her digital decision is blindly taking it, jeopardising its entire business because digital security risk can quickly contaminate all of the organisation's lines of activities by propagating through networks.

When business decision makers manage both the socio-economic opportunities and the digital security risk related to the use of ICTs, security measures can be appropriately tailored to the economic and social activities of the organisation and viewed as a strategic asset, part of a profit centre, rather than only as a cost centre. Security risk management and security measures can also be integrated into business models and the design of products and services rather than being addressed is isolation, or as an afterthought. In this way they can be turned into a market advantage and contribute to increasing competitiveness. Digital security becomes a driver for innovation, no longer a burden and a constraint.

The economic and social risk management approach promoted by the OECD Security Risk Recommendation is missing from the Swedish National Cybersecurity Strategy. The National Audit Office audit reports include some findings which illustrate a situation in government agencies typical of a digital security approach severed from business decision makers because it is focused primarily on information systems and networks.

For example, the reports note that agencies' leadership, when aware of the digital security risk, has often delegated responsibility to technical staff who do not have the ability to act: government "agency managements have delegated responsibility for information security without ensuring that those responsible have an adequate mandate to carry out their tasks"; "the functions in charge of information security find it hard to contend with core activities that tend to see information security requirements as obstacles"; "it is the IT or security functions that impose security requirements rather than the core organisation"; "the core organisation does not perceive that it has any responsibility for information security, but that this lies somewhere else in the agency, such as the IT or security functions".

The findings of surveys carried out by the MSB and the Swedish Association of Local Authorities and Regions (SKL in Swedish) in 2015 highlight a similar situation, where digital security efforts are disconnected from the leadership of municipalities and are not integrated in their decision making and broader risk management (Box 4.4).

The OECD is currently working to develop comparable indicators to measure digital security risk management practice in businesses. Currently, the lack of such indicators, which is not specific to Sweden, prevents from understanding the extent to which the lack of economic and social digital security risk management is limited to the public administration or cuts across all organisations in Sweden. Nevertheless, the strong focus of the National Cybersecurity Strategy on technical aspects suggests that this is a common issue.

The evolution from a technical to an economic and social digital security risk management approach does not mean that all the efforts accomplished by Sweden over the last 15 years were not useful and should be discontinued. Rather, they form an excellent foundation on which Sweden can lay additional building blocks to strengthen trust and lead in the digital transformation.

Box 4.4. **Digital security efforts in municipalities**

In 2015, the SKL released aggregated results from the use of a self-assessment tool by 70% of Swedish municipalities and 16 of the 21 Swedish county councils. The same year, 255 out of the 290 Swedish municipalities responded to a questionnaire circulated by the MSB in co-operation with the SKL. They showed that in 2014 (SKL) and 2015 (MSB):

- Municipalities had increasingly focused on the introduction of digital platforms and citizen-oriented services, in comparison with 2012. However, attention to digital security had fallen for most of them and three out of four municipalities still did limited work in this area (SKL).
- While 42% of municipalities' management manifested visible support for digital security efforts, management received systematic reporting on compliance with digital security objectives in only 10% of municipalities (SKL).
- Less than half of the municipalities surveyed had conducted a digital security risk analysis that is consistent with the organisation's other risk management activities, and nine out of ten municipalities had not established criteria for acceptable risk (SKL). Similarly, 41% of municipalities perform a digital security risk assessment, 63% of which do so irregularly (MSB).
- Only three out of ten municipalities had a systematic digital security approach. Forty-one per cent had not designated a digital security function, and for 47% of those that did, the person in charge spent less than 10% of his/her time on digital security. Seventy-one per cent said they did not have enough time to work on digital security (MSB). Only 14% of municipalities had a full-time person or more dedicated to digital security.
- Between half (SKL) and 70% (MSB) of municipalities had adopted a digital security strategy or policy, 25% had created a steering group in this area (SKL). However, 60% had not started to assess risks related to digital services (SKL) and 60% did not monitor compliance and most of those that had done it did so only after incidents had occurred (MSB).
- Between one-third (SKL) and 40% (MSB) of municipalities had a business continuity or contingency plan, leaving two-thirds without assurance that digital service would be available in the event of major operational problem. Existing plans are generally never or only occasionally tested (MSB).
- Only 4% of municipalities had allocated funds to increase the digital security awareness of employees, and 90% had not taken any initiative in this area. Only 5% of municipalities had measured staff's digital security skills. A quarter of municipalities had adopted a framework for digital security training for staff, from one-fifth in 2012 (SKL).

The MSB found no clear correlation between the number of inhabitants per municipality and how well municipal digital security was carried out. There were also no major geographical differences across the results.

Sources: SKL (2015a), "Nordiskt samarbete om informationssäkerhet i kommuner, landsting och regioner promemoria om informationssäkerhet och digitalisering svenska kommuner", https://skl.se/download/18.1ea1a4111513965b0179e6d/1448536942895/NordSec_Rapport%20Svenska%20kommuner%202015.pdf; SKL (2015b), "Nordiskt samarbete om informationssäkerhet i kommuner, landsting och regioner promemoria om informationssäkerhet och digitalisering svenska kommuner 2015", https://skl.se/download/18.1ea1a4111513965b0179e6c/1448536925762/NordSec-Rapport%20Svenska%20Landsting%20och%20Regioner%202015.pdf.

Nevertheless, digitalisation and data-driven innovation, the growing use of artificial intelligence (AI), and reliance on the Internet of Things (IoT) will considerably expand all stakeholders' exposure to digital security risks. As the digital transformation affects all sectors and all stages of value chains, it will increase all stakeholders' digital reliance and exacerbate the need to systematically integrate digital security risk management in every economic and operational decision that implies ICT use.

Concretely, the digital transformation blurs the distinction between ICT-related activities and non-ICT related activities, as illustrated by automated vehicles or smart grids. Digital technologies and data will be at the core of most activities and decision makers will have to understand the risks of using big data, AI, blockchain and other technologies to increase competitiveness, productivity, innovation, etc. It will become hazardous for a decision maker to entirely delegate the security risk to a technical expert who is not responsible for realising the benefits of using ICTs, or to manage the security risk without being informed by these experts in order to take the most appropriate decisions.

This requires a cultural shift whereby the government, as well as economic and social decision makers in public and private organisations, and ultimately all individuals in Sweden, understand and manage the digital security risk of using ICTs just as well as they understand and manage the benefits of digital technologies. From this perspective, digital security risk management not only aims to protect assets, it also aims to increase the likelihood of success, it is part of economic and social decision making as it helps decision makers to take informed choices, prioritise actions and distinguish among alternative courses of action (ISO/IEC, 2009; OECD, 2015).

This cultural shift is likely to take time and, to make progress, the government should set priorities. A good starting point would be to formulate a vision of digital security for prosperity in Sweden and promote it throughout the country, with perhaps economic and social decision makers in public and private organisations as primary target audiences.

Digital security public policies and stakeholders

Digital security in Sweden is addressed by several government bodies in line with their respective mandate. As a general rule, each ministry, government agency, county council and municipality is responsible for addressing digital security in its areas of competence.

Sweden's digital security policy places a major emphasis on crisis management preparedness (also called critical infrastructure protection). As a result, the Ministry of Justice (MoJ), the MSB and the Post and Telecommunications Agency (PTS) play a key role discussed in the first section below. The next section discusses how the implementation of the NIS Directive in Sweden will change the digital security policy landscape. The following section describes other initiatives unrelated to crisis management preparedness, including by the Swedish e-Identification Board, Vinnova and the Swedish Foundation for Strategic Research as well as by the SKL.[4] Digital security activities of municipalities and county councils are important to consider since local self-governments are responsible for the largest operational part of the Swedish welfare state, including for health and education. Finally, the section discusses the overarching governance of digital security from an economic and social perspective in Sweden.

Other government agencies addressing digital security in Sweden focus more exclusively on national security, an area which is beyond the scope of this report. They include the armed forces, the National Defence Radio Establishment, the Swedish Certification Body for IT Security and the Swedish Security Service. For example, since 2014, the military intelligence, security service and defence radio establishment have set up the national Co-operation for Protection against Serious IT Threats in order to analyse and assess digital threats and vulnerabilities related to Sweden's most security-sensitive national interests.

A strong focus on crisis preparedness and the protection of critical infrastructures

Digital security policy in Sweden started as a crisis management and preparedness matter, considered in Sweden as the civilian side of a national defence and security framework. As a result, the most important bodies in charge of digital security policy development and implementation are the MoJ and the MSB. The MoJ defines the high-level policy and prepares legislation; the MSB implements the policy by providing overall support to the society. However, each sectoral agency is responsible for digital security policy in its area of competence. The PTS is the most advanced example. Other sectoral agencies have a limited focus on digital security, but this is likely to change with the implementation of the NIS Directive in Sweden (see next section).

The Ministry of Justice defines digital security crisis management preparedness policy and co-ordinates the development of digital security policy more generally

The MoJ is the main ministry in charge of digital security policy in Sweden. It is responsible for developing digital security policies related to the continuous functioning of society, the prevention of major incidents and the management of crisis preparedness. This role fits within its broader mission in the area of crisis preparedness. The MoJ is responsible for the MSB whose role and activities are described below.

In accordance with the Swedish Constitution, the MoJ's influence over agencies is primarily a matter of co-operation and collaboration with other ministries as the MoJ cannot directly instruct a government agency within another ministry's remit. For example, if the MoJ identifies the need for the telecommunications regulator (the PTS) to enhance its digital security, it needs to first contact the PTS' parent ministry, the Ministry of Entreprise and Innovation, to explore whether a new instruction setting a new target for the PTS should be developed and what it should contain.

The MoJ does not address digital security policy in specific areas covered by other ministries. For example, it does not address digital security for economic and social prosperity, which would fall under the umbrella of the Ministry of Entreprise and Innovation, or digital security-related education, which would be a matter for the Ministry of Education and Research. However, an interdepartmental working group has been set up with several ministries including Enterprise and Innovation, Defense and Foreign Affairs. The group discusses overall digital security issues to achieving equal policy direction in the area of digital security regardless of the departments' responsibilities.

Nevertheless, the MoJ is in charge of developing digital security policy for the Swedish society as a whole and monitoring digital security-related developments. For example, it co-ordinated the development of the 2017 National Cybersecurity Strategy.

Lastly, the MoJ also has a "catch-all" role for digital security in Sweden: it can address all issues pertaining to digital security which do not fall within the responsibility of another ministry.

Like other Swedish ministries, the MoJ is a light structure of 400 civil servants which focuses on public policy making and monitoring. As of May 2018, digital security policy is managed by four full-time and two part-time persons within the MoJ Division for Crisis Preparedness, which is responsible for co-ordination and development for strengthening and monitoring society's emergency preparedness and civil defence (approximately 20 persons). This does not include cybercrime policy, which is addressed by another division.

The MoJ has responsibility for 20 government agencies, from the Swedish police to the prison and probation service. Four of them have a role with respect to digital security: the MSB; the Swedish police authority, which addresses cybercrime law enforcement investigations; the Swedish Security Service (SÄPO), which prevents and detects offences against national security, fights terrorism and protects the central government; and the Data Protection Agency (Datainspektionen).

The Civil Contingencies Agency supports society regarding digital security

The MSB is the main agency with respect to digital security. Overall, it is responsible for issues concerning civil protection, public safety, emergency management and civil defence as long as no other authority has responsibility. This responsibility covers measures taken before, during and after an emergency or crisis.

With respect to digital security, the MSB supports and co-ordinates the digital security efforts in the society and analyses developments in the area. This includes providing advice and support regarding systematic and risk-based digital security to other government agencies, municipalities and businesses. The MSB reports to the MoJ on digital security issues that may require action at different levels and areas of society. The MoJ analyses this information to provide advice to other ministries.

The MSB operates CERT-SE, the Swedish National Computer Security Incident Response Team (CSIRT). As the national CSIRT, CERT-SE addresses government bodies as well as regional authorities, municipalities and businesses (MSB, 2011). It monitors digital security threats and vulnerabilities, disseminates information and warnings, responds to incidents, and participates in efforts to mitigate their consequences. CERT-SE is member of regional and international networks, such as the European Governmental CERTs, the EU CSIRTs Network, TF-CSIRT, and the international Forum of Incident Response and Security Teams (FIRST). Since 2016, a regulation from the MoJ requires government agencies to report serious digital security incidents to the MSB (CERT-SE, 2017). Two hundred fifty incident reports were received in 2016 and 310 reports in 2017. CERT-SE was founded in 2003 at the PTS as the Swedish IT Incident Center, prior to being renamed and transferred to the MSB in 2011. Its staff is increasing, from approximately 20 to 30 people in 2018.

CERT-SE is the only part of the MSB which has operational (i.e. technical) digital security capacity. For its other activities, the MSB acts as a co-ordinator and adviser for other government agencies, municipalities and county councils, as well as companies and organisations, in order to help them meet the standard set by the government. This includes the support and/or co-ordination of several cross-sectoral and sectoral fora and groups as well as the development and publication of various types of guidance information.

Cross-sectoral groups chaired by the MSB include:

- The Cooperation Group on Information Security, which, since 2003, gathers government agencies with a role in information security: the armed forces, Defence Materiel Administration (certification body), Defense Radio Establishment, the telecommunications regulator (PTS), Police Authority and the Security Service. SAMFI meets six times a year to co-operate and exchange digital security-related information, including through specialised working groups. It discusses strategy and regulations, technical questions and standardisation issues, national and international developments in information security, information activities, exercises and education, as well as management and prevention of incidents (MSB, 2014b).

- The Information Security Council (Informationssäkerhetsråd), which gathers since 2009 representatives of significant parts of the public administration, academia, municipalities and industry. The council is the main body that connects the MSB with non-governmental stakeholders. It provides the MSB with information about digital security trends, makes suggestions about its work and helps disseminate information to the rest of society. The MSB's Director General chairs the council, which meets 4 times a year and gathers a maximum of 15 people in their personal expert capacity. Affiliations of members in 2014 included a mix of government agencies (e.g. police, defense, intelligence, regulators), municipality/county councils, university, public and private companies, and the Internet Infrastructure Foundation (IIS).
- Sectoral fora on information sharing in healthcare services, the financial sector and the telecom sector. The MSB also chairs the Media Preparedness Council, the Swedish CERT Forum, the Swedish IT Security Network for PhD Students (SWITS, a research network for PhD students studying in fields related to IT security), the Forum on Information Sharing in SCADA Systems, and the National Centre for Security in Industrial Control Systems (Oehme, 2015).

Unlike broad public-private partnership initiatives such as the British Cybersecurity Information Sharing Partnership or the German UP Kritis, which bring together a wide spectrum of actors involved in digital security across critical sectors, the MSB's co-ordination activities are focused on some key actors. This is, however, likely to evolve with the implementation of the NIS Directive (see below).

The MSB publishes free guides and recommendations regarding systemic and risk-based digital security covering many areas, such as industrial control systems, information security training, toolboxes to organisations, digital security exercises, guidelines for classification modelling, procurement recommendations, guidance for start-ups, etc.[5] It also maintains a website aimed at public sector bodies, companies and non-governmental organisations which gathers methodological and practical information, tools and factsheets about how to systematically manage digital security risk (informationssakerhet.se). This site is a result of the co-operation between the agencies involved in SAMFI. The MSB also carries out awareness-raising initiatives, including in the context of the EU cybersecurity awareness month. It has also allocated research funds, for example to finance a study on the cost of cybersecurity.

The MSB can also issue digital security regulations for government authorities (MSB, 2012b). One example is the 2016 "Regulation about digital security in government agencies" (MSB, 2016), which updates a 2009 regulation and requires government agencies to manage digital security taking into account standards such as ISO/IEC 27001 and 27002, including with respect to risk assessment and business continuity planning. This regulation follows up on reports by the National Audit Office highlighting numerous cases of non-compliance, a survey by the MSB of agencies' digital security (MSB, 2014a) and a 2015 report on "Information and cyber security in Sweden" (Government Offices of Sweden, 2015).

The MSB organises digital security exercises on a regular basis for organisations in essential sectors. The exercise in February 2018 included sectors within the framework of the NIS Directive and the theme was co-operation activities, situational awareness and analysis of consequences.

The MSB's mandate extends beyond the protection of critical infrastructure to support every part of the society. For example, the MSB has issued guidelines for start-ups and small businesses, and provides an e-learning tool on digital security for employees. It also supports research and funds university projects, for instance within the area of economic aspects of threats and incidents. Lastly, the MSB co-ordinates civilian authorities' efforts related to cryptography.

Digital security work at the MSB is carried out by four units: CERT-SE, systematic information security (guidance), analysis and strategic aspects, and critical information infrastructure protection.

Digital security crisis management preparedness in the telecommunications sector is advanced

Other government bodies are responsible for developing and implementing digital security policy in their area of competence and the MSB provides them with support, primarily in relation to crisis management preparedness. This is, for example, the case in the telecommunications sector, under the responsibility of the PTS, which reports to the Ministry of Enterprise and Innovation. Around 20 people are involved in digital security matters at the PTS, including 6 technical staff.

The PTS carries out a number of public-private digital security-related activities to foster higher network security robustness (PTS, 2015). These activities are partially funded by a fee paid by the largest operators (SEK 100 million, or EUR 10 million). The National Telecommunications Coordination Group (NTCG) is an important tool to best manage the funds collected through this fee. The NTCG was created in 2005 as a voluntary co-operation forum to support the restoration of national infrastructures of electronic communications during extraordinary events. Chaired by the PTS, it consists of the ten largest telecommunications operators and Internet service providers (ISPs), the leading distributor of radio and television, the national power grid operator (backbone), the Swedish Transport Agency, and the armed forces. Initially built as a facilitation group with a crisis management focus, it became a venue to also explore how to best manage the funds collected from the operators' annual fee by identifying the most useful initiatives. As a gathering of trusted partners, the NTCG is also the interface with market operators where more sensitive security-related issues are discussed, and sensitive information is shared. It is also a means to preview and discuss secondary legislation prior to its adoption.

The PTS' digital security activities include:

- The "Education and training strategy for crisis preparedness 2017-2021" (PTS, 2017), which includes sectoral and cross-sectoral crisis management training courses for companies, in partnership with other agencies (e.g. energy sector). It also includes exercises for business executives, crisis management and communications staff in the electronic communications sector. So-called "Telö" exercises are carried out every other year to increase the telecommunications sector's preparedness and ability to support the armed forces and civilians in the event of a crisis.

- A system to facilitate the standardised exchange of operational information between electronic communication actors about disturbances caused by emergency or planned interruptions (DIO) (PTS, 2013).

- A free online platform (Ledningskollen)[6] that matches queries from anyone who is planning excavation work with the relevant cable and pipe owners at a particular location in order to reduce the risk of excavation damage. The platform also lowers cable indication costs for cable and pipe owners and improves co-ordinated digging opportunities. The participation of pipe and cable owners is voluntary. This service has been operational since 2011 across Sweden as a result of a co-operation between the PTS, the state-owned electricity transmission monitoring company Svenska Kraftnät and the Swedish Transport Agency.

- Initial support for the industry programme "Robust Fiber" that aims to create a standard for how a fibre network should be deployed to be robust and reliable. Robust Fiber provides instructions for minimum robustness requirements, certification as well as professional degrees and diplomas.[7]
- Activities to foster the adoption of Domain Name System Security Extensions (DNSSEC) in municipalities and counties in partnership with the IIS. Box 4.5 provides more details about the IIS' DNSSEC initiatives. The .se zone was the first DNSSEC signed top-level domain (TLD) in 2005, and since then the number of signed domains in Sweden has significantly increased thanks to a financial incentive provided by the IIS to registrars (Figure 4.1). The percentage of DNSSEC validated queries in Sweden is one of the three largest in the world, which means that users of .se domains enjoy a high protection against attacks based on forged Domain Name System data, such as Domain Name System (DNS) cache poisoning (Figure 4.2).

Box 4.5. **Domain Name System Security Extensions in Sweden**

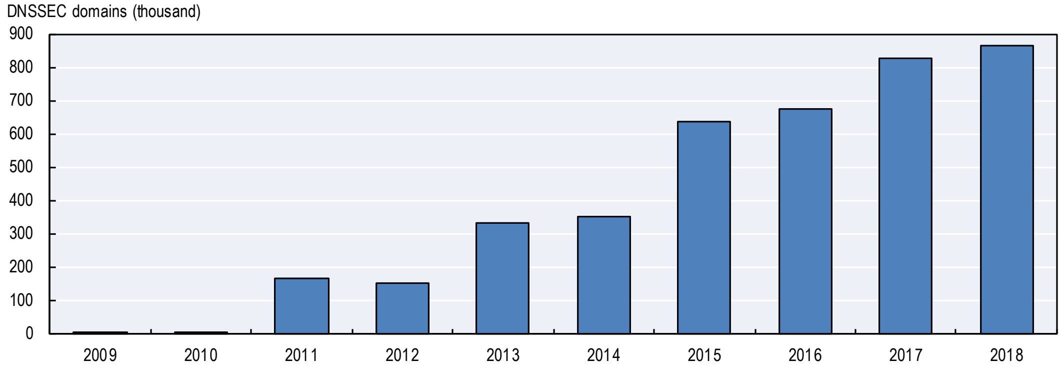
Sweden is one of the leading countries for the adoption of the DNSSEC, a technical protocol that strengthens the security of the DNS. This is the result of an effort led by the Swedish registry responsible for the .se TLD, the IIS and was supported by the government.

With the DNSSEC, users can check that DNS information is correct and was not modified, i.e. that they are communicating with the correct remote system (e.g. website). This requires, however, that domain names are digitally signed in the first place. The IIS was the first registry in the world to sign its TLD (.se) with the DNSSEC (2005) and to offer a complete DNSSEC service (2007). It then convinced important Swedish Internet users such as public authorities, banks, municipalities and counties to sign their domains. It also convinced the largest Swedish ISPs to turn on signature validation on their name servers.

The Post and Telecommunications Agency and the MSB contributed to financing, training and implementing the DNSSEC in municipalities' information systems. Out of 290 municipalities, 231 were granted a total of SEK 10 million (EUR 1 million) to introduce the DNSSEC in 2012-14. The IIS offered a testing tool for municipalities to see on a map which DNSSEC implementation is active, works as expected or generates errors (see https://kommunermeddnssec.se). This tool generated a healthy competition between municipalities.

The number of signed domain names skyrocketed as of 2011 (Figure 4.1) when the IIS offered registrars a yearly discount of SEK 6 for every correctly signed domain name in their portfolio. The IIS also financed an experimental site for naming and shaming non-DNSSEC sites of big organisations and companies (https://dnssec-name-and-shame.com) and continues to actively promote the DNSSEC in Sweden and elsewhere.

Figure 4.1. **Number of DNSSEC signed .se domains by year end and on 1 April 2018**

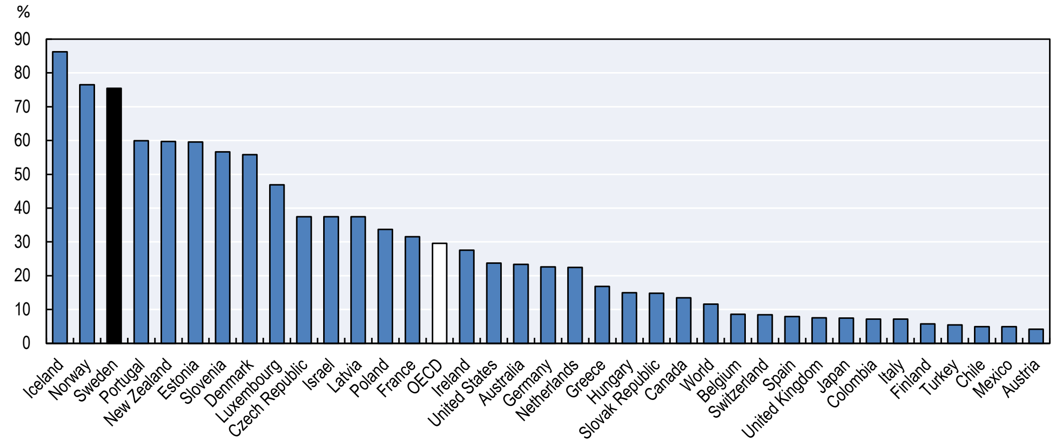


Notes: DNSSEC = Domain Name System Security Extensions. 2018 shows the number of DNSSEC signed .se domains on 1 April 2018.

Source: IIS (2018), "Number of DNSSEC domains per year end and today", www.iis.se/english/domains/domain-statistics/growth/?chart=per-type.

Figure 4.2. **Use of DNSSEC validation, 2018**

Proportion of end users



Notes: These statistics reflect the proportion of end users who passed their DNS queries to a DNS resolver that performs the DNSSEC validation from 12 January 2017 to 12 April 2018. It does not reflect the use of the DNSSEC by domain name zone administrators to sign the contents of their DNS zone.

Source: APNIC (2018)," DNSSEC validation rate by country (%)", http://stats.labs.apnic.net/dnssec.

The NIS Directive: A driver for change

This section provides a brief overview of the current (April 2018) plan to transpose the Directive on Security of Network and Information Systems (NIS Directive) in Sweden, with the objective of informing the overall analysis in this chapter. It does not discuss all the aspects covered by the directive.

The NIS Directive is expected to be transposed by EU countries by 10 May 2018. It establishes a framework for enhancing digital security and resilience of essential services, including by requiring that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks, and by establishing a notification requirement for significant incidents. The directive covers seven sectors, including energy, transport and banking, as well as so-called digital services. It can be viewed as a game changer for digital security in Sweden as its transposition will set clearer requirements for systematic risk management by operators of essential services.

A commission of enquiry nominated in May 2016 developed proposals for the transposition of the directive (Government Offices of Sweden, 2017d). Based on these elements and comments received from stakeholders, a proposal for a new legislation (thereafter the "legislative proposal") was submitted by the MoJ in February 2018 to the Council on Legislation, the body which scrutinises draft bills that the government intends to submit to parliament. A bill has been prepared for consideration by the parliament, with a proposal for legislation to enter into force on 1 August 2018.[8]

The legislative proposal promotes technical risk assessment rather than economic risk management

According to this proposal, the MSB would issue a regulation identifying operators of essential services in line with the NIS Directive. Operators would then examine whether the provision of their service is dependent on networks or information systems and if an incident would cause a significant disruption in the provision of the service, taking into account certain factors, such as the number of users who are dependent on the service in question and sector-specific and cross-sectoral factors included in regulation.

Consistent with the directive, operators of essential services would be required to take appropriate and proportionate technical and organisational measures to manage digital risk, including to ensure business continuity. This would include using a documented risk assessment as a basis for selecting security measures.

According to the legislative proposal, operators of essential services would have to carry out a "systematic and risk-based digital security risk assessment so as to enable business to systematically control digital security efforts in order to plan, implement, control, monitor, evaluate and improve the security of the organisation's information management".[9] This would include different types of analysis, such as business analysis, risk analysis and gap analysis. The proposal confirms that the Swedish government, and in particular the MSB, promotes a risk-based approach to digital security in essential services. Nevertheless, it also confirms that there is no particular emphasis on the need for the risk analysis to be driven by business leadership or to be integrated within the broader entreprise risk management framework of operators of essential services. It addresses risk assessment as a means to select security measures but it does not consider other risk treatment options such as risk acceptance, risk transfer and risk avoidance. In other words, it addresses digital security risk management as a methodology to protect systems and networks in a manner that fits already decided business objectives rather than as an integral part of business decision making. This is consistent with the analysis of the National Cybersecurity Strategy introduced earlier.

The apparent lack of promotion of an economic and social digital security risk management approach in a document such as the legislative proposal might result from its legal nature and from the context of the transposition of the NIS Directive. Guidance documents published by the MSB and discussions with government digital security experts show that there is an understanding of the need for business leadership to integrate digital security risk management in their decision-making processes as promoted by the OECD and explained in the previous section. This is confirmed, for example, by the National Audit Office audit reports and surveys by the MSB and the SKL which show that these bodies are asking the right questions and identify in their findings the same issues as the one pointed out above and in the analysis of the National Cybersecurity Strategy.

This suggests that expertise on what the OECD calls digital security risk management is present in Sweden but that the political and policy leaderships have not yet understood its importance or the need to integrate it more systematically in the economic and social digital culture of the country.

Towards a distributed model of supervision

The directive also requires the establishment of one or more "competent authorities" with the necessary powers and means to assess the compliance of operators of essential services with their obligations and to issue binding instructions to the operators of essential services to remedy the deficiencies identified (Articles 8 and 15). The transposition of the directive will therefore transform the governance of digital security in many EU countries, including Sweden.

As the agency in charge of regulating telecommunications networks, it is not surprising that the PTS is the most advanced sectoral regulator in the area of digital security, and has already established strong co-operation with the MSB in this area. However, the situation with respect to other critical sectors is less clear. With the current governance mechanism, the capacity to develop policies, supervise their application and, if necessary, support the operators of digital infrastructures lies with the government agencies in charge of each sector. However, it seems that sectoral regulators other than the PTS lack the expertise, capacity and perhaps awareness to accomplish this task. In addition, Sweden, like most other countries, faces a general skills shortage for digital security experts.

In deciding upon its governance structure, Sweden faces the following dilemma. While a large percentage of digital security issues are the same across sectors, a small but highly sensitive fraction can be very specific to each sector, for example with respect to industrial devices in the energy and transport sectors, or medical equipment in the health sector. It is important to take into account sector-specific market and regulatory constraints for effective digital security regulation. Should sector-specific digital security regulatory power and expertise be located as close as possible to the digital activity at stake with the risk of spreading resources across sectors and reducing critical mass? Or should they be concentrated in a central position such as the MSB to facilitate a national overview and an overarching operational critical mass, but at the cost of moving the regulation away from the day-to-day reality of the sectoral actors?

The legislative proposal suggests that one supervisory agency in each sector covered by the directive would be competent for monitoring compliance with the rules established by the new law. Concretely, the Energy Agency would be the competent agency for supervising compliance in the energy sector, the PTS for the digital infrastructures sector and digital services, the financial supervisory agency for the banking sector and financial market infrastructures, etc. These agencies would decide on penalty fees for failure to report incidents or taking security measures.

Nevertheless, recognising that the level of digital security knowledge in many sectoral agencies is often quite low, the legislative proposal suggests that the MSB lead a co-operation forum bringing together the agencies to foster uniform supervision and coherent supervisory practices, and prevent an uneven level of digital security in the society. In the context of this forum, the MSB would provide methodological support to sectoral agencies.

In addition to its co-ordination role, the MSB (CERT-SE) would also receive operators' reports of digital security incidents having a significant impact on continuity of service.

The law and additional regulation would set out the factors to be taken into account in assessing whether the incident has such an effect and should be reported. The MSB would issue regulations on mandatory incident reporting and the conditions for voluntary incident reporting. Lastly, the MSB would act as the Swedish national point of contact and represent Sweden in the European Cooperation Group and the CSIRTs Network established by the directive to facilitate cross-border co-operation and communication.

In this framework, it is not anticipated that sectoral competent authorities would acquire operational capacity. CERT-SE would remain the national CSIRT serving essential services operators (i.e. there would be no new domestic sectoral CSIRT) and providing situational awareness, informing the MSB, which would develop a more holistic risk picture.

This distributed supervision model is consistent with Sweden's decentralised model of governance with a strong constitutional principle of separation between ministries, between ministries and agencies, and between agencies. It is not unique in the context of the transposition of the NIS Directive. The United Kingdom, for example, plans to follow a distributed approach where sectoral agencies have responsibility for digital security risk with a strict separation from the National Cyber Security Centre, which will act as a centre of excellence providing them with expert advice and incident response capability (DCMS, 2018). Some other EU countries such as France, however, are following a centralised approach where a single agency (the Agence nationale de la sécurité des systèmes d'information [ANSSI]) is responsible for digital security and co-ordinating with relevant sectoral ministries and agencies. Each country follows an approach that is consistent with its culture and style of government, each with its own pros and cons. Sweden will need to significantly increase the MSB's and sectoral agencies' resources to enhance the level of protection and enable a consistent and uniform level of digital security across essential services. Effective co-ordination will be key to avoid scattering scarce resources and expertise.

A relatively more limited and uncoordinated set of other activities

As noted above, each government agency is responsible for digital security within its area of competence. Digital identity management was identified many years ago as an important area to foster the development of the digital economy, including with respect to payments and e-government. In this area, the Swedish market-led approach is a success story. Other initiatives are relatively modest, and, overall, do not seem co-ordinated and articulated around a common vision and objectives.

Digital identity

Digital identity and electronic authentication play an important role to reduce digital security risks. Sweden has succeeded in creating a favourable environment for a market-based e-ID ecosystem to emerge in order to support the online delivery of public and private sector services (Box 4.6). The main policy goal is that everyone should be able to logon with a user-friendly e-ID. The Swedish e-Identification Board promotes and co-ordinates e-ID and e-signature for public sector e-services. Its goals are to ensure that: i) everyone can access an easy-to-use and secure e-ID; ii) digital services can easily and securely make use of e-ID and e-signatures; iii) public sector use of e-ID and e-signatures is cost-effective. The board reviews Swedish e-ID solutions and provides the market with quality support for secure e-signature service. The Board audits e-ID against a trust level framework based on international standards. Approved e-IDs can use the "Swedish e-ID" logo ("*Svensk e-legitimation*"). The Board, which a public authority under the Ministry of Finance, is the Swedish eIDAS,[10] a node that enables cross-border authentication within the European Union.

Box 4.6. **Digital identity (e-ID) in Sweden**

The Swedish digital or electronic identity (e-ID) system is a success story: most citizens have an e-ID, they made over 1.1 billion transactions in various private and public e-services in 2015 and over 2.5 billion transactions in 2017 (BankID, 2017).

Although e-IDs can be issued by the private and the public sectors, the four operators offering e-ID solutions are private companies: a consortium of 11 banks called BankID has the largest market share (over 7 million users), followed by the telecommunications operator Telia (over 500 000 users), and 2 new entrants: Swedish passports "Svenska Pass" (Gemalto) and Freja eID Plus (Verisec).

Online banking has been the main driver for e-ID adoption in Sweden, explaining why BankID is the market leader with 7.5 million users out of a total Swedish population of 9.9 million. Almost the entire Swedish population aged between 21 and 50 holds a BankID e-ID. The percentage of mobile BankID users has continued to increase, reaching 91.9% users in December 2017: 29.3% users hold a BankID on card and 9.2% on file. BankID is primarily (92%) used for private sector services: Internet and mobile banking (61% of all transactions), payment services (18%), financial services (7%), and other private services (6%). Of the total number of BankID transactions, 6% are made with central government agencies and less than 2% with local government (BankID, 2017). Over 200 government agencies accept e-ID authentication for the delivery of online public services, and half of them also use e-signature. E-ID is used for public sector services such as social insurance, tax, student loans, business registrations and e-health. End users have the freedom to use the e-ID service of their choice, which requires that public services accept all providers on the market that reach the relevant trusted security level.

In 2012, Swedish banks launched Swish, an extremely user-friendly mobile app that enables individuals to make real-time payments to anyone registered in the Swish system (individuals, companies, associations and organisations). It takes a few seconds to create a Swish account with a mobile phone and link it to one's bank account. Then wiring money to another person only requires knowing the person's phone number. A EUR 1.05 transaction fee is borne by the relying party such as a store or business. Over 25 million payments were made in October 2017 using Swish, which only accepts Swedish crowns. Together with a high share of card payments, Swish contributes to the rapid decline of cash in Sweden, with only 20% cash payments in shops in 2014 (Segendorf and Wretman, 2015).

Nevertheless, BankID has experienced technical limitations in the past and does not cover 100% of the population, including migrants and individuals without a bank account. That is why the government is currently exploring the development of a robust public sector alternative to BankID's market dominance. A public sector solution would ensure that everyone can have equal access to authenticated online public service, an important priority in Sweden.

Sources: BankID (2017), "Statistik BankID–användning och innehav – fördjupning", www.bankid.com/assets/bankid/stats/2017/statistik-2017-12.pdf; Segendorf and Wretman (2015), "The Swedish payment market in transformation", www.riksbank.se/Documents/Rapporter/POV/2015/2015_3/rap_pov_artikel_2_151120_eng.pdf.

Innovation and research

In 2015, the Swedish Innovation Agency, Vinnova, analysed Sweden's strengths and challenges in a large range of technological areas, including digital security, in order to develop an action plan to promote the digitalisation of Swedish industry (Vinnova, 2015). The analysis used strategic innovation agendas developed by groups of actors in each area. With respect to digital security, Vinnova's mapping exercise used the "strategic innovation agenda" developed by a coalition gathering the Swedish Security and Defence

Industry Association, academia, research institutes and government agencies (SOFF, 2013). The mapping identified several strengths with respect to enhanced innovation in the area of digital security, such as the presence of major Swedish international companies which represent an attractive and relevant local market for digital security solutions, excellent digital infrastructures and leading security research. The lack of co-ordination between ICT and security as well as the lack of meeting venues were identified as weaknesses. Vinnova's action plan proposed five initiatives, including a "platform of knowledge and problem solving" that covered cybersecurity.

In 2018, the Swedish Foundation for Strategic Research announced a SEK 300 million (EUR 30 million) grant for ten cybersecurity research projects over five years in order to stimulate collaborative interdisciplinary research of relevance to present or future Swedish-based industry and to society (SSF, 2017; 2018). This initiative takes place in concert with the Swedish Government Strategic Partnership Program on Connected Industry, one of the five innovation partnership programmes launched in 2016 to help meet the societal challenges faced by Sweden (Government Offices of Sweden, 2016). The project includes applications involving the IoT, transport, data/telecommunications, power grids, smart cities and buildings, industrial control systems, public administration, healthcare, finance and insurance as well as cloud technologies and virtualised systems. The Swedish Foundation for Strategic Research is a public foundation which supports research in science, engineering and medicine for the purpose of strengthening Sweden's future competitiveness.[11]

Regional growth and activities by municipalities

The Agency for Economic and Regional Growth (Tillväxtverket), under the Ministry of Entreprise and Innovation, promotes economic growth by increasing the competitiveness of companies, facilitating entrepreneurship and creating attractive environments for companies in regions. It has developed information pages about privacy protection and is developing training modules about digital security in partnership with the MSB and the IIS.

The SKL represents municipalities and county councils and supports them in a wide range of areas, including digital security. The SKL recommends that municipalities use the ISO 27001 standard to manage digital security in municipalities and county councils. The SKL's website provides information to help local self-governments address digital security, including advice on digital security and outsourcing, digital identity, cloud computing, and personal data. The SKL developed an online tool to facilitate information classification for system administrators.[12] The SKL's site also points to useful resources compiled by the MSB and other actors. In 2015, the SKL released the results of a survey of municipalities' and county councils' digital security risk management efforts (SKL, 2015a; 2015b).

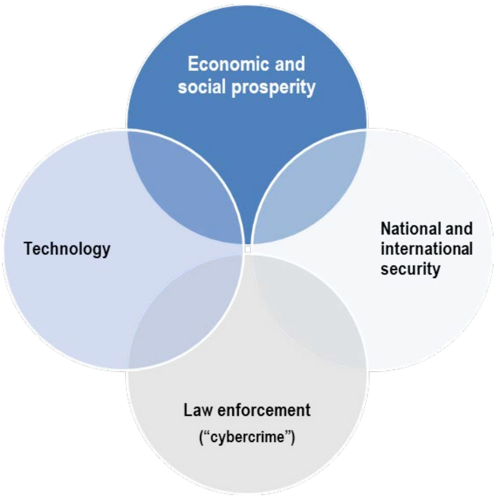
Towards a more holistic governance framework

Sweden's primary focus on crisis management preparedness and lack of leadership on the economic aspects of digital security prevents it from adopting a more holistic approach to digital security.

Ideally, digital security should be approached holistically as a single policy area. However, the reality is more complex and most governments struggle to find the best governance framework. Digital security is a multifaceted issue that includes technical, economic and social, criminal, as well as national and international security aspects (Figure 4.3).

These facets are interrelated and overlap to a certain extent. However, they can also compete and involve different priorities, actors, cultures and target audiences. They are all important and governments have to address the complex challenge of striking the right balance and ensuring coherence and consistency between them in order to approach this area more holistically. For example, regulation aiming to improve digital resilience of critical infrastructures' operators could inhibit innovation if it does not appropriately balance national security objectives with economic and social prosperity.

Figure 4.3. **Digital security is a multifaceted policy area**


Economic and social prosperity
Technology
National and international security
Law enforcement ("cybercrime")

In addition to being multifaceted, digital security also cuts across all sectors affected by the digital transformation (e.g. health, energy, transport, retail, finance, manufacturing, etc.) as well as policy areas. Digital security policies relate to skills policies to fill the digital security skills shortage and enhance security risk management business skills; innovation and research policies; policies to foster the development of a market for digital security products and services; insurance policies; small and medium-sized enterprise (SME) policies; policies to foster trusted public-private partnerships that enable information sharing on threats, vulnerabilities, incidents and good risk management practice; etc. Overall, most strategies related to the digital transformation, sector strategies, as well as technology-specific strategies (e.g. the IoT, AI, big data, etc.) should address digital security to a certain extent.

There is no one-size-fits-all model to digital security governance. Governance arrangements vary and reflect cultures and styles of government. Governments have taken different approaches to establish a policy co-ordination mechanism. For example, Australia, Japan and the United Kingdom have assigned policy co-ordination to the prime minister through the Cabinet Office; France established a national co-ordination agency within a pre-existing co-ordination body under the prime minister (ANSSI); Slovenia plans to establish a "national cyber authority"; the United States has established a "cybersecurity co-ordinator" who reports to the president; Canada, Germany and the Netherlands have placed the main responsibility for digital security under an existing ministry (respectively Public Safety, Interior, and Security and Justice).

In all these cases, there are also different arrangements with respect to how public policy co-ordination is concretely carried out, and where the government operational capacity is located, ranging from within the policy co-ordination agency (France) or ministry (Germany, the Netherlands) to a separate structure (the UK National Cyber Security Centre) or department (the US Department of Homeland Security). In Australia, for example, the Australian Cyber Security Centre is a joint responsibility of the Attorney-

General and the Minister for Defence. Over time, there has been a trend towards bringing together scattered operational bodies and resources to achieve critical mass and generate synergies, and to foster public-private partnerships with businesses across all sectors for information sharing and better situational awareness.

Many countries which developed a "national cybersecurity strategy" at the beginning of the decade have modified their governance arrangement and often also revised their strategy at least once since then to strike a better balance and to bring together scattered operational resources. Several countries have significantly elevated the level at which digital security policy making is being supported and addressed (e.g. prime minister, president). This reflects the increased importance of this area and is consistent with the OECD Security Risk Recommendation which suggests that national strategies should be supported at the highest level of government precisely to facilitate the balancing exercise between economic and social prosperity and national security objectives. Compared to the above-mentioned countries, Sweden has made a first step towards approaching digital security at a strategic level, but it has not yet started to improve its governance framework.

Some voices in Sweden have underlined that the Swedish style of governance with slim and relatively siloed central government and strong independent agencies is particularly challenging with respect to cross-cutting issues such as digital security. Such a governance model is particularly cost-effective for short-term siloed objectives but fails to effectively address longer term cross-cutting issues such as digital security. Some suggest the establishment of a central co-ordination mechanism such as a cybersecurity co-ordinator in the Cabinet Office, who could have an overarching view of all the facets of digital security and balance them most appropriately. The co-ordinator would be supported by an advisory group who would represent different perspectives (Nicander, 2017).

In 2015, a Swedish government report focusing on digital security in the public sector stressed the need to avoid the current fragmentation of digital security arrangements across agencies, municipalities and county councils, an approach which does not scale when the number of stakeholders increases significantly, such as in e-health. The report called for enhanced harmonisation and coherence of digital security across government agencies, encouraged the government to take a holistic approach, and called for a common framework and long-term sustainable national governance model, supported by continuously improved competence for digital security efforts in the public sector.

The authors suggested that such a national model could be eventually extended to public and private organisations. They proposed a governance structure based on a new government authority, the "Information Security Council", consisting of relevant government agencies representatives to enable in-depth co-ordination and facilitate more common systematic risk management. The MSB would lead the council and manage its administration. Policy discussions would be led by the Government Offices (i.e. as opposed to government agencies). The council would include the authorities involved in the existing co-operation group SAMFI (introduced above), as well as authorities and actors not directly involved in the functioning of the public sector, such as sectoral agencies. It would establish working groups to accommodate the various aspects and dynamic nature of the digital transformation. Agencies would be responsible for taking appropriate decisions in their respective areas after consultation with the council, which would not have regulatory capacity. The council would ensure the implementation of the National Cybersecurity Strategy and provide an assessment of the digital security risk level in government agencies. It would develop standards and certification requirements in relation to public procurement (Government Offices of Sweden, 2015).

In December 2017, the government agreed to establish a co-ordination agency for the digitalisation of the public sector that would develop, manage, provide and promote the use of a national digital infrastructure for the public sector. The agency will be responsible for the security of this infrastructure, including key services such as electronic identification, trust services and secure email (Government Offices of Sweden, 2017c). While the details of this agency are still to be determined, it looks like a first step towards bringing together in a central point digital security expertise with respect to public sector electronic services. As an operational technical body, however, it is very different from the 2015 proposal mentioned above which was more focused on digital security co-ordination.

It is clear that Sweden needs a more holistic approach to digital security policy governance, but it is too early to make a realistic detailed recommendation on what it would look like. Sweden would first need to clarify its vision of digital security for prosperity. It is likely that the co-operation process to do so will raise awareness about the cross-cutting nature of digital security.

Policy recommendations

Sweden identified digital security as an important issue as early as 2003. The basic components of digital security policy are in place, with an emphasis on the protection of essential services and critical infrastructure, in particular in the telecommunications sector, both areas where roles and responsibilities are clearly defined. The transposition of the NIS Directive will drive significant improvements by establishing a clearer and more robust framework to strengthen digital security in essential sectors, beyond telecommunications. Other agencies are involved in digital security policy in areas such as innovation and regional growth. However, there does not seem to be a clear co-ordination framework to ensure that such initiatives serve a common vision and objectives. Sweden's market-led digital identity management approach is a success story. Non-governmental stakeholders such as the SKL and the IIS play an important role in promoting digital security.

Sweden should adopt a clear vision of digital security risk management for prosperity to change businesses' and organisations' culture

At the strategic level, the Swedish approach to digital security is characterised by a general focus on the security of information systems and networks rather than on the economic and social activities that rely on them. While strategic documents address many aspects of digital security, they do not yet place a sufficient emphasis on digital security as a business leadership priority and responsibility. They are based on the 2002 OECD Security Guidelines rather than on the 2015 *Recommendation on Digital Security Risk Management* that replaced them.

To become a world leader in harnessing the opportunities of the digital transformation, Sweden must also lead in managing the digital security risk associated with these opportunities. Sweden needs to devise and promote a clearer vision of digital security risk management as an economic and social responsibility for public and private organisations' leaders and decision makers.

Such a vision should promote a cultural shift in organisations, and more broadly across the economy and society. In particular, leaders and decision makers in businesses and other organisations (chief executive officers, board members, business line managers, etc.) should own the responsibility for managing both the opportunities from and the security risks of the digital transformation. They should use digital security risk management as an essential tool to increase the likelihood of success in an increasingly digital-dependent environment, take informed economic and social choices, and prioritise actions. They should integrate digital security risk management into their decision-making processes and rely on technical experts for technical aspects rather than delegate the entire risk management responsibility to them.

The current gap between technical experts and economic decision makers is jeopardising Sweden's efforts to protect essential services against digital security risk. At the operational level, digital security experts (e.g. at the MSB) understand and support the need to tie opportunities and risk management together to effectively protect essential services. But they struggle to get this message across beyond the community of security experts. The current legislative proposal for the transposition of the NIS Directive does not seem to address this important issue. The transposition of the NIS Directive offers a good opportunity to promote a culture of digital security risk management to the leadership of the most important businesses and public bodies in Sweden and to develop enhanced co-operation between ministries and agencies addressing the different facets of digital security (protection and prosperity).

Policy leadership on digital security for prosperity should be clearer and stronger

There is lack of clear policy leadership with respect to the economic aspects of digital security in Sweden. Lack of leadership probably explains why digital security for prosperity is akin to a blind spot, with strategic policy documents that do not yet reflect a vision in this area and economically oriented digital security policy initiatives that are relatively uncoordinated (e.g. research and innovation) or limited (e.g. towards SMEs or in relation to education).

Currently, digital security is primarily a crisis management preparedness matter, an area led by the Ministry of Justice. The MoJ also co-ordinates digital security policy making more broadly. Constitutionally, however, the MoJ cannot address digital security in areas falling under the mandate of other ministries, such as economic prosperity. Clearer and stronger policy leadership on digital security for prosperity would be necessary to develop an economic and social vision of digital security policy for Sweden. Such leadership would strengthen the profile of digital security for prosperity within the broader co-ordination carried out by the MoJ.

Sweden should adopt a more holistic governance, taking stock of the different approaches adopted by other OECD countries

Digital security policy efforts in Sweden are relatively scattered and their co-ordination is partial. Sweden's primary focus on crisis management preparedness and lack of leadership on the economic aspects of digital security prevents it from adopting a more holistic approach to digital security. Other countries' experience shows that leading countries tend to rationalise their governance with stronger co-ordination mechanisms under leadership at the highest level of government. However, there is generally a learning curve towards a balanced governance, and no ideal one-size-fits-all model.

While it is too early to make a realistic detailed recommendation on what an appropriate holistic governance would look like in Sweden, it is clear that the government should strengthen ministerial co-ordination in this area. It is likely this process would raise awareness about the cross-cutting nature of digital security. Proposals made by experts and investigation commissions form a good basis for addressing this issue, as well as comparison with other countries' approaches.

The Digitalisation Council could become a hub for co-operation on digital security

The government should address business and decision makers in the public and private sectors on this issue, and gather all stakeholders to develop a more holistic digital security strategy for prosperity in Sweden (regardless of what it is called).

Nevertheless, because all the facets of digital security are interrelated, it is important that the strategy be developed in co-operation or jointly with other ministries and agencies with a mandate and expertise on digital security, starting with the MoJ. Strong co-operation between ministries and agencies with mutually reinforcing and complementary mandates is essential to foster a holistic approach to digital security policy. The Digitalisation Council might be a useful platform to foster such co-operation, and promote a common vision and more co-ordinated agenda.

Notes

[1] All agencies in Sweden are independent from the central government. For more details, see Chapter 1.

[2] "Digital *trygghet*" is translated as "digital security" in the government's digital strategy factsheet (Government Offices of Sweden, 2017a) and in the strategy's press release (Government Offices of Sweden, 2017b). English-Swedish dictionaries translate "*trygghet*" as "security".

[3] The English translation of the strategy uses the term "authenticity". However, "integrity" seems to be more appropriate since the term used is defined as meaning "that the information is not modified, manipulated or destroyed in an unauthorised manner".

[4] This section focuses primarily on government bodies with a strategic digital security policy role. Other bodies may also have a role for digital security. For example, the National Archives of Sweden aims to ensure the integrity of government information in general, and prescribes standards for all government bodies regarding metadata and digital file formats to ensure long-term information availability and usability in e-archives.

[5] https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet (in Swedish).

[6] www.ledningskollen.se.

[7] https://robustfiber.se (in Swedish).

[8] Elements in the following sections are based on the legislative proposal (i.e. not the bill) which was available at time of writing.

[9] Non-official translation.

[10] An eIDAS node enables the participation of a country in the European Union cross-border authentication network established by the EU regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (Regulation 910/2014 of 23 July 2014 on electronic identification).

11. For more details about the Swedish Foundation for Strategic Research, see: www.government.se/government-policy/education-and-research/research-funding-in-sweden and OECD (2016: 69).

12. https://klassa-info.skl.se/page/start (in Swedish).

References

Anderson, C (2017), "Swedish government scrambles to contain damage from data breach", *New York Times*, 25 July, www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html (accessed 18 April 2018).

APNIC (2018), "DNSSEC validation rate by country (%)", Asia Pacific Network Information Center, April, http://stats.labs.apnic.net/dnssec.

BankID (2017), "Statistik BankID–användning och innehav – fördjupning" (in Swedish), www.bankid.com/assets/bankid/stats/2017/statistik-2017-12.pdf (accessed 18 April 2018).

CERT-SE (2017), "Vad ska rapporteras?" (in Swedish), webpage, www.cert.se/it-incidentrapportering/vad-ska-rapporteras (accessed 18 April 2018).

DCMS (2018), "Security of network and information systems: Government response to public consultation", January, Department for Digital, Culture, Media and Sport, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf (accessed 6 April 2018).

European Union (2016), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, European Union, Brussels, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG (accessed 18 April 2018).

Government Offices of Sweden (2017a), "Action on digital transformation", press release, 5 June, www.government.se/press-releases/2017/06/action-on-digital-transformation (accessed 4 April 2018).

Government Offices of Sweden (2017b), "For sustainable digital transformation in Sweden: A digital strategy", Ministry of Enterprise and Innovation, N2017.23, Factsheet, June, www.government.se/information-material/2017/06/fact-sheet-for-sustainable-digital-transformation-in-sweden--a-digital-strategy (accessed 4 April 2018).

Government Offices of Sweden (2017c), "Kommittédirektiv. Inrättande av en myndighet för digitalisering av den offentliga sektorn" (in Swedish), Dir. 2017:117, www.regeringen.se/rattsdokument/kommittedirektiv/2017/12/dir.-2017117 (accessed 11 April 2018).

Government Offices of Sweden (2017d), "Utredning om genomförande av NIS-direktivet överlämnad till inrikesminister Anders Ygeman" (in Swedish), www.regeringen.se/pressmeddelanden/2017/05/utredning-om-genomforande-av-nis-direktivet-overlamnad-till-inrikesminister-anders-ygeman7 (accessed 18 April 2018).

Government Offices of Sweden (2016), "Innovation partnership programmes: Mobilising new ways to meet societal challenges", webpage, Government Offices of Sweden, www.government.se/articles/2016/07/innovation-partnership-programmes--mobilising-new-ways-to-meet-societal-challenges (accessed 18 April 2018).

Government Offices of Sweden (2015), "Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten" (in Swedish), ID-nummer: SOU 2015:23, www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201523 (accessed 4 April 2018).

Hufford, A. (2017), "Merck swings to loss as cyberattack hurts sales", MarketWatch, 27 October, www.marketwatch.com/story/merck-swings-to-loss-as-cyberattack-hurts-sales-2017-10-27-134853159 (accessed 18 April 2018).

IIS (2018), "Number of DNSSEC domains per year end and today", www.iis.se/english/domains/domain-statistics/growth/?chart=per-type (accessed 1 April 2018).

ISO/IEC (2009), "ISO 31000:2009: Risk management – Principles and guidelines", International Organization for Standardization, https://www.iso.org/standard/43170.html.

Merck (2017), "Merck announces second-quarter 2017 financial results", press release, 28 July, Merck, www.mrknewsroom.com/news-release/corporate-news/merck-announces-second-quarter-2017-financial-results (accessed 18 April 2018).

MSB (2016), *MSBFS 2016:1 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet* (in Swedish), Swedish Civil Contingencies Agency, www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-20161 (accessed 18 April 2018).

MSB (2014a), *En bild av myndigheternas informationssäkerhetsarbete 2014* (in Swedish), Swedish Civil Contingencies Agency, www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-myndigheternas-informationssakerhetsarbete-2014 (accessed 18 April 2018).

MSB (2014b), "Samverkansgruppen för informationssäkerhet, SAMFI" (in Swedish), Swedish Civil Contingencies Agency, www.msb.se/Upload/Forebyggande/Informationssakerhet/Faktabad%20SAMFI.pdf (accessed 18 April 2018).

MSB (2012a), *Sweden's Information Security: National Action Plan 2012*, MSB455, Swedish Civil Contingencies Agency, www.msb.se/en/Products/Publications/Publications-from-the-MSB/Swedens-Information-Security---National-Action-Plan-2012 (accessed 3 April 2018).

MSB (2012b), "The MSB and societal information security", February, Swedish Civil Contingencies Agency, www.msb.se/Upload/English/About_MSB_fact/Societal%20information%20security.pdf (accessed 18 April 2018).

MSB (2011), "CERT-SE: Independent and neutral IT security for private and public sectors", June, Swedish Civil Contingencies Agency, www.msb.se/RibData/Filer/pdf/25968.pdf (accessed 18 April 2018).

MSB (2010), *Strategy for Information Security in Sweden 2010-2015*, Swedish Civil Contingencies Agency, https://www.msb.se/RibData/Filer/pdf/25940.PDF.

NAO (2016a), "Information security work at nine agencies", Report No. RiR 2016:8, 26 May, Swedish National Audit Office, www.riksrevisionen.se/en/audit-reports/audit-reports/2016/information-security-work-at-nine-agencies.html (accessed 4 April 2018).

NAO (2016b), "Informationssäkerhetsarbete på nio myndigheter" (in Swedish), Report No. RiR 2016:8, Swedish National Audit Office, https://www.riksrevisionen.se/rapporter/granskningsrapporter/2016/informationssakerhetsarbete-pa-nio-myndigheter.html (accessed 4 April 2018).

NAO (2014), "Information security in the civil public administration", Factsheet. Report No. RIR 2014:23, https://www.riksrevisionen.se/en/audit-reports/audit-reports/2014/information-security-in-the-civil-public-administration.html.

Nicander, L. (2017), "Nu behövs en koordinator för cybersäkerheten", in: Dagens Nyheter, 21 July, www.dn.se/debatt/nu-behovs-en-koordinator-for-cybersakerheten.

OECD (2016), *OECD Reviews of Innovation Policy: Sweden 2016*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264250000-en.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264245471-en.

OECD (2002), *Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris, www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm.

Oehme, R. (2015), "Cyber security in Sweden: With focus on National Collaboration Forum and private public partnership", presentation, www.viestintavirasto.fi/attachments/esitykset/Richard_Oehme_Presentation_Fi_2015-11-04.pdf (accessed 18 April 2018).

Palmer, D. (2017), "Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk", ZDNet, 16 August, www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk (accessed 18 April 2018).

PTS (2017), *Utbildnings - och övningsstrategi för krisberedskap 2017 -2021 Sektorn Elektronisk kommunikation* (in Swedish), PTS-ER-2017:02, Swedish Post and Telecom Authority, www.pts.se/globalassets/startpage/dokument/icke-legala-dokument/rapporter/2017/internet/rapport_utbildnings--och-ovningsstrategi-2017-2021_pts-er-2017-02.pdf (accessed 18 April 2018).

PTS (2015), "Safer communications for everyone" (in Swedish), Swedish Post and Telecom Authority, https://www.pts.se/globalassets/startpage/dokument/icke-legala-dokument/faktablad/internet/sv-nat-april-2015.pdf (accessed 18 April 2018).

PTS (2013), "Driftinformation mellan operatörer -för kortare avbrott" (in Swedish), Swedish Post and Telecom Authority, https://diowebb.se/media/57/Faktablad-DIO.pdf (accessed 18 April 2018).

Rushe, D. (2014), "Target CEO Gregg Steinhafel resigns in wake of customer data breach", The Guardian, 5 May, www.theguardian.com/business/2014/may/05/target-chief-executive-steps-down-data-breach (accessed 3 April 2018).

Saint-Gobain (2017), "Résultats du 1er semestre 2017", press release, 27 July, www.saint-gobain.com/sites/sgcom.master/files/cp_vf_resultats_s1_2017_t.pdf (accessed 18 April 2018).

Segendorf, B. and A. Wretman (2015), “The Swedish payment market in transformation”, in: *Sveriges Riksbank Economic Review*, No. 2015:3, www.riksbank.se/Documents/Rapporter/POV/2015/2015_3/rap_pov_artikel_2_151120_eng.pdf (accessed 18 April 2018).

SKL (2015a), “Nordiskt samarbete om informationssäkerhet i kommuner, landsting och regioner promemoria om informationssäkerhet och digitalisering svenska kommuner” (in Swedish), Swedish Association of Local Authorities and Regions, Stockholm, https://skl.se/download/18.1ea1a4111513965b0179e6d/1448536942895/NordSec_Rapport%20Svenska%20kommuner%202015.pdf (accessed 5 April 2018).

SKL (2015b), “Nordiskt samarbete om informationssäkerhet i kommuner, landsting och regioner promemoria om informationssäkerhet och digitalisering svenska kommuner 2015” (in Swedish), Swedish Association of Local Authorities and Regions, Stockholm, https://skl.se/download/18.1ea1a4111513965b0179e6c/1448536925762/NordSec-Rapport%20Svenska%20Landsting%20och%20Regioner%202015.pdf (accessed 5 April 2018).

SOFF (2013), “Strategisk Forsknings - och Innovationsagenda: Säkerhet” (in Swedish), Swedish Security & Defence Industry Association, May, http://soff.se/wp-content/uploads/2015/04/fia-sakerhet.pdf (accessed 18 April 2018).

SSF (2018), “300 miljoner till cybersäkerhet –en värdefullinjektion i det digitala samhället” (in Swedish), Swedish Foundation for Strategic Research, Stockholm, https://strategiska.se/app/uploads/pm-ssf-300-miljoner-till-cybersakerhet.pdf (accessed 18 April 2018).

SSF (2017), “SSF call for proposals: Framework grants for research on cybersecurity and information security”, Swedish Foundation for Strategic Research, Stockholm, http://strategiska.se/app/uploads/rit17_en.pdf (accessed 18 April 2018).

Sverige Radio (2016), “Online attack hits Swedish media sites”, Radio Sweden, 20 March, http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6393804 (accessed 18 April 2018).

Swedish Emergency Management Agency (2008), “Information security in Sweden: Action Plan 2008-2010”, Swedish Emergency Management Agency, www.msb.se/Upload/Produkter_tjanster/Publikationer/KBM/Information%20Security%20in%20Sweden.pdf (accessed 3 April 2018).

The Local (2017), “Swedish government battles political fallout from transport data leak”, The Local, 25 July, www.thelocal.se/20170725/swedish-government-battles-political-fallout-from-transport-data-leak (accessed 18 April 2018).

Vinnova (2015), “Slutrapportering ‘Uppdrag att utföra insatser för att främja digitalisering av svensk industri’” (in Swedish), N/2015/6246/IF, www.vinnova.se/contentassets/ecd0206440df49a5aea396f74c90d060/2015-04724-rapp.pdf (accessed 18 April 2018).

Zetter, K. (2016a), “A cyberattack has caused confirmed physical damage for the second time ever”, Wired, https://www.wired.com/2015/01/german-steel-mill-hack-destruction.

Zetter, K. (2016b), “Inside the cunning, unprecedented hack of Ukraine’s power grid”, Wired, 3 March, www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid (accessed 3 April 2018).

From:

OECD Reviews of Digital Transformation: Going Digital in Sweden

Access the complete publication at:

https://doi.org/10.1787/9789264302259-en

Please cite this chapter as:

OECD (2018), “Digital security policy”, in *OECD Reviews of Digital Transformation: Going Digital in Sweden*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264302259-6-en