Audit Compendium

Cybersecurity in the EU and its Member States: auditing the resilience of critical information systems and digital infrastructures to cyber attacks

Audit reports
published between 2014 and 2020

December 2020

The Contact Committee of the European Union's (EU) supreme audit institutions (SAIs) offers a forum for discussing and addressing EU public audit issues. By increasing dialogue and cooperation between its members, the committee helps to make the external audit of EU policies and programmes more effective. It also helps to enhance accountability, improve the EU's financial management and consolidate good governance, to the benefit of all EU citizens.

Contact: www.contactcommittee.eu

Contents

Page

Contents

Contents

Opening words

Dear Reader,

Digitalisation and the growing use of information technology in all aspects of our daily lives is opening up a new world of opportunities. In turn, the risks to individuals, businesses and public authorities of falling victim to cybercrime or a cyber attack have increased, and so has their societal and economic impact.

In the EU, cybersecurity is a prerogative of the Member States. The EU has a role to play in creating a common regulatory framework within the EU's single market and creating the conditions for Member States to work together in mutual trust.

Cybersecurity and our digital autonomy has become a subject of strategic importance for the EU and its Member States. Weaknesses in cybersecurity governance persist in the public and private sectors across all Member States, albeit at different levels. This impairs our ability to limit and, when necessary, respond to cyber attacks. Disinformation, often orchestrated from outside the EU, is on the rise, as illustrated once again during this year's Covid-19 pandemic. This represents a threat to social cohesion in our societies and to citizens' trust in our democratic systems that we cannot ignore.

In 2018, a survey of the supreme audit institutions (SAIs) in the EU showed that so far around half had not audited cybersecurity. Since then, our SAIs have geared up their audit work on cybersecurity, with a particular focus on data protection, system readiness against cyber attacks, and the protection of essential public utilities systems. Understandably, not all of these audits can be made public, as some may concern sensitive (national security) information.

During this year, the Covid-19 crisis has been testing the economic and social fabric of our societies. Given our dependence on information technology, a "cyber crisis" could well turn out to be the next pandemic. We need to be prepared and to step up the resilience of critical information systems and digital infrastructures against cyber attacks.

We hope that the overview provided in this compendium will further stimulate the interest of public auditors across the Union in this critical area.

Klaus-Heiner Lehne

President of the European Court of Auditors
Chair of the Contact Committee
& Leader of the project

Executive summary

I Cybersecurity and our digital autonomy has become a **subject of strategic importance for the EU and its Member States** and, as the threat level rises, we must step up our efforts to protect our critical information systems and digital infrastructures against cyber attacks. Cybersecurity not only concerns our utilities, defence, or health systems, it is also about protecting our personal data, business models and intellectual property. Ultimately, cybersecurity is about protecting our democratic societies, our independence as Europeans and the way we live together.

II The first section of this third compendium of the Contact Committee sets out **what cybersecurity entails**. It describes how cybersecurity is a challenge for public authorities, companies and individuals, and highlights the new phenomenon of disinformation, which is a growing threat to social cohesion in our societies and democratic systems. It also explains the EU's cybersecurity competencies and actors, its strategy and legislation as well as the EU funding available in this area.

III The second part of the compendium summarises the **results of selected audits carried out by twelve contributing Member State SAIs and the European Court of Auditors**, published between 2014 and 2020. These audits addressed important aspects of cybersecurity, such as the protection of private data, the integrity of national data centres, the security of public utilities installations, and the implementation of national cybersecurity strategies in a broader sense.

IV The third part of the compendium contains **detailed factsheets for the selected audits**, together with a synopsis of other audits relating to the topic of cybersecurity published by the SAIs.

PART I – Cybersecurity in the European context

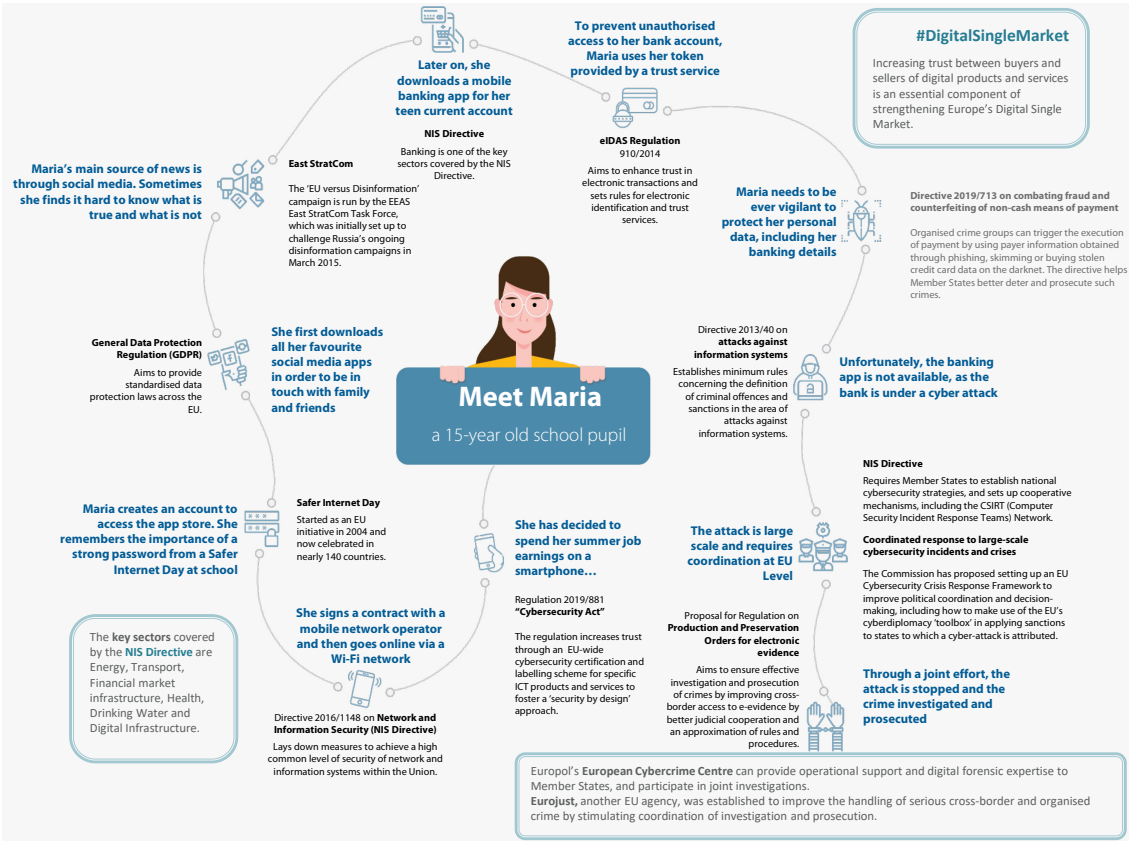
What is cybersecurity?

1 There is no standard universal **definition of cybersecurity**. In this document, cybersecurity refers to the **activities needed to protect network and information systems, their users and other persons affected by cyber threats**. It involves preventing, detecting, responding to and recovering from cyber incidents. These incidents may be intentional or unintentional and range from the accidental disclosure of information to attacks on businesses and critical infrastructure, the theft of personal data, or even interference in democratic processes up to electoral interferences, or general disinformation campaigns to influence public debates.

Cybersecurity affects all EU citizens' daily lives

2 Cybersecurity affects the daily lives of all EU citizens, whenever we use personal IT devices such as smartphones, WIFI networks, social media or electronic banking. In 2020, more than ever, the question is no longer whether cyber attacks will occur, but how and when they will occur. This concerns us all: **individuals, businesses and public authorities**. ***Picture 1*** illustrates how the EU endorses cybersecurity and has created a framework to protect citizens' daily electronic activities from cyber attacks. Protecting critical information systems and digital infrastructures against cyber attacks has become a strategic challenge.

Picture 1 – The EU endorsing cybersecurity in EU citizens' daily life

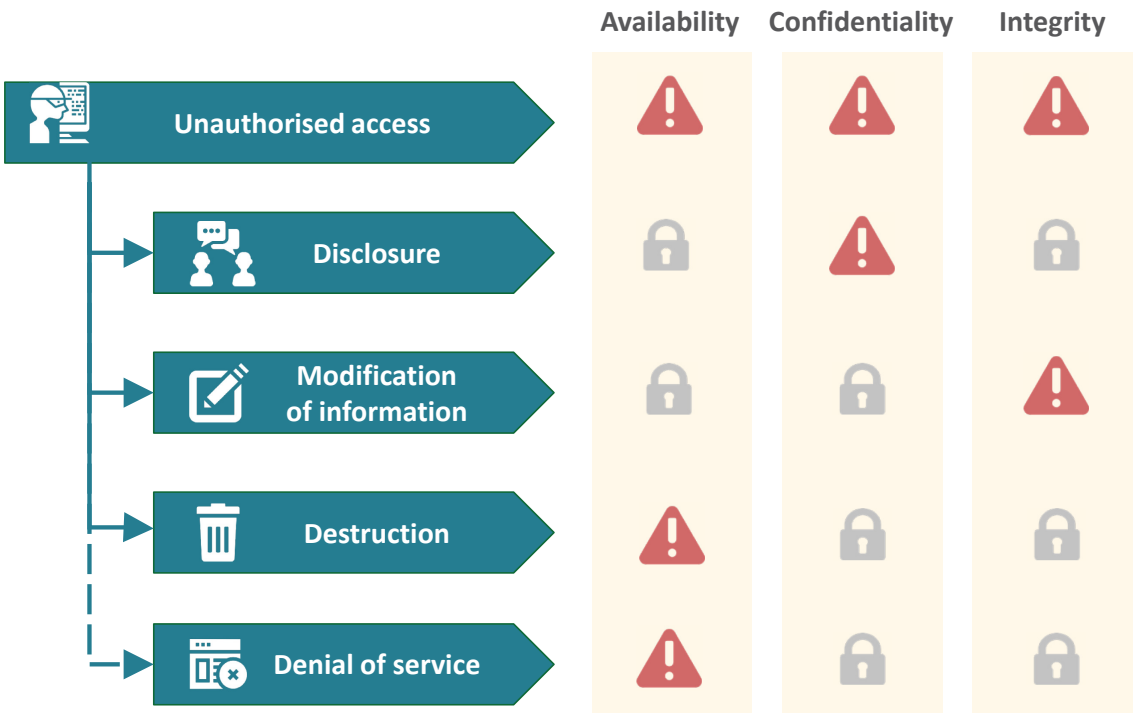


Source: ECA, icons made by Pixel perfect from www.flaticon.com.

There are numerous types of cybersecurity threats

3 The numerous types of cybersecurity threats our societies face can be classified according to **what they do to data – disclosure, modification, destruction or access** denial – or the core information security principles they violate (see ***Figure 1***).

Figure 1 – Threat types and the information security principles they endanger



Padlock = security not impacted; Exclamation mark = security at risk

Source: ECA, based on a European Parliament study[1].

4 Every time a device goes online or connects with other devices, the so-called cybersecurity "attack surface" increases. The exponential growth of the "Internet of Things" (IoT), the cloud, big data and the digitisation of industry has been accompanied by a growth in the exposure of vulnerabilities, enabling attackers to target ever more victims. The variety of attack types and their growing sophistication make it difficult to keep pace[2]. ***Box 1*** describes examples of **possible cyber attacks**.

[1] European Parliament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, Study for the LIBE Committee, September 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017*, 18 January 2018.

Box 1

Types of cyber attack

Malware (malicious software) is designed to harm devices or networks. It can include viruses, Trojans, ransomware, worms, adware and spyware (e.g. NotPetya).

Ransomware encrypts data, preventing users from accessing their files until a ransom is paid, typically in cryptocurrency, or an action is carried out. According to Europol, ransomware attacks dominate across the board, and the number of ransomware types has exploded over the past few years (e.g. Wannacry[3]).

Distributed Denial of Service (DDoS) attacks, which make services or resources unavailable by flooding them with more requests than they can handle, are also on the rise, with one-third of organisations facing this type of attack in 2017[4].

Web-based attacks are an attractive method by which threat actors can delude victims using web systems and services as the threat vector. This covers a vast attack surface, for instance facilitating malicious URLs or malicious scripts to direct the user or victim to the desired website or downloading malicious content (watering hole attacks, drive-by attacks) and **injecting** malicious code into a legitimate but compromised website to steal information (i.e. formjacking) for financial gain or information theft[5].

Users can be manipulated into unwittingly performing an action or disclosing confidential information. This ruse can be used for data theft or cyberespionage, and is known as **social engineering**. There are different ways to achieve this, but a common method is **phishing**, where emails appearing to come from trusted sources trick users into revealing information or clicking on links that will infect devices with downloaded malware. More than half of Member States reported investigations into such network attacks[6].

Perhaps the most nefarious threat type is **advanced persistent threats** (APTs). These threats come from sophisticated attackers engaged in long-term monitoring and theft of data, sometimes with destructive goals. Their aim is to stay under the radar for as long as possible. APTs are often state-linked and target especially sensitive sectors such as technology, defence and critical infrastructure. This type of **cyberespionage** is said to account for at least one-quarter of all cyber incidents[7].

---

[3] The *Wannacry* ransomware exploited vulnerabilities in a Microsoft Windows protocol enabling the remote takeover of any computer. A patch was issued by Microsoft after it

The economic impact of cyber attacks is significant

5 The threat of **cyber attacks and cybercrime** has become a major issue in recent years. Already in 2016, 80 % of EU businesses had experienced at least one cybersecurity incident[8]. In 2018, 40 % of survey respondents from organisations using robotics or automation said that the disruption of operations would be the most critical consequence of a cyber attack on their systems. Nonetheless, despite an awareness of disruptive cyber risks, companies often have no system in place to handle them[9].

6 Since then, the number of cyber attacks, their seriousness and financial costs have continued to rise. Cybercrime, as far as its **financial impact** can be estimated, will cost the global economy **$6 trillion annually by 2021**, up from an estimated $3 trillion in 2015[10], compared to an estimated worldwide GDP of $138 trillion in 2020. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, post-attack disruption to the normal course of business, reputational harm. The European Systemic Risk Board (ESRB) estimates that the average cost of cyber incidents increased by 72 % between 2015 and 2020[11].

---

discovered the vulnerability. However, hundreds of thousands of computers were not updated and many were subsequently infected. *Source:* A. Greenberg, *Hold North Korea Accountable for Wannacry – and the NSA, too*, WIRED, 19 December 2017.

4 Europol, *Internet Organised Crime Threat Assessment 2018*.

5 ENISA, *ENISA Threat Landscape 2020 – Web-based attacks*, 20 October 2020.

6 Europol, see before, 2018.

7 European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper No 2/18, February 2018.

8 Europol, *Internet Organised Crime Threat Assessment 2017*.

9 PWC, Global State of Information Security (GSISS), *Survey – Strengthening digital society against cyber shocks*, 2017.

10 Cybersecurity Ventures, *2019 Official Annual Cybercrime Report*, sponsored by Herjavec Group, 2019.

11 ESRB, European Systematic Risk Board, *Systemic cyber risk*, February 2020.

7 Cybercrime **affects the various economic sectors differently**, as shown by a recent study from 2020[12]: it was the most disruptive fraud phenomenon in government and public administration, the technology, media and telecommunications sector and the health sector (see ***Box 2***); it was also the second most disruptive fraud phenomenon in the financial sector and the industrial and manufacturing sector.

Box 2

Finnish psychotherapy patients blackmailed with personal medical data stolen between 2018 and 2019

Patients of a large Finnish psychotherapy clinic with branches all over the country were contacted individually in 2020 by a blackmailer, after their personal data was stolen in November 2018, with a further potential breach in March 2019. The data appears to have included personal identification records and notes about what was discussed in therapy sessions.

Both the clinic and the patients were asked to pay the blackmailer ransoms with bitcoin, so the data would not be made public. The incident led the Finnish government to hold an emergency meeting[13].

8 In 2019, EUROPOL[14] again highlighted the **persistence and tenacity of a number of key cybercrime threats**:

- ransomware attacks remain the top threat; they are becoming more precisely targeted, more profitable and cause greater economic damage. As long as ransomware provides a relatively easy income for cybercriminals, and continues to cause significant damage and financial losses, it is likely to remain the top cybercrime threat;
- phishing and vulnerable remote desktop protocols (RDPs) are the key primary malware infection vectors; and

[12] PWC, *Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey*, 2020.

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach*, 26 October 2020.

[14] EUROPOL, *INTERNET organised crime threat assessment (IOCTA)*, 2019.

- data remains a key target, commodity and enabler for cybercrime.

9 Similarly, in its **2020 report "Main incidents in the EU and worldwide"**[15], the European Union Agency for Cybersecurity (ENISA) provides a number of examples of cybersecurity incidents (see ***Box 3***).

Box 3

European Union Agency for Cybersecurity (ENISA): 2019-2020 cybersecurity incidents

The e-mail platform verifications.io, suffered a major data breach due to an unprotected MongoDB database. Data from over 800 million emails were exposed, containing sensitive information that included personally identifiable information (PII).

Over 770 million e-mail addresses and 21 million unique passwords were exposed in a popular hacking forum hosted by the cloud service MEGA1. It became the most significant collection of breached personal credentials in history, named "Collection #1".

The cloud and virtualisation provider Citrix was a victim of a targeted cyber attack. To gain access to Citrix's systems, the attackers exploited several critical software vulnerabilities such as CVE-2019-19781 and employed a technique called password spraying.

The cloud hosting provider iNSYNQ19 experienced a ransomware attack that left customers unable to access their data for more than a week, forcing customers to rely on local backups.

10 According to EUROPOL, cyber attacks designed to cause **lasting damage** doubled during the first six months of 2019, mainly in the manufacturing sector. Unlike conventional' ransomware attacks, these are acts of sabotage which permanently erase or otherwise irreversibly damage company data (see ***Box 4***).

[15] ENISA, *Main incidents in the EU and worldwide – January 2019 to April 2020*, October 2020.

Box 4

Destructive ransomware - the 2019 "Germanwiper" attacks

In 2019, a series of ransomware attacks targeting companies operating in Germany was identified. Dubbed as *Germanwiper*, the ransomware has the ability to replace the infected files with zeroes and ones, thus making the recovery of the files impossible. The ransomware is spread through email phishing campaigns and in particular targeted HR staff of top companies, as it was embedded in fake job applications[16].

Awareness of cybersecurity threats is growing in step with their increasing frequency

11 Nevertheless, until recently, awareness and acknowledgement of these risks was still fairly low. In 2017, 69 % of companies in the EU had no, or only a basic understanding, of their **exposure to cyber threats**[17], and 60 % had never estimated the **potential financial losses**[18]. Furthermore, according to a global survey in 2018, one-third of organisations would rather pay the hacker's ransom than invest in information security[19].

12 The **2020 Eurobarometer "Europeans' attitudes towards cyber security"**[20] identifies the rising awareness, and concern, of EU citizens:

- internet-using respondents are most likely to be concerned about someone misusing their personal data (46 %), the security of their online payments (41 %),

[16] Cybersecurity Insiders, *GermanWiper Ransomware attack warning for Germany*, undated.

[17] European Commission, *Factsheet on cybersecurity*, September 2017.

[18] These losses may include: lost revenue; costs for repairing damaged systems; potential liabilities for stolen assets or information; customer retention incentives; higher insurance premiums; increased protection costs (new systems, employees, training); potential settlement of compliance costs or litigation.

[19] NTT Security, *Risk: Value 2018 Report*.

[20] European Commission, *Special Eurobarometer 499 – Europeans' attitudes towards cyber security*, January 2020.

being unable to inspect goods or ask a real person for advice, or to say they are afraid they might not receive the goods or services they buy online (both 22 %);

- over three quarters (76 %) of respondents believe that the risk of becoming a victim of cybercrime is increasing. However, far fewer (52 %) think they can protect themselves sufficiently against it – and this represents a decline of nine percentage points since 2018.
- still, just over half of respondents (52 %) think they are well informed about cybercrime, but only 11 % say they feel very well informed.

Cybersecurity is relevant to social cohesion and political stability

A new threat: cybersecurity and disinformation

13 The spread of deliberate, systematic large-scale **disinformation is an acute strategic challenge for our democracies**[21]. Disinformation and "fake news" have the potential to divide societies, sow mistrust and even undermine social cohesion and confidence in democratic processes (see ***Box 5***).

[21] According to the study *The Global Disinformation Order* by Oxford University (September 2019), the number of countries with political disinformation campaigns has more than doubled to 70 in the last two years.

Box 5

Disinformation

The European Commission defines disinformation as the creation, presentation and dissemination of verifiably false or misleading information for the purposes of economic gain or intentionally deceiving the public, when this could cause public harm[22]. Public harm could include undermining democratic processes or threats to public assets such as health, the environment and security.

As opposed to illegal content (which includes hate speech, terrorist content or child sexual abuse material), disinformation covers content that is legal. It therefore intersects with the fundamental core EU values of freedom of expression and media freedom. Under the Commission's definition, disinformation does not include misleading advertising, reporting errors, satire and parody, or clearly-identified partisan news and commentary.

14 New technologies and software enable disinformation to be spread easily and comparatively cheaply through **social and other online media**. Disinformation typically concentrates on sensitive topics that are likely to polarise opinion and stir up emotions, and are therefore more likely to be shared. Such topics include health issues (e.g. anti-vaccination campaigns), migration, climate change or social justice issues.

Disinformation campaigns by third countries to influence democratic processes

15 Disinformation aims to polarise democratic debate, create or intensify tensions in society and undermine electoral systems, and has a wider impact on European societies and security. It ultimately impairs freedom of opinion and expression. Disinformation is often **sponsored by actors in third countries**, aiming to destabilise our societies and democratic systems. In this context, large-scale disinformation campaigns may also involve network hacking. An example of that is the Russian influence campaign in the UK referendum on leaving the European Union (see ***Box 6***).

[22] European Commission, *Communication on tackling online disinformation*, COM(2018) 236.

Box 6

Russian disinformation campaigns targeting democratic decision processes[23]

In mid-2016, actors from Russia had launched a campaign to influence the United Kingdom's June 2016 referendum vote to leave the EU. One analysis of tweets found that in the 48 hours leading up to the vote, over 150 000 Russian accounts tweeted about *#Brexit* and posted more than 45 000 messages about the vote. On the day of the referendum, Russian accounts tweeted 1 102 times with the hashtag *#ReasonsToLeaveEU*.

16 Combating disinformation represents a major challenge given the need to strike the right balance between security and our fundamental rights and freedoms, encouraging innovation and an open market. The EU has taken a number of measures to **address disinformation**.

- In 2015, the EEAS-based **East StratCom Task Force** was set up to challenge Russian disinformation campaigns[24]. Experts have praised its work in promoting EU policies, supporting independent media in the European Neighbourhood countries, and forecasting, tracking and tackling disinformation[25].

[23] Park advisors, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Christina Nemr and William Gangware, 2019.

[24] European Council Conclusions, EUCO 11/15, 20 March 2015. Two additional Task Forces have been added since, for the Western Balkans and the Neighbourhood South.

[25] An Atlantic Council report called for the EU to require all Member States to send national experts to the Task Force. See: D. Fried and A. Polyakova, *Democratic Offense Against Disinformation*, 5 March 2018.

- In 2018, ENISA issued a **communication on tackling online disinformation**[26]. Action includes helping to make content more trustworthy and supporting efforts to increase media and news literacy.
- The Commission's Joint Research Centre has developed a voluntary, **self-regulatory code of practice**, based on existing policy instruments, which has been adopted by online platforms and the advertising industry[27].
- An independent European **network of fact-checkers** has been launched.

Disinformation in times of Covid-19 and the EU´s response to it

17 Disinformation has also been a problem in the context of the **Covid-19 health crisis**[28] (see ***Box 7*** for examples of such disinformation).

[26] ENISA, *Strengthening Network & Information Security & Protecting against Online Disinformation ("Fake News")*, April 2018.

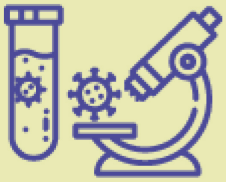
[27] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, April 2018.

[28] Reuters Institute and University of Oxford, *Types, Sources, and Claims of Covid-19 Misinformation*, April 2020.

Box 7

Examples of disinformation relating to Covid-19 reported by the Commission[29]

False claims such as "drinking bleach or pure alcohol can cure the coronavirus infections": on the contrary, drinking bleach or pure alcohol can be very harmful. **Belgium's Poison Control Centre has recorded an increase of 15 % in the number of bleach-related incidents.**



Conspiracy theories, such as the claim that coronavirus is "an infection caused by the world's elites for reducing population growth". The scientific evidence is clear: the virus comes from a family of viruses originating in animals that include other viruses such as SARS and MERS.

Non-scientific claims that "5G installations would be spreading the virus". These theories had no specific substantiation and led to attacks on masts.

18 In March 2020 the Commission, ENISA, CERT-EU and EUROPOL issued a **joint statement on Covid-19-related threats**[30], stating that malign actors were actively exploiting the challenging circumstances during the public health crisis to target remote workers, businesses and individuals alike. Moreover, ENISA has developed dedicated information campaigns for sectors affected by disinformation during the Covid-19 pandemic[31].

---

29 European Commission, *Tackling coronavirus disinformation*, undated.

30 Joint Statement European Commission, ENISA, CERT-EU and Europol, *Coronavirus outbreak*, 20 March 2020.

31 ENISA, *Information sheets relating to Covid-19*, 2020.

Fact-checking is instrumental to combating disinformation

19 The EU has also stepped up its efforts to support European fact-checkers and researchers on disinformation. In particular, it has established a **European Digital Media Observatory** to examine and better understand the phenomena of disinformation: relevant actors, vectors, tools, methods, dissemination dynamics, prioritised targets and the impact on society. Other examples of EU-funded projects addressing disinformation are PROVENANCE, SocialTruth, EUNOMIA and WeVerify.

20 In 2018, with its **Code of Practice on disinformation**[32], the EU proposed the first worldwide self-regulatory set of standards to fight disinformation. That voluntary code was signed by platforms, leading social networks, advertisers and the advertising industry in October 2018. Signatories are Facebook, Twitter, Mozilla, Google and associations and members of the advertising industry. Microsoft subscribed to the Code of Practice In May 2019. TikTok joined the code in June 2020.

Securing the 2019 elections to the European Parliament

21 The legitimacy of our European democratic systems is based on an informed electorate expressing its democratic will through **free and fair elections**. Any attempt to maliciously and intentionally undermine and manipulate public opinion therefore represents a grave threat to our societies. Interference in elections and electoral infrastructure may seek to influence voter preferences, turnout or the election process itself, including actual voting, as well as vote tabulation and communication. In the wake of the UK referendum, the 2019 European elections led to the first coordinated actions between Member States to **protect the integrity of democratic elections**: those to the European Parliament, but also those to national parliaments.

22 As already stated above, the Commission issued a **Communication on tackling online disinformation: a European approach**[33] in April 2018. This was followed by an **Elections Package** in September 2018[34] designed to protect the EU and Member State elections from disinformation and cyber attacks. The package focused on data

---

[32] *EU Code of Practice on Disinformation*, September 2018.

[33] European Commission, *Tackling online disinformation: a European Approach*, COM(2018) 236 final.

[34] European Commission, *State of the Union 2018*, September 2018.

protection, transparency of political advertising and funding, cybersecurity and elections, as well as sanctions for abuse of data protection rules by political parties. Moreover, there was a **joint exercise** to test how effective Member States and the EU's response practices and crisis plans are in protecting the elections to the European Parliament (see ***Box 8***).

Box 8

ELEx19 – protecting the 2019 elections to the European Parliament[35]

The ELex19 exercise on the resilience of the upcoming European Parliament elections aimed to identify ways to prevent, detect and mitigate cybersecurity incidents that may have affected the 2019 elections.

Based on various scenarios featuring cyber-enabled threats and incidents, the exercise allowed participants to:

— acquire an overview of the level of resilience (in terms of policies adopted, available capabilities and skills) of election systems across the EU;

— enhance cooperation between relevant authorities at national level (including election authorities and other relevant bodies and agencies);

— test existing crisis management plans as well as relevant procedures to prevent, detect, manage and respond to cybersecurity attacks and hybrid threats, including disinformation campaigns;

— improve cross-border cooperation and strengthen the link with relevant cooperation groups at EU level (e.g. Election Cooperation Network, NIS Cooperation Group, CSIRTs Network); and

— identify all other potential gaps as well as adequate risk mitigation measures which should be implemented ahead of the European Parliament elections.

More than 80 representatives from the EU Member States, together with observers from the European Parliament, the Commission and the EU Agency for cybersecurity, participated in this exercise.

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 5 April 2019.

23 Finally, in December 2018, the European Council adopted an **Action plan against disinformation**[36] to provide a coordinated response and to complement national efforts. This action plan included specific actions based on four pillars: improving the capabilities of Union institutions to detect, analyse and expose disinformation; strengthening coordinated and joint responses to disinformation; mobilising the private sector to tackle disinformation; and raising awareness and improving societal resilience.

Cybersecurity in the EU: competences, actors, strategies and legislation

Cybersecurity is primarily a Member State responsibility

24 In the EU, cybersecurity is primarily the **responsibility of the Member States**. This is particularly the case as regards the protection of sensitive information relating to national security. All Member States have a **National Cybersecurity Strategy** (NCSS) to help them tackle risks that could potentially undermine the achievement of economic and social benefits from cyberspace. However, Member States still differ in terms of their capacity and commitment regarding cybersecurity.

25 The EU has a role to play in building a **common regulatory framework** within the EU's single market and creating the conditions for Member States to work effectively together in different policy areas with cybersecurity relevance, such as justice and home affairs, the single market, transport, public health, consumer policy and research. In external policy, cybersecurity features in diplomacy, and is increasingly part of the EU's emerging defence and security policy.

26 The main cybersecurity **actors at EU level** are described in ***Box 9*** below.

---

[36] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Action Plan against Disinformation*, JOIN(2018) 36 final. The plan focuses on: improving EU institutions' capabilities to detect, analyse and expose disinformation; strengthening coordinated and joint responses; mobilising the private sector; and raising awareness and improving societal resilience.

Box 9

The main cybersecurity actors at EU level

The **European Commission** aims to increase cybersecurity capabilities and cooperation, strengthen the EU as a cybersecurity player, and mainstream cybersecurity into other EU policies.

A number of the EU agencies support the Commission, notably **ENISA**, **EC3** and **CERT-EU**. The **European Union Agency for Cybersecurity** (known as **ENISA** due to its original name, the European Network and Information Security Agency) is principally an advisory body and supports policy development, capacity building and awareness raising. EUROPOL's **European Cybercrime Centre (EC3)** was established to strengthen the EU's law-enforcement response to cybercrime. A **Computer Emergency Response Team (CERT-EU)**, supporting all Union institutions, bodies and agencies, is hosted by the Commission.

The **European External Action Service (EEAS)** takes the lead on cyber defence, cyber diplomacy and strategic communication, and hosts intelligence and analysis centres. The **European Defence Agency (EDA)** aims to develop cyber defence capabilities.

At EU level, Member States act through the **Council**, which has numerous coordination and information-sharing bodies (among them the Horizontal Working Party on Cyber Issues). The **European Parliament** acts as co-legislator.

Private sector organisations, including industry, internet governance bodies, and academia, are contributing partners in policy development and implementation, for example through a contractual public-private partnership (**cPPP**).

The EU's cyber strategy: cybersecurity has been a major concern since 2013

27 Cybersecurity has been a major political concern at least since 2013 when the Commission adopted its **cybersecurity strategy**[37]. This strategy has five core objectives:

- increasing cyber resilience;

[37] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final, 7 February 2013.

- reducing cybercrime;
- developing cyber defence policies and capabilities;
- developing industrial and technological cybersecurity resources;
- establishing an international cyberspace policy aligned with core EU values.

In the subsequent years, the issue of cybersecurity was also addressed by other EU strategies (see ***Box 10***).

Box 10

Further EU strategies addressing the issue of cybersecurity

- the **European Agenda on Security** (2015)[38], which was aimed at improving law enforcement and the judicial response to cybercrime, mainly by renewing and updating existing policies and legislation;
- the **Digital Single Market Strategy** (2015)[39], which was aimed at creating better access to digital goods and services: strengthening online security, trust and inclusion are essential to this;
- the **EU Global Strategy** (2016)[40], which set out a number of initiatives to boost the EU's role in the world. Cybersecurity, and the rebuttal of disinformation through strategic communication, formed a core pillar in this.

28 Moreover, in 2017, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued a **joint communication on cybersecurity for the EU**[41] to the European Parliament and the Council, in which they

[38] European Commission, *The European Agenda on Security*, COM(2015) 185 final, 28 April 2015.

[39] European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, 6 May 2015.

[40] EEAS, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, June 2016.

[41] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450, 13 September 2017.

called for more robust and effective structures to promote cybersecurity and to respond to cyber attacks in the Member States, but also in the EU institutions, agencies and bodies.

29 In July 2020, the European Commission updated its 2015 agenda and adopted the **EU Security Union Strategy**[42] for 2020-2025, identifying cybersecurity as an issue of strategic importance. In this strategy, the Commission in particular highlights what are known as hybrid threats involving both cyber attacks and disinformation campaigns, with state and non-state actors from third countries acting in concertation, with the intention of manipulating the information environment and attacking core infrastructures.

The EU's cybersecurity legislation: the Network and Information Security Directive, the GDPR, the Cybersecurity Act and a new sanction mechanism

30 As the main pillar of the 2013 cybersecurity strategy, the legal centrepiece is the 2016 **Network and Information Security (NIS) Directive**[43], the first EU-wide legislation on cybersecurity. The directive aims to achieve a minimum level of harmonised capabilities by obliging Member States to adopt national NIS strategies and create single points of contact and computer security incident response teams (CSIRTs)[44]. It also sets security and notification requirements for operators of essential services in critical sectors and digital service providers.

31 Member States had to transpose **the NIS Directive into their national laws** by May 2018. They also had to identify so-called "operators of essential services" by

---

[42] European Commission, *Communication on the EU Security Union Strategy*, COM (2020)605 final, 24 July 2020.

[43] 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.

[44] These are integrated into cooperative structures established by the directive, the CSIRTS Network (a network composed of EU Member States' appointed CSIRTs and CERT-EU; ENISA hosts the secretariat) and the Cooperation Group (supports and facilitates strategic cooperation and information exchange among Member States; the Commission hosts the secretariat).

November 2018. The European Commission is required to review the functioning of this Directive periodically. From July to October 2020, as part of its key policy objective to make "Europe fit for the digital age" as well as in line with the objectives of the Security Union, the Commission held a consultation, with the results of to be used for a first evaluation and ex-post impact assessment of the NIS Directive.

32 In parallel, the **General Data Protection Regulation**[45] (GDPR) came into force in 2016 and has been applied since May 2018. Its objective is to protect European citizens' personal data by setting rules on its processing and dissemination. It grants data subjects certain rights and places obligations on data controllers (digital service providers) regarding the use and transfer of information.

33 Moreover, the EU´s **Cybersecurity Act**[46] introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes. That means that companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the EU. The EU Cybersecurity Act has also set up the **European Union Agency for Cybersecurity** (ENISA, taking over from the former European Network and Information Security Agency). It mandates the agency to increase operational cooperation at EU level, by helping EU Member States who request it to handle cybersecurity incidents and supporting the coordination of the EU in the event of large-scale cross borders cyber attacks and crises.

34 Finally, in May 2019, the Council established a legal instrument, which allows the EU to impose targeted restrictive **measures to deter and respond to cyber attacks** that

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[46] Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, 17 April 2019.

constitute an external threat to the EU or its Member States[47]. As a result, the EU has the legal power to sanction persons or entities that:

- are responsible for cyber attacks or attempted cyber attacks; or
- provide financial, technical or material support for such attacks; or are involved in other ways.

In July 2020, the Council used these new prerogatives for the first time (see ***Box 11***).

Box 11

Getting robust – the EU imposes the first ever sanctions against cyber attacks[48]

In July 2020, the Council imposed restrictive measures against six individuals and three entities responsible for or involved in various cyber attacks. These include the attempted cyber attack against the Organisation for the Prohibition of Chemical Weapons and those publicly known as "WannaCry", "NotPetya", and "Operation Cloud Hopper".

The sanctions imposed include a travel ban and an asset freeze. In addition, EU persons and entities are forbidden from making funds available to those listed.

Cybersecurity and cyber defence

35 In recent years, cyberspace has become increasingly militarised[49] and weaponised[50]. It is now considered as the fifth domain of warfare in addition to land,

[47] Council Decision (CFSP) 2019/797 concerning restrictive measures against cyber attacks threatening the Union or its Member States, 17 May 2019.

[48] Council Decision (CFSP) 2020/1127 of 30 July 2020 amending the aforementioned Decision (CFSP) 2019/797 concerning restrictive measures against cyber attacks threatening the Union or its Member States.

[49] Centre for European Policy Studies, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, November 2018.

[50] The malware behind the Wannacry ransomware attack which was attributed to North Korea by the United States, the UK and Australia, was originally developed and stockpiled by the US National Security Agency to exploit vulnerabilities in Windows.

sea, air and space. An **EU Cyber Defence Policy Framework** was adopted in 2014, and updated in 2018[51]. The 2018 update identifies priorities, including the development of cyber defence capabilities, as well as the protection of the EU Common Security and Defence Policy (CSDP) communication and information networks. Cyber defence also forms part of the Permanent Structured Cooperation (PESCO) framework and EU-NATO cooperation.

36 Instances of using cyberspace for political means and aggressively testing and penetrating EU and Member State cybersecurity have become common. These cyber espionage and hacking activities – targeting national governments, political entities and the EU institutions in order to extract and collect classified information – suggest that sophisticated cyber espionage and data manipulation operations are being carried out against the EU and its Member States. The EU's **Joint Framework on countering hybrid threats** (2016) tackles cyber threats to both critical infrastructure and private users, highlighting the fact that cyber attacks can also be carried out through disinformation campaigns on social media[52]. It also notes the need to improve awareness and enhance cooperation between the EU and NATO, which was given substance in the Joint EU-NATO Declarations of 2016 and 2018[53].

Cybersecurity-related spending in the EU: scattered and lagging behind

Less spending on cybersecurity in the EU-27 than in the USA

37 It is difficult to estimate public spending on cybersecurity, due to its crosscutting nature and because cybersecurity and general IT spending are often

Source: A. Greenberg, WIRED, 19 December 2017. In the wake of the attacks, Microsoft condemned the stockpiling of software vulnerabilities by governments and repeated its call for the need for a Digital Geneva Convention.

[51] *EU Cyber Defence Policy Framework (2018 update)*, 14413/18, 19 November 2018.

[52] European Commission/European External Action Service, *Joint Framework on countering hybrid threats: a European Union response*, JOIN(2016) 18 final, 6 April 2016.

[53] Joint declaration by the Presidents of the European Council and the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 8 July 2016 and 10 July 2018.

indistinguishable[54]. This said, available data would indicate that **public spending on cybersecurity** in the EU has been comparatively low:

- In 2020, the USA federal government budget on cybersecurity alone was around **$17.4 billion**[55].
- In comparison, the Commission has estimated public spending on cybersecurity to range between **one and two billion euros** per year for all EU Member States (which taken together have nearly the same GDP as the USA)[56].
- For many Member States, public spending on cybersecurity as a percentage of GDP is estimated at **one-tenth of USA levels**, or even lower[57].

2014-2020: EU funding for cybersecurity scattered over several different instruments

38 According to the Commission[58], there are at least **ten different instruments** under the EU's general budget through which matters related to cybersecurity can be financed (see ***Box 12*** for the main programmes in financial terms). In total, EU funding for non-military cybersecurity has amounted to **less than €200 million per year** during the 2014-2020 period. There is also no EU-wide funding instrument which supports Member States in coordinating their cybersecurity activities.

---

54 European Commission, COM(2018) 630 final, 12 September 2018.

55 The White House, *Cybersecurity budget fiscal year 2020*.

56 European Commission, Commission Staff Working Document: Impact Assessment Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027", SWD(2018) 305 final, 6 June 2018.

57 The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, December 2016.

58 European Commission, *Impact assessment accompanying the proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*, SWD(2018) 403 final, 12 September 2018.

Box 12

EU programmes supporting cybersecurity projects (2014-2020)

- The EU's **Horizon 2020 research programmes** allocated about €600 million to cybersecurity and cybercrime projects for the period 2014-2020. This includes €450 million for the cybersecurity cPPP ("contractual public-private partnership") for 2017-2020, with the aim of attracting an additional €1.8 billion from the private sector;
- the **European Structural and Investment Funds (ESIF) provide for** a contribution of up to €400 million for Member States' investments in cybersecurity until the end of 2020;
- the **Connecting Europe Facility (CEF)** financed investments for about €30 million per year. This includes the co-financing of the national Computer Emergency Response Teams (CERTs) which Member States are required to set up under the NIS Directive for about €13 million per year, from 2016 to 2018[59];
- the **Internal Security Fund – Police (ISF-P)** supports studies, expert meetings, and communication activities; these amounted to nearly €62 million between 2014 and 2017. Member States can also receive grants for equipment, training, research and data collection under shared management. 19 Member States have taken up these grants, for a total of €42 million;
- the **Justice Programme** provided €9 million to support judicial cooperation and mutual legal assistance treaties, with a specific focus on the exchange of electronic data and financial information.

39 Moreover, €500 million have been allocated from the EU budget to the **European Defence Industrial Development Programme** in 2019 and 2020[60]. The programme focuses on improving the coordination and efficiency of Member States' defence

[59] Article 9(2), of 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 (the "NIS Directive").

[60] European Commission, Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry (OJ L 200, 7.8.2018, p. 30).

spending through incentives for joint development. It aims to generate a total of €13 billion in post-2020 defence capability investment through the European Defence Fund, some of which will cover cyber defence. Finally, under the **European Security Initiative**, the European Investment Bank will provide €6 billion in dual-use funding (research and development/cybersecurity and civilian security) between 2018 and 2020[61].

2021-2027: the new Digital Europe programme

40 With its July 2020 conclusions on the new Multiannual Financial Framework (MFF) for the period 2021-2027, the Council decided that the **Digital Europe programme (DEP)**[62] would invest in key strategic digital capacities, such as the EU's high-performance computing, artificial intelligence and cybersecurity. It will complement other instruments, notably Horizon Europe and the Connecting Europe Facility, in supporting the digital transformation of Europe.

41 The Council has also decided to allocate €6.8 billion to the DEP for the period 2021-2027, or about **€970 million per year**. This is a considerable increase compared to 2014-2020, but still less than initially proposed by the Commission (€8.2 billion for that same period, with €2 billion euro dedicated to strengthening the EU cybersecurity industry and overall societal protection, for example by supporting the implementation of the NIS Directive).

---

[61] European Investment Bank, *The EIB Group Operating Framework and Operational Plan 2018*, 12.12.2017.

[62] European Commission, *Europe investing in digital: the Digital Europe Programme*, September 2020.

PART II – Overview of the SAIs' work

Introduction

42 Cybersecurity and our digital autonomy have become subjects of strategic importance for the EU and its Member States. Weaknesses in cybersecurity governance persist in the public and private sectors across all Member States, albeit at different levels. This impairs our ability to limit and, when necessary, respond to cyber attacks.

43 Nevertheless, in 2018 a survey of the supreme audit institutions (SAIs) in the EU showed that around half had never audited the area of cybersecurity. Since then, the SAIs have geared up their audit work on cybersecurity, with a particular focus on data protection, system readiness against cyber attacks, and the protection of essential public utilities systems. They also examined other highly relevant subjects. Understandably, not all of these audits can be made public, as some may concern sensitive (national security) information.

44 Because of the importance of cybersecurity for the functioning of our societies and political institutions, the Contact Committee decided to dedicate this year's audit compendium to this topic. This part II summarises the results of selected audits carried out by the 12 contributing Member States' SAIs and the European Court of Auditors regarding cybersecurity. Each participating SAI contributed with one selected audit report that is further summarised in part III. Many other audits were undertaken on the subject, as can be seen by the further reports indicated by the participating SAIs.

Audit methodology and topics covered

45 Concerning the type of audit carried out for the audit reports summarised in this Compendium, most of the SAIs that contributed had carried out performance audits on subjects related to cybersecurity, while two (the Polish and the Hungarian SAIs) had carried out compliance audits and one (the ECA) had performed a policy review.

46 When determining their audit approach, most of the SAIs designed their audits to include at least two ways of assessing the audit subject. That could consist of a review of high-level (e.g. national) strategic documents or defined policies, of a review of procedures to assess their compliance with the established COBIT methodology (see ***Box 13***) or of a review of the effectiveness of IT management systems in place. One SAI (the Netherlands Court of Audit) even used ethical hackers to test the effectiveness of

cybersecurity systems in border control and critical water structures. In ***Box 14*** we summarise schematically the methods and techniques the different SAIs used to conduct their audit work.

Box 13

What is COBIT?

Control Objectives for Information and Related Technology (COBIT) is a framework of recognised best practices and procedures for IT management and IT Governance, defined by ISACA – the Information Systems Audit and Control Association. It helps the organisation to achieve strategic objectives through an effective use of available resources and minimisation of the IT risks. COBIT interconnects enterprise governance and IT governance. This connection is made by linking business and IT goals, defining metrics and maturity models to measure achievement of objectives and defining the responsibilities of owners of business and IT processes.

47 The topics addressed while auditing cybersecurity varied widely. Some SAIs audited very specific areas of public interest; the Netherlands SAI, for example, audited the cybersecurity of its vital sea defences and water management systems. Others, such as the Irish and Hungarian SAIs, had addressed more horizontal questions, such as the implementation of the national cybersecurity strategy and the protection of personal data and national data assets. Nevertheless, all SAIs addressed issues that might have a negative impact on public services or infrastructure.

48 The Estonian and Lithuanian SAIs recognised the strategic importance of national data assets, which have crucial importance in national security and the protection of their integrity against external cyber attacks. The Danish SAI devoted an audit specifically to assessing the security of four public bodies with regard to ransomware attacks. The Netherlands, Polish and Portuguese SAIs audited the effectiveness of different IT systems supporting border control checks (respectively at Schiphol airport, the Chief Border Guards Command and the Ministry of Internal Affairs and Administration in Poland and the Portuguese borders), which therefore also addressed security within the EU as well.

Audit period

49 The selected audit reports contained in this Compendium were published between 2014 and 2020. Most had an audit period spanning two or more years, although four (Denmark, Estonia, France and Portugal) had audited periods of one year.

Audit objectives

50 The different SAIs contributing to this Compendium addressed a variety of risks while conducting their audit work. The risks addressed in their contributions were: threats to individual EU citizens' rights through mishandling of personal data, risk for institutions of not being able to deliver an important public service or having constrained performance, serious consequences for public security, welfare and the economy in the Member State as well as cybersecurity within the EU. At least four of the SAIs (Estonian, Hungarian, the Netherlands and Portuguese) covered three or more of the topics mentioned in their audit reports included in this compendium.

51 Cybersecurity remains the remit of Member States. Nevertheless, as EU legislation has become broader and more specific over time, most of the institutions and bodies audited by the SAIs already contribute to achieving the EU Cybersecurity strategic objectives, though to at differing extent. For example, Ireland's Office of the Comptroller and Auditor General audited the implementation of the EU Network and Information System Directive, which aims to improve the resilience of key network and information systems and advised on how to improve it. Similarly, the State Audit Office of Hungary in its audit covered the aspect of compliance with existing EU directives.

52 ***Box 14*** also identifies when the outcome of the audit either contributed to an increase in the auditees' cyber resilience, to a reduction of cybercrimes, or would help to develop cyber defence policies and strengthen competencies, improve the development of technologies and make progress in cooperation at international level; those being notably the main objectives of the EU cybersecurity strategy. Recommendations provided by SAIs in most of the cases addressed more than two strategic objectives that the EU aims to reach.

53 In addition, the audit work carried out by the SAIs identified security or implementation gaps that prompted the audited institutions to make additional

efforts. For instance, during the audit work four institutions audited in Denmark already started implementing several of the forward-looking security controls to increase significantly the level of protection against ransomware attacks, developing defence capabilities and increasing cyber resilience, thus reducing their exposure to cybercrime in the future.

54 We also see that audit recommendations were submitted at various levels of management and responsibility, addressing central government, operational level-ministries and agencies, or IT systems owners.

Box 14

Overview of SAIs' audit work for the contributions provided in the compendium (part 1)

Main focus area		Denmark	Estonia	Ireland	France	Latvia	Lithuania	Hungary	The Netherlands	Poland	Portugal	Finland	Sweden	EU (ECA)
Audit type	Performance	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Compliance							✓		✓				
	Review													✓
Audit approach	Review of policies	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Review of procedures	✓	✓		✓		✓	✓		✓	✓	✓		
	Review of systems	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Assessing robustness by direct testing								✓		✓			
Threats addressed	Impact on individual rights		✓		✓			✓			✓			✓
	Impact on public infrastructure or services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Impact on national security		✓	✓		✓	✓	✓	✓		✓			
	Impact on security within EU	✓							✓		✓			✓

Overview of SAIs' audit work for the contributions provided in the compendium (part 2)

Main focus area		Denmark	Estonia	Ireland	France	Latvia	Lithuania	Hungary	The Netherlands	Poland	Portugal	Finland	Sweden	EU (ECA)
EU Cybersecurity strategic objectives covered	Increasing cyber resilience	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Reducing cybercrime	✓					✓							✓
	Developing defence policies and capabilities	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Developing technological resources				✓	✓			✓				✓	
	Improving international cooperation (policies)			✓				✓						✓
Recommendations' addressee level	Central government	✓	✓				✓					✓	✓	✓
	Operational (ministries and agencies)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	IT system owners	✓			✓			✓	✓	✓				

Main audit observations

55 The main audit observations made by the SAIs are summarised in the following sections.

Performance audits

56 The **Danish *Rigsrevisionen*** assessed whether selected essential government institutions had satisfactory protection against ransomware. Government institutions are frequent targets of cyber attacks and ransomware is currently one of the biggest threats to cybersecurity. The audit concerned the Danish Health Data Authority, the Ministry of Foreign Affairs, Banedanmark (the Danish rail network) and the Danish Emergency Management Agency. These four institutions were selected because they are responsible for delivering essential services in health, foreign affairs, transport, and emergency preparedness, where ensuring data access can be of critical importance. The audit found that the four institutions did not have satisfactory protection against ransomware. The audit work showed that several common security controls to mitigate attacks had not been implemented by the four institutions. The audit concluded that it was important for the institutions to consider implementing forward-looking security controls to increase their resilience to ransomware attacks.

57 The **Estonian *Riigikontroll*** recognised that the preservation of Estonian independence requires not only the physical defence of the territory, but also protection of the digital assets of primary importance to the State. The digital assets in need of most protection are data concerning citizens, the territory and legislation. Data regarding the property, real estate and rights of Estonian residents also need to be secured. The Estonian Audit Office considered the possibility of cyber threats in the event of an escalation of security problems. Such risk scenarios and an increase in the number of information security incidents, such as cyber attacks and data leaks, could jeopardise the data and databases that are of greatest importance to the State. Therefore, the audit looked at how the State determined which data and databases were critical to guaranteeing national security. The audit concluded that despite the implementation of the three-level baseline security system ISKE[63] that is mandatory

[63] ISKE is an information security standard that is developed for the Estonian public sector; it is compulsory for state and local government organisations who handle databases/registers.

for state agencies, there were significant deficiencies in guaranteeing information security in several critical databases.

58 The **Irish *Office of the Comptroller and Auditor General*** reviewed the progress made in respect of cybersecurity measures since the establishment of the Irish National Cyber Security Centre. The Centre, run by the Department of Communications, Climate Action and Environment, was established in 2011. Its primary focus is on securing government networks, on assisting industry and individuals in protecting their own systems, and on securing critical national infrastructure. The audit concluded that although the National Cyber Security Centre performed a critical function, the level of resourcing in its first four years of operation was significantly less than that originally envisaged and the overall strategic direction of the Centre was lacking a strategic plan. Further, more clarity was required in relation to the respective roles of bodies involved in the investigation of cybercrimes and national security incidents. Further, the requirements of the EU Network and Information Systems Directive relating to the development of a national strategy were still to be implemented.

59 The **French *Cour des comptes*** scrutinised "*Parcoursup*", a new digital platform that operates as an information source on available university courses and entry requirements, the purpose of which is to strengthen the match between secondary students' aptitude and academic results and the content of tertiary education courses. The audit found that the government had successfully centralised access to all post-secondary study through the digital platform in order to deal with the expansion of higher education. However, the previous system had been hastily reworked to become the new "*Parcoursup*", with no substantive structural changes. The information system's vulnerabilities in terms of security, performance and robustness were therefore not remedied. The platform is still affected by significant risks in terms of the quality and continuity of public service and personal data security.

60 The **Latvian *Valsts Kontrole*** completed a performance audit on the efficiency of the public information and communications technology (ICT) infrastructure. The purpose of the audit was to verify whether public administration had a unified approach to the efficient management of ICT infrastructure and whether the institutions had assessed the benefits of centralisation. The audit found that the reluctance of the authorities to manage ICT infrastructure centrally had led to a number of server rooms being established, significantly increasing maintenance costs. Security threats were present in most server rooms, with data centres insufficiently

protected from physical access and environmental risks. In addition, no practice had been introduced in the institutions to carry out regular evaluations of whether it would be cheaper to maintain the ICT infrastructure internally, cooperate with another institution or outsource ICT maintenance. The audit recommended a regular monitoring system that would enable to evaluate the entire public administration as a single system.

61 The **Lithuanian *Valstybės kontrolė*** recognised the importance of critical electronic State information resources, such as the management of government finances, tax administration and health care being implemented. The loss of critical information and the unavailability of the corresponding information systems could have serious consequences for public security, welfare and the economy. The audit aimed to evaluate the management (general control) and maturity of critical State information resources. It identified systemic problems both in the formation and in implementation of the State information resources policy and in the management mechanism of them. The audit concluded that a low level of maturity of critical State information resources indicated weaknesses in the formation and implementation of the State information resources policy, rendering these resources more vulnerable. In order to increase the security of State information resources, the management mechanism needed to be improved.

62 In 2018, the **Netherlands *Court of Audit*** decided to carry out audits on cybersecurity in sectors that are critical for the society. The first two sectors audited were water management and automated border controls, the first being vital for a nation largely below sea-level, the second due to the position of Amsterdam Schiphol airport as an international hub and gateway to the country. The Minister of Infrastructure and Water Management has designated a number of water structures managed by the Directorate-General for Public Works and Water Management (the auditee) as "critical parts" of the water management sector. Many computer systems used in operating the critical water structures date back to the 1980s and 1990s, a time when cybersecurity was not commonly taken into account. The Minister of Defence and the Minister of Justice and Security share responsibility for border control checks carried out by Dutch border guards at Schiphol airport. Both ministries own IT systems on which the border guards rely. The systems are critical for airport operations and are used to process highly sensitive data. This makes them an interesting target for cyber attacks aimed at sabotage, espionage or manipulation of the border control checks. The audit examined whether the auditees were prepared for dealing with cyber threats and if this was done effectively. In the case of the water

structures the auditee still needed to do more in terms of both detection and response in order to meet its own cybersecurity targets. As to the border controls, the cybersecurity measures were found to be neither adequate nor future-proof.

63 The **Portuguese *Tribunal de Contas*** audited the information systems that support the granting, issuing and use of the Portuguese Electronic Passport (PEP), particularly in the automated screening of passengers by reading biometric data at the Portuguese borders. The audit verified compliance with EU and national law, international standards and guidelines for granting, issuing and using the PEP, including the adequacy of the national legal framework. It examined the effectiveness of key processes associated with the life cycle of the PEP, in particular those associated with granting, issuing and using the PEP. The audit also reviewed critical aspects of the performance of information systems, in particular the fulfilment of security requirements concerning the PEP information systems (SIPEP).

64 The **Finnish *Valtiontalouden tarkastusvirasto*** investigated whether cyber-protection in central government was as effective and cost-efficient as possible. The audit focused on how central government cybersecurity was managed. The audited entities included the authorities governing cyber-protection in central government (the Prime Minister's Office, the Ministry of Finance, and the Ministry of Transport and Communications) and the authorities responsible for centralised cyber-protection tasks and centralised IT services in central government. In the Finnish government, the responsibility for cyber-protection is decentralised, with each corporate body responsible for its own cybersecurity. The audit recommended that the Ministry of Finance should define and implement an extensive operational management model in case of cybersecurity incidents in central government ICT services. The Ministry of Finance should also find out how the cybersecurity of services is to be addressed in funding services throughout their lifecycle and improve operative situational awareness by instructing authorities to report cyber violations to the Cybersecurity Centre.

65 The **Swedish *Riksrevisionen*** addressed the incidence of obsolescent IT systems in central government administration to assess whether the government and the authorities had taken suitable measures to prevent IT systems from becoming an obstacle to effective digitalisation. The audit identified obsolescent IT systems in a large number of government agencies. At many agencies audited, one or more business-critical IT systems were obsolescent and a large proportion of the agencies examined did not have the correct approach to development and administration of IT

support. A large proportion of the agencies lacked an overall description of how strategies, operational processes and systems were linked. The overall conclusion was that most agencies had not yet managed to deal effectively with the problems involved with obsolescent IT systems. The Swedish audit office considers that the problem is so serious and widespread that it is an obstacle to the continued efficient digitalisation of State administration.

Compliance audits carried out on cybersecurity

66 The ***State Audit Office*** **of Hungary** recognised that the security of national data assets is a fundamental interest of society for the preservation and protection of national values. Ensuring the enhanced security of personal and public data within the national data assets of Hungary is essential in order to strengthen citizens' trust in the state and to ensure the continuous and smooth functioning of public administration. The purpose of the compliance audit on data protection was to assess whether the regulatory and operational framework for data protection had been established in Hungary and whether the major data management organisations had complied with the requirements for safe data management and outsourcing of data processing. The audit concluded that the internal regulations of data management organisations regarding data management activities had ensured the protection of the national data assets as part of the national assets, in accordance with the legal provisions in force between 2011 and 2015. Data controllers had properly applied the requirements and the transfer of data to third parties had been implemented appropriately.

67 The **Polish** ***Najwyższa Izba Kontroli*** assessed whether data collected in the systems intended to implement important public tasks were secure. The audit covered six selected institutions carrying out significant public tasks. The degree of preparation and implementation of the Information Security System did not provide an acceptable level of security for the data collected in the IT systems used to perform important public tasks. The information security processes were carried out in a disorderly manner and, in the absence of procedures – intuitive. Of the six units audited, only one had implemented the Information Security System, although it should be noted that its operation had also been affected by significant faults. The audit concluded that general recommendations and requirements relating to IT security need to be developed and implemented at central level, applicable to all public entities.

Reviews of cybersecurity

68 The ***European Court of Auditors*** reviewed the EU's cybersecurity policy landscape and identified the main challenges to effective policy delivery. It covered network and information security, cybercrime, cyber defence and disinformation. The review identified a number of gaps in EU cybersecurity law, and noted that the existing legislation was not consistently transposed by Member States. Finally, the review drew attention to the fact that there was a lack of reliable data on cyber incidents at EU level and no comprehensive overview of spending on cybersecurity by the EU and its Member States. The review also noted resource constraints affecting the EU's cyber-relevant agencies, including difficulties in attracting and retaining talent. Another challenge concerned the misalignment of cybersecurity financing with the EU's strategic goals.

PART III – Summary of SAI reports

Denmark
Rigsrevisionen

Protection against ransomware attacks

Publication date: 2017

Hyperlink to the report: Summary of report (English version)

Audit type and period

Type of audit: Performance Audit

Audited period: April – September 2017

Summary of the report

Audit topic

This report looked at whether selected essential government institutions had satisfactory protection against ransomware.

Government institutions are frequent targets of cyber attacks and ransomware is currently one of the biggest threats to cybersecurity. Ransomware is malicious software that blocks access to data. Generally, ransomware encrypts data and prevents the institutions under attack from using it. Hackers demand a ransom to decrypt the data and enable the institutions to regain access. It follows that ransomware represents a particular threat to the accessibility of data.

A sudden inability to access data can make it difficult for institutions to deliver important services or prevent them from doing so entirely. Institutions affected by a ransomware attack are generally forced to shut down parts of or their entire IT network to investigate the extent of the attack. Ransomware attacks may have a significant economic impact as institutions risk suffering a loss of production, for instance if they are prevented from accessing their IT network or if data collected and processed over an extended period is lost. In 2017, a ransomware attack on the British national health service led to the cancellation of 19 000 operations and appointments.

The management of the institutions should therefore focus on the risk of ransomware attacks and implement the necessary security controls to protect against ransomware and reduce the impact of a potential attack.

The study included the Danish Health Data Authority, the Ministry of Foreign Affairs, Banedanmark (the Danish rail network) and the Danish Emergency Management Agency. These four institutions were selected because they are responsible for delivering essential services in health, foreign affairs, transport and emergency preparedness, where data access can be of critical importance. The Health Data Authority also delivers centralised IT services to the majority of government bodies under the Ministry of Health.

The purpose of the study was to assess whether the four institutions had satisfactory protection against email-based ransomware attacks. *Rigsrevisionen* therefore examined 20 common security controls that provide basic protection against ransomware. In addition, the SAI reviewed five security controls that the institutions should consider in connection with future risk assessments. Forward-looking controls include, for example, new technology that can reduce the number of fake emails entering an institution or detect and send alerts regarding unusual activity on computers. The study was initiated by *Rigsrevisionen* and based on the findings of four IT audits carried out from April to September 2017. The study provides a snapshot of how well protected the institutions were against ransomware. The institutions had the opportunity to implement the 20 common security controls following completion of the IT audits. Therefore, the results of the study concern only the institutions' protection against ransomware at the time of the four IT audits. The study provides a presentation of the performance of the four institutions, but does not include a comparative analysis and ranking of their performance.

Findings and conclusions

It is *Rigsrevisionen's* assessment that the four institutions did not have satisfactory protection against ransomware. The study shows that several common security controls to mitigate attacks had not been implemented by the four institutions. In particular, the Health Data Authority and Banedanmark had considerable gaps in security. This meant that all four institutions were exposed to an increased risk of email-based ransomware attacks that would leave them unable to deliver their services for varying lengths of time. All four institutions have informed *Rigsrevisionen* that they have worked on implementing several of the security controls to increase the level of protection against ransomware since the study was completed.

The institutions' prevention of ransomware attacks, including both internal and external threats, was inadequate. It is of particular concern that none of the institutions ensured that security software patches were up to date, and that three of the institutions had not implemented whitelisting to prevent staff from running malware. This increases the risk of ransomware infecting part of or the entire IT network and spreading.

In three of the institutions, management was not sufficiently focused on the ransomware threat, and the risk assessments carried out by management in the Health Data Authority and Banedanmark did not cover all relevant aspects. This meant that the institutions did not have an up-to-date assessment of the ransomware threat and were therefore in a weak position to prevent new attacks and reduce the impact of future attacks. Management in the Health Data Authority and Banedanmark had not focused sufficiently on risk assessment, and IT security in these two institutions was therefore not based on priorities defined by the management.

Three of the institutions did not have adequate incident response plans in place to help them re-establish their operations after a ransomware attack. It is particularly significant that three of the institutions did not regularly test whether they would be able to restore data and systems affected by a ransomware attack. This increases the risk of the data held by these institutions being lost in connection with a ransomware attack and of the institutions being unable to deliver their services for an extended period of time.

As the risk scenarios are constantly changing, it is important that the institutions consider implementing forward-looking security controls to increase their resilience to ransomware attacks, i.e. controls that facilitate verification of the identity of email senders and can detect and filter out potentially harmful emails. All four institutions are currently working on some of the forward-looking security controls that can help increase their protection against ransomware attacks.

Further reports in the area

Title of the report:	Report on the protection of research data at the Danish universities
Hyperlink to the report:	Summary of report (English version)
Date of publication:	2019
Title of the report:	Report on the protection of IT systems and health data in three Danish regions
Hyperlink to the report:	Summary of report (English version)
Date of publication:	2017
Title of the report:	Report on management of IT security in systems outsourced to external suppliers
Hyperlink to the report:	Summary of report (English version)
Date of publication:	2016
Title of the report:	Report on the access to IT systems that support the provision of essential services to the Danish society
Hyperlink to the report:	Summary of report (English version)
Date of publication:	2015

Estonia
Riigikontroll

Guaranteeing the security and preservation of critical State databases in Estonia

Publication date: May 2018

Hyperlink to the report: Summary of report (English version)
Report (Estonian version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2017

Summary of the report

Audit topic

The preservation of Estonian independence requires not only the physical defence of its territory, but also protection of the digital assets of primary importance to the State with regard to those events that pose the biggest threat. The digital assets in need of most protection are data concerning citizens, the territory and legislation. Data regarding property, real estate and the rights of Estonian residents also need to be secured.

The National Audit Office checked how the State had determined which data and databases were critical to guaranteeing national security. Protection of the security and continuity of these data and databases was checked, including an overview of the tools used for protection.

As Estonia is now a member of NATO and the European Union, its physical security is better guaranteed than before joining these networks. However, Estonia has to consider the possibility of cyber threats in the event of an escalation of security problems. Such risk scenarios and an increase in the number of information security incidents, such as cyber attacks and data leaks, could also jeopardise the data and

databases that are the most important to the State. If the data of primary importance to the State were to be changed without authorisation, leaked or lost, the State would no longer be able to perform necessary functions, including guaranteeing the security of the people, providing necessities, creating the environment required for business and much more. Estonia initially plans to spend about one million euros on storing critical data abroad.

Audit questions

- Did the ministries identify all critical databases and handling requirements?
- Are the critical databases and registers secured?
- Is the long-term continuity of critical data and databases guaranteed?

Findings

The National Audit Office made the following observations about the critical databases audited:

- No action plan or requirements had been established for the implementation of the concept of critical databases. The conditions for selecting critical databases had not been determined and there was no certainty that all the necessary databases were included in the process. The additional protection of databases had been organised informally and was not mandatory for database owners, which was why the data in the five critical databases was not backed up abroad.
- No additional information security rules had been established in critical databases. Neither the information security system ISKE (an information security standard that was developed for the Estonian public sector and is compulsory for state and local government organisations who handle databases/registers), nor any legal act or standard included additional requirements for critical databases, such as backing up the data outside Estonia. Backup copies of the audited databases were taken abroad, but recovering the work of information systems from them had not been tested.
- The implementation of ISKE and related auditing were a problem with regard to critical databases. At the time of the audit, no ISKE audits had been carried out on two of the 10 databases, and the audits had only been organised by the end of this audit (30 November 2017). Only two critical databases had been audited as

frequently as required by law. There were also cases in which the problems highlighted by the auditor had not been solved during the time between two ISKE audits (two-three years).

- In the course of the audit, the National Audit Office found that some important information security measures had not been implemented in some critical databases. For example, the requirements for regular assessment of the vulnerabilities of information systems had not been determined in information security guidelines, regular checks or analyses of event logs had not been carried out, there were no information security training plans or analyses of information security awareness in the area of government that is the basis of such training plans, the integrity of files was not inspected in some cases and no external penetration tests were carried out.

Conclusions and recommendations

The audit revealed that, despite the implementation of the three-level baseline security system ISKE, the use of which is mandatory for State agencies and their audits, there were significant deficiencies in guaranteeing information security in several critical databases, such as the analysis of logs, penetration testing and protection of mobile devices. The special requirements needed for protecting critical data had not yet been established.

The Ministry of Economic Affairs and Communications had launched the first activities required for the protection of critical data, but the critical databases project was at a stage where it would require a legally mandatory set of rules. Nor was there a detailed risk analysis or an action plan for the future.

Backup copies of five critical databases were held at embassies located in foreign countries, but in the event of the physical destruction of the data centres located in Estonia, the preservation of the critical data in the remaining five databases would not be guaranteed.

Two general recommendations were given:

- Determine the rules for additional protection of critical databases, including the selection of critical databases, processing data in these databases and backing up the data that are critical to the State, and assess how to provide additional funding for these activities.

- Analyse the different stages of the establishment of databases both in terms of financial planning and information security, and implement the best project management practices in the implementation of these stages.

Ireland
Office of the Comptroller and Auditor General

Measures Relating to National Cyber Security

Publication date: September 2018

Hyperlink to the report: Summary of report (English version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2011-2018

Summary of the report

Audit topic

The Department of Communications, Climate Action and Environment is responsible for cybersecurity policy in Ireland. The Department is also responsible, through the National Cyber Security Centre, for coordinating the governmental emergency response to any national-level cybersecurity incidents.

The National Cyber Security Centre was established in 2011. Its primary focus is on securing government networks, on assisting industry and individuals in protecting their own systems, and on securing critical national infrastructure.

Audit questions

This examination reviews the progress made in respect of cybersecurity measures since the establishment of the National Cyber Security Centre. In particular, it considers issues relating to:

- the mandate and resourcing for the Centre;
- the National Cyber Security Strategy (2015-2017);

- implementation of the EU Network and Information Systems Directive;
- governance and oversight arrangements.

Findings and conclusions

While the Government decision on the establishment of the National Cyber Security Centre approved annual funding of €800 000, the actual annual funding for cybersecurity between 2012 and 2015 was less than a third of that amount. In 2017, the allocation increased to €1.95 million. Staffing of the Centre almost doubled during 2017 to 14.5 whole-time equivalents. Approval was given to appoint a further 16 staff in 2018.

The National Cyber Security Strategy (2015-2017) set out 12 measures to be achieved over the lifetime of the strategy. As at May 2018, four measures had been completed, four had been partially implemented, and four had not been implemented.

The EU Network and Information Systems Directive aims to improve the resilience of key network and information systems. An assessment of progress in Ireland in relation to each of the three pillars under the Directive found that:

- *Pillar 1 – Improving cybersecurity capabilities of EU Member States.* Partially implemented – structural requirements have been addressed, but gaps remain in strategic planning.
- Pillar 2 – Facilitating cooperation on cybersecurity among EU Member States. Implemented.
- *Pillar 3 – Introducing security measures and incident reporting obligations for key sectors.* Partially implemented – work remains to be done in relation to the identification of critical network and information systems, the formal designation of entities as Operators of Essential Services (OESs) and the management of digital service providers.

The Government decision (July 2011) approving the establishment of the National Cyber Security Centre also approved the setting up of an interdepartmental committee to set and implement policy to address the challenges of cybersecurity in Ireland. While the group met five times between 2013 to 2015, minutes of only one meeting were available for review. The committee has not met since 2015.

The National Cyber Security Strategy Implementation Plan commits to publishing an annual report and to conducting a formal impact assessment of their work in late 2017. These are outstanding, though the work of the Centre is outlined in the Department's annual report.

An assessment of the Centre's performance was formally requested from the Department. No evidence of an assessment having been carried out was provided. The Department stated that performance assessment of the work of the National Cyber Security Centre formed part of the normal performance management and corporate governance of the Department.

The audit concludes:

- Although the National Cyber Security Centre performs a critical function, the level of resourcing in its first four years of operation was significantly less than that originally envisaged.
- The overall strategic direction of the Centre is not clear, with no strategic plan currently in place.
- More clarity is required in relation to the respective roles of bodies involved in the investigation of cybercrimes and national security incidents.
- Requirements of the EU Network and Information Systems Directive relating to the development of a national strategy have yet to be implemented.
- While governance structures have been prescribed, it is not clear how governance arrangements are operating in practice.

There is a lack of transparency around the availability and cost of resources dedicated to cybersecurity.

France
Cour des comptes

Access to higher education: an initial assessment of the law on student guidance and success

Publication date: February 2020

Hyperlink to the report: Report (French version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2019-2020

Summary of the report

Audit topic

The aim of the 2018 law on student guidance and success (*loi relative à l'orientation et à la réussite des étudiants*, ORE) was to improve the three main stages along the pathway followed by young people entering higher education: guidance and support for upper-secondary students, course selection, and success in the initial years of study. It introduced "*Parcoursup*", a new digital platform operating as an information resource on available courses and entry requirements, the purpose of which was to strengthen the match between secondary students' aptitude and results and the content of tertiary education courses.

The first two years of the ORE saw the first step towards transforming access to higher education. Despite numerous constraints, the rollout of "*Parcoursup*" had gone very smoothly, although it still lacked security and sustainability guarantees, and data could have been better exploited, given its importance.

The ORE was enacted to resolve two major problems in educational policy. The first was the high dropout rate among university students. The second was that the old

digital platform had led to deep-seated dissatisfaction because it used random selection as its final stage.

The ORE reform was granted €867 million in funding over five years. It was based on the notion of a "-3/+3" continuum, with the underlying principle that the more upper-secondary students knew about the content of tertiary education courses, the greater their chances of exam success, since they would choose courses that best corresponded to their aptitude and ambitions. The ORE sought to overcome the lack of guidance available to upper-secondary students, and thus to reduce course-switching, which the *Cour* estimated cost almost €550 million per year for the first year of higher education alone.

The auditors carried out an initial assessment of access to higher education in the context of the ORE, looking at the IT security issues raised by the platform.

The information system was characterised by an expansion of load factors (inclusion in 2020 of all higher-education courses and a rapid increase in user numbers in just a few years). This reflected the hasty switch from the previous platform to "*Parcoursup*" without changing the architecture, thus generating significant risks in terms of the quality, continuity, adaptability and further development of the service. The system's weaknesses in the areas of security, performance and robustness had not been corrected. It was possible to set up "*Parcoursup*" rapidly because it was managed in beta mode by a limited group of highly skilled and motivated people, but this approach meant that the arrangement lacked strategic direction and satisfactory governance.

The auditors assessed the quality of the information system and the performance of the new "*Parcoursup*" platform. "*Parcoursup*" was set up under the ORE with the aim of improving the quality of assignment to higher-education courses and thus boosting the graduation rate.

Findings

While "*Parcoursup*" worked satisfactorily, it was exposed to IT risks, which needed to be reduced. Guarantees were needed on the platform's security and sustainability, and greater use could have been made of the data.

An old information system

There was little new in "*Parcoursup*", which had inherited the unwieldiness and frailty of the previous "*Admission Post-Bac*" (APB) platform, along with many unresolved

risks. The information system forming the structural basis of "*Parcoursup*" was taken directly from the earlier platform. Despite being touted as a new assignment tool, the heart of the information system had only been slightly modified since the APB. In fact, over 72 % of the information infrastructure was unchanged, as just under 30 % of the APB code had been rewritten.

The platform's IT underpinnings were designed in the early 2000s to handle about one million applications for around 100 000 places each year, but the scope of the information system was broadened to deal with an annual influx of some 10 million applications for approximately one million places. "*Parcoursup*" came across as an old tool rebranded. The increase in load raised questions about the platform's capacity to achieve its intended purpose.

A poorly-documented information system

Despite the Ministry's efforts at transparency, the source code for "*Parcoursup*" was still 99 % closed. What little was published was of limited interest for understanding, assessing and evaluating the process of assigning applicants to courses.

Like its predecessor, "*Parcoursup*" was a poorly-documented operational information system. The results of the code audit suggested that the application was low-quality and high-risk, and the audit identified numerous critical violations. The system was of poorer quality than other software of a similar age, with a high risk of crashing.

"*Parcoursup*" used both public and closed source code. The open code presented a far higher rate of critical violations than the closed code, meaning that service disruption was a risk. Nor was the platform hacker-safe (July 2018 security audit of the source code). However, at the end of 2019 the Ministry announced that a certification procedure had begun for the "*Parcoursup*" code.

The source code documentation that did exist was neither coherent nor exhaustive. The "*Parcoursup*" code was abnormally complex. The auditors considered that the source code should be restructured to reduce the number of complex components.

The architecture of the "*Parcoursup*" information system was high-risk; archaically, the database was managed manually. The frailty of the system lay in its heavy reliance on operator availability and vigilance. The Ministry acknowledged that high risks were associated with the "*Parcoursup*" architecture, and that these could not be corrected without developing the application further.

The "*Parcoursup*" information system was poorly documented and essentially relied on the expertise of the staff of the national government agency (*Service à Compétence Nationale* SCN). By way of documentation, comments were written in the database at the core of the system, making it difficult to maintain and develop the information system and exploit the data. User information held on the platform could not easily be extracted and evaluated without in-depth investigation. Given the lack of structured technical documentation, the SCN's ability to carry out its strategic tasks depended entirely on the head of the IT centre.

Security strategy – improvements needed

Owing to the sensitivity of the personal data contained in the system, "*Parcoursup*" presents a real security challenge. In principle, all organisations managing an information system must have a formal written information systems security policy (ISSP). Despite being recognised by the Prime Minister as a key service provider, "*Parcoursup*" had no ISSP. Immediate action was required to put one in place.

Each "*Parcoursup*" team had an information systems security officer (ISSO) attached to the IT centre. It would have been good practice to attach the ISSOs directly to the Director of the SCN to guarantee their independence.

As of mid-2019, "*Parcoursup*" was still being made GDPR-compliant. Some measures were still outstanding, in particular the need to formally establish the various procedures used for processing. Personal data security remained inadequate, and too much exhaustive individual data was still stored.

The "*Parcoursup*" unit reported both to the "*Parcoursup*" project manager, assigned from the Minister's office, and to the training strategy and student affairs department of the Directorate-General for Higher Education and Vocational Integration, creating split loyalties. Practical matters relating to the "*Parcoursup*" information system were dealt with at weekly meetings. Although this form of organisation had the advantage of quick reaction times in terms of the day-to-day management of student flows, it left "*Parcoursup*" strategically rudderless.

Finally, the system was not sufficiently transparent. It did not allow best use to be made of the data held on the platform, despite the enormous potential. Mobilising that potential would almost certainly have delivered performance gains.

Conclusions and recommendations

The government had successfully centralised access to post-secondary study through a digital platform combining all education programmes, in order to deal with the generalisation of higher education. The former system had been hastily reworked as "*Parcoursup*", but without substantive structural change. The information system's vulnerabilities in terms of security, performance and robustness had therefore gone unremedied, even though the increase in load was bound to continue given the ultimate aim of including all undergraduate courses. The system was also poorly documented, with a somewhat homespun approach to IT development, and its unusual complexity increased the risks of error in the event of any operational changes. The platform was therefore beset by significant risks in terms of the quality and continuity of public service and personal data security.

The *Cour des comptes* made the following recommendations:

- SCN's IT team should be better staffed, and ORE funding should be redeployed to enhance the human and financial resources of the Sub-Directorate for information systems and statistical research;
- the information system should be established for the long term by correcting its most urgent flaws, modernising or redeveloping its architecture, and documenting the primary databases of both the old system and "*Parcoursup*" in a systematic and structured way;
- the "*Parcoursup*" information system should be endowed with a security policy;
- a joint steering body should be set up for the Ministry of Education and Youth and the Ministry of Higher Education, Research and Innovation to oversee the "*Parcoursup*" platform, with resources redeployed from ORE funding for "guidance" activities.

Latvia
Valsts Kontrole

Has public administration used all opportunities for efficient management of ICT infrastructure?

Publication date: June 2019

Hyperlink to the report: Summary of report (English version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2017-2019

Summary of the report:

Audit topic

The State Audit Office of Latvia completed a performance audit on the efficiency of the public ICT infrastructure. The purpose of the audit was to verify whether the public administration had a unified approach to the efficient management of ICT infrastructure and whether the institutions had assessed the benefits of centralisation. Furthermore, the security of data centres was identified as an important issue in evaluating options for further optimisation planning.

The reluctance of the authorities to manage ICT infrastructure centrally, at least at the level of one ministry, had led to a number of server rooms being established, thus significantly increasing the maintenance costs. In the four ministries audited, their 22 sub-entities were found to use 38 data centres. During the audit, the national audit office witnessed situations where information systems of significant, even national, importance, were located on premises with an insufficient level of security. Not only would optimising the number of server rooms make it possible to reduce ICT expenses, but a sufficient security level could then be provided at a lower cost. Meanwhile high-security server rooms were already available in the institutions but were not used to their full capacity.

Main audit subject

The audit aimed to verify that all the prerequisites for the unified management of the ICT infrastructure were created and implemented such as to promote more efficient and secure use of ICT resources.

Findings and conclusions

ICT governance and optimisation

- There was no long-term vision of ICT development and optimisation either nationally or in the ministries. The ministries and their sub-entities optimised ICT infrastructure in accordance with their understanding and capacity.

Between 2011 and 2017, the total ICT maintenance costs of the audited institutions rose from 17 to 20 million euros per year. No practices were introduced in the institutions to carry out regular evaluations of whether it would be cheaper to maintain the ICT infrastructure themselves, cooperate with another institution or outsource ICT maintenance. Neither ICT centralisation nor ICT decentralisation is seen as a goal in itself, but an analysis of specific situation and alternatives is needed to provide clarity on existing costs and possible alternatives.

ICT security

- The legal framework did not clearly define the security requirements of the ICT infrastructure in a logical system depending on the relevance of the information to be processed. There were no detailed technical requirements for the protection of ICT data centres.

- Shortcomings in security requirements led to costly protection or, on the contrary, the protection of information of national importance was not ensured. Important information systems were even hosted in low-security data centres.

- Security threats existed in most server rooms – data centres were not sufficiently protected from physical access and environmental risks. For the prevention of security threats, at least €247 000 – €765 000 was required, depending on the approach chosen. These included: 1) improving server rooms containing more important information systems and ensuring storage of significant ICT resources in higher-security data centres; or 2) improving all existing server rooms. This, however, would require an amount of investment that the auditors could not justify unless the number of data centres were minimised.

The legal framework was incomplete as there were no detailed security requirements for ICT infrastructure. For instance, there were requirements for various criteria relating to logical security, but no criteria for the physical and environmental safety of the infrastructure, which also affects the availability of systems and data protection. Although public policy planning documents highlighted the importance of ICT infrastructure security and the need to strengthen it, nobody had planned specific activities in this area. The lack of clear, traceable and logical differentiation of security requirements posed the risk that security requirements for processing information of equal importance and significance might vary across the country.

Security in the digital space was monitored by the state centrally, and the state responded to incidents taking place there, but responsibility for the implementation of IT infrastructure security was left to each head of institution. Thus the institutions' understanding of ICT security issues, the assessment of the importance of the information processed and the resources available to the institutions for addressing ICT security issues varied widely.

A regular monitoring system for those processes was needed, in order to evaluate the entire public administration as a single system independently and using standard criteria, to identify different approaches and prevent them by identifying common risks, and to plan preventive actions to mitigate the latter.

Lithuania
Valstybės Kontrolė

Management of Critical State Information Resources

Publication date: June 2018

Hyperlink to the report: Summary of report (English version)
Report (Lithuanian version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2014-2017

Summary of the report

Audit topic

When using critical State information resources – critical electronic information – important governmental functions, such as management of government finances, tax administration and healthcare, are being implemented. Any loss of critical information or unavailability of corresponding information systems could have serious consequences for public security, welfare and the economy. The assessments of general IT control conducted by the National Audit Office of Lithuania (NAOL) from 2006 to 2016 revealed recurring problems in IT management (planning, information architecture definition, organisational structure, changes, ensuring business continuity, data security, IT management monitoring and evaluation). The NAOL carried out an audit of critical State information resources to assess the management and security of these resources and to provide for improvement measures.

The audit aimed to evaluate the management (general control) and maturity of critical State information resources and identify systemic problems.

The NAOL assessed the maturity of IT management in 12 public sector organisations[64] that manage 44 class-one State information systems. The audit was performed following the Public Auditing Requirements and the International Standards of Supreme Audit Institutions. The assessment was carried out in accordance with the COBIT[65] methodology in the following most risky areas: IT strategic planning; determination of informational architecture; IT risk management; change management; assurance of uninterrupted service provision; system security; data management; monitoring and evaluation of IT activities; IT management assurance. The process evaluation included both organisational and national IT management and the interaction of these levels of management.

Audit findings

The trends in changes in maturity level regarding the management of critical State information resources were positive. However, given the growing level of cyber threats, the progress observed was too slow and the security of these resources needed to be increased. This was due to the following weaknesses:

- The system for identifying critical State information resources was not effective enough to allow for the implementation of security solutions meeting actual needs:
  - Assessments designed to prove the criticality of State information resources lacked objectivity, changes were not always evaluated in reassessments, this process was not monitored at national level, and the guidelines for determining criticality did not ensure effective implementation.
  - The system for the identification of critical State information resources and critical information infrastructure was not standardised; resources and infrastructure were identified in different ways based on importance of

[64] State Tax Inspectorate, State Enterprise Centre of Registers, Information Technology and Communications Department, State Social Insurance Fund Board, State Enterprise Agricultural Information and Rural Business Centre, Customs Information System Centre, State Food and Veterinary Service, Office of the Seimas of the Republic of Lithuania, Ministry of Finance, Information Society Development Committee, State Patient Fund, State Forest Service.

[65] COBIT (Control Objectives for Information and Related Technologies) is a standard of the international ISACA organisation setting out best practice for IT management.

information and services, which complicated the process of identifying these resources.

— No national information architecture had been developed to represent the State information systems and their interrelations, show the scale of critical State information resources and allow informed decisions to be made regarding the importance of these resources.

- The management of State information resources needed to be more in line with best IT management practices and standards in order to achieve the integrated improvement of the IT field that would contribute to better progress in the management of critical State information resources:

  — IT planning was not sustainable: the planned IT tools were presented in different documents, there was a lack of any systematic approach due to the excess of strategic documents, making it difficult to identify the key priorities and channel resources to manage the greatest threats.

  — IT monitoring did not ensure that organisations measured the efficiency of IT operations and that audits carried out by the critical state information resources managers showed the actual maturity of IT management. State IT management was not scrutinised at national level, and IT management issues were not systematically analysed. A system for monitoring the compliance of the State information resources with the requirements of electronic information security had been created, intended only to facilitate the monitoring of security compliance, but its functionality was not sufficiently utilised.

- Measures to ensure the resilience of critical information resources to the level of cyber threats were not effective enough; therefore, there was still a risk of vulnerability of these resources:

  — The effectiveness of the assessment of IT security risks needed to be increased, as not all relevant risks were identified and their assessment methodology did not comply with the latest IT management practices; timely management of unacceptable risks was not ensured.

  — Organisational security measures capable of reducing cyber threats were not systematically used. Insufficient testing of security, incomplete training of staff during information system development, upgrading and modification; unmanaged safe software configurations and upgrades; improper

management of IT business continuity and backup files threatened the recovery of going concerns; security performance measurements were insufficient and did not contribute to security enhancement.

Conclusions

On average, the IT management of the public sector entities audited over the last ten years achieved the first level of maturity out of 5[66] and was at a level of 1.7 at the time of writing. This low level of maturity of critical State information resources was indicative of weaknesses in the formulation and implementation of the State information resources policy, making the resources more vulnerable. In order to increase the security of these resources, the management mechanism of State information resources needs to be improved to match best practices as far as possible. The auditors also noted that measures to guarantee the resistance of critical information resources to cyber threats were not sufficiently effective. Therefore, the assessment of IT security risks needs to be made more effective by putting more emphasis on safety testing when creating and modernising information systems and educating staff.

Further reports in the area

Title of the report:	Is Cybercrime Combatted Effectively
Hyperlink to the report:	Summary report (English version) Report (Lithuanian version)
Date of publication:	2020

Title of the report:	Environment of Cyber Security in Lithuania
Hyperlink to the report:	Summary of report (English version) Report (Lithuanian version)
Date of publication:	2015

[66] Following the COBIT methodology.

Hungary
State Audit Office

Audit on data protection – Audit of the domestic data protection framework and certain priority data records in the framework of international cooperation

Publication date: March 2017

Hyperlink to the report: Report (Hungarian version)

Audit type and period

Type of audit: Compliance

Audited period: 2011-2015

Summary of the report

Audit topic

The security of national data assets is a fundamental interest of society in every country for the preservation and protection of national values. Accordingly, ensuring the enhanced security of personal and public data within the national data assets of Hungary is essential in order to strengthen citizens' trust in the State and to ensure the continuous and smooth functioning of public administration. Therefore, the protection of data and the safety net ensured by the legal framework for its enforcement are of key importance to society.

Regarding the area of data protection, the public administration plays a key role in managing the largest and most sensitive registers of data belonging to national data assets. The data controllers for the registers work in close cooperation in order to carry out their tasks. They regularly transfer registers containing large amounts of data, and must pay attention to the statutory data protection requirements. The use of electronic information systems to manage and process data is essential nowadays, so proper and reliable operation of the systems must be guaranteed by properly designed and operated controls.

During its audits, the State Audit Office of Hungary places great emphasis on data protection. The SAO conducted comprehensive audits on data protection from 2011 to 2015, issuing its report in the first quarter of 2017. The audit also covered aspects of parallel international audits carried out in cooperation with the EUROSAI IT Working Group, which primarily concerned compliance with existing European Union directives.

The purpose of the compliance audit on data protection in Hungary was to assess whether the regulatory and operational framework for data protection had been established in Hungary and whether the major data management organisations had complied with the requirements for safe data management and outsourcing of data processing. The audit focused in particular on the protection of personal data and national data assets.

In the context of the audit, the SAO evaluated data management of six data management organisations (for example: tax authority, national treasury, health insurance, payment of pensions, education office, personal data and address, vehicle and travel records, and administrative agencies for criminal data management), and also the activities of the data protection authority and the information security authority.

The audit placed particular emphasis on the mandate of data management organisations, in particular in the case of data transfers to third parties. During the audit of internal controls on data management and data processing, the existence of up-to-date regulations on duties, responsibilities and competencies, human resources management and processes were evaluated.

Regarding the electronic systems used in data management, the SAO assessed the related security measures, including the areas of physical protection, access rights, logging, security assessment procedures, system and communications security, and the compliance of the security classification of the organisation as a whole.

The outsourcing of data processing was audited on the basis of the contracts concluded, looking at whether the data management organisations obliged the data processing organisations to meet the requirements related to data processing activities in accordance with the legislative regulations.

Findings and conclusions

Based on the audit, the State Audit Office of Hungary found that the internal regulations of data management organisations regarding data management activities

ensured the protection of national data assets as part of national assets in accordance with the legal provisions in force between 2011 and 2015. In practice, data controllers had properly applied the requirements of secure data management and outsourcing of data processing. The transfer of data to third parties was implemented with the appropriate mandate and a clear delineation of responsibilities and powers.

In respect of some data controllers, it was found that the security classification of electronic systems and organisation as a whole was not always in accordance with the legal requirements, but the extent of the deficiencies did not substantially affect the security of the data being processed. Based on the recommendations included in the audit report, the deficiencies were remedied by data management organisations within the framework of action plans approved by the SAO.

In connection with the parallel international audit carried out in cooperation with the EUROSAI IT Working Group, the SAO found that the Hungarian data protection legislation was in compliance with the existing directive of the EU.

In conclusion, by auditing data protection, the State Audit Office of Hungary contributed to good governance and the protection of national data assets.

Further reports in the area

Title of the report:	Report – Follow-up audits – Data protection audit – Audit of the domestic data protection framework and certain key data records in the framework of international cooperation
Hyperlink to the report:	Report (Hungarian version)
Date of publication:	2020

The Netherlands
Court of Audit

Cybersecurity of critical water management structures and border controls in the Netherlands

Publication dates: March 2019 and April 2020

Hyperlink to the reports: Summary of report on cyber security and critical water structures Report (English version)

Summary of report on cyber security and automated border controls Report (English version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2018-2020

Summary of the report

Audit topic

In 2018, the Netherlands Court of Audit decided to carry out audits on cybersecurity in sectors that are critical for society. Based on long experience of auditing information security compliance in central government, the Court of Audit saw added value in auditing the *performance* of policies and measures in practice. The first two audited sectors were water management and automated border controls, the first being vital for a nation largely below sea-level, and the second due to the position of Amsterdam Schiphol airport as an international hub and gateway to the country.

The Minister of Infrastructure and Water Management has designated a number of water structures managed by the Directorate-General for Public Works and Water Management (the auditee) as “critical parts” of the water management sector. Many computer systems used in operating the critical water structures date back to the 1980s and 1990s, a time when “cybersecurity” was not commonly taken into account. These systems were originally designed for stand-alone operation, but have been

gradually linked up with bigger computer networks, for example in order to facilitate remote operation. This trend has made the systems more vulnerable to cyber threats.

The Minister for Defence and the Minister for Justice and Security share responsibility for border control checks carried out by Dutch border guards at Schiphol airport. Both ministries (the auditees) own IT systems on which the border guards rely. The systems are critical for airport operations and are used to process highly sensitive data. This makes them an interesting target for cyber attacks aimed at sabotage, espionage or manipulation of the border control checks.

The audits examined the way in which the auditees were prepared for dealing with cyber threats and if this was done effectively.

- Audit questions with the aim of answering the following questions: How do the auditees *protect* systems from cyber threats and *prevent* cyber attacks?
- How do the auditees *detect* cyber threats and attacks?
- How do the auditees *respond* in a situation in which a cyber attack takes place?

One stand-out focus of both audits was effectiveness. In close cooperation with the auditees, ethical hackers worked on critical water structures and one of the border control systems. Needless to say, all test findings were acted on before the reports were published and no technical details were disclosed.

The main difference between the two audits was that the water structures audit focused on the achievement of the auditee's goals, while the border control audit was based on the NIST-cybersecurity framework.

Findings

First of all, both audits found that the auditees were aware of cyber threats and were in the process of implementing a professional approach to the matter.

In the case of the water structures, however, the auditee still needed to do more in terms of both detection and response in order to meet its own cybersecurity targets. The auditee did establish a Security Operations Centre (SOC) to detect and respond to cyber attacks. However, the objective set for the end of 2017 of instantly detecting any cyber attacks directed against critical water structures had not been achieved by the autumn of 2018. This meant that there was a risk of failing to detect a cyber attack directed at a critical water structure, or of detecting such an attack too late.

Furthermore, the test performed at one of the critical water structures showed that it was possible to gain physical access to it. Hackers were able to access the control room and found themselves alone with unsecured work stations. Lastly, no scenario had been constructed by the auditee for a crisis caused by a cyber attack and information relating to response was lacking or not kept up to date. The presence of up-to-date information could prove critical for a rapid and effective response to a crisis situation.

For the border controls, the cybersecurity measures were neither adequate nor future-proof. First of all, important border control systems had to be formally approved before commencing operation to ensure that all cybersecurity measures were implemented. We found that two of the three systems were operational without approval, meaning there was no guarantee that the necessary security measures were in place. Secondly, one SOC was operational but none of the systems were directly connected to it. Although generic infrastructure was connected to the SOC, this still posed a risk of cyber attacks going unnoticed or being detected too late. Third, security tests were not carried out regularly. In fact, only one of the three systems had been tested in the past, and this only to a limited extent. Lastly, just as in the first audit, no specific scenario had been constructed for a crisis caused by a cyber attack.

During the security test of one of the systems that had never been tested before, ethical hackers found a number of vulnerabilities. These vulnerabilities could be exploited in combination by a malicious unauthorised insider to launch a cyber attack to access, copy and even manipulate information in the system. These results show the importance of regular security testing.

The findings are worrying because of the ongoing automation of border processes. In the near future, a growing number of border control systems will process more and more data using a growing amount of connections. This increases the risk of cyber attacks; therefore the approach used was not future-proof.

Conclusions

In the case of the water structures, some key elements prevented the auditee from taking the final cybersecurity steps. For instance, it was unclear what the level of threat was, making it difficult to assess whether or not the measures taken and budget allocated were sufficient. Furthermore, the central department responsible for cybersecurity did not have a mandate to implement necessary cybersecurity measures at the decentralised water structures. The audit recommendations were followed in this respect and helped the organisation going forward.

For the border controls, there was no clear reason for the insufficient level of cybersecurity. The audit research found complete and detailed cybersecurity procedures and policies as well as sufficient expertise and skilled employees. Therefore the audit recommendations centred mainly on ensuring that every possible step was in fact taken.

Both audits generated a lot of attention from parliament and the media. The audits raised awareness of cybersecurity in relation to vital infrastructure and provided the auditees with insights into how to improve their cybersecurity. Close cooperation with the auditee was essential to fully understand their situation and deal with the risks of investigating and testing cybersecurity.

A third audit in this series is also planned. Furthermore, the information security level of the Netherlands national government is a key element of the yearly compliance audit cycle. Over the years, the Netherlands SAI has seen that many ministries are under par on information security measures. The Court of Auditors is currently using the experience gained in its cybersecurity audits to broaden its perspective on information security auditing, looking beyond papers and policies and testing the actual effectiveness of measures.

Further reports in the area

Title of the report:	Chapter 3 of “Staat van de rijksverantwoording 2019”
Hyperlink to the report:	Report (Dutch version)
Date of publication:	2020

Title of the report:	Focus on digital home working
Hyperlink to the report:	Report (Dutch version)
Date of publication:	2020

Poland
Najwyższa Izba Kontroli (NIK)

Ensuring the security of the operation of IT systems used to carry out public tasks

Date of publication: 2016

Hyperlink to the report: Report (Polish version)

Audit type and period

Type of audit: Compliance

Period audited: 2014-2015

Summary of the report

Audit topic

The purpose of the audit was to assess whether data collected in the systems intended to implement important public tasks were secure in the units audited. The audit covered six selected institutions carrying out significant public tasks. Following analysis, one essential IT system was selected in each of the institutions, then examined in detail. Version 4.1 of the COBIT (Control Objectives for Information and related Technology) method was applied to the audit.

This audit was carried out following the 2015 audit of "Public bodies" performance of cybersecurity tasks in Poland'[67], the findings of which pointed to systemic problems. The 2016 audit demonstrated, inter alia, that the State Administration had not taken action up to that time to ensure IT security at national level. It was concluded that public entities' activities related to the protection of cyberspace had been carried out in a fragmented manner and lacked a systematic approach. In the absence of central arrangements to ensure the concrete security conditions for specific IT systems, essential to the operation of the State, audit aimed at examining whether institutions

[67] https://www.nik.gov.pl/kontrole/P/14/043/

administering IT systems used to carry out important public tasks ensured that such tasks could be implemented securely.

Another cybersecurity-related system audit entitled “Cybersecurity in Poland” was approved in 2019, but the findings are confidential.

Audit questions

The sub-objectives were split between two evaluation areas, seeking answers to specific questions.

In the area of supporting IT security, the audit examined at the level of the entire organisation whether, inter alia:

- IT security management was carried out;
- plans to ensure IT security were implemented;
- IT security was tested, supervised and monitored;
- IT security incidents were defined;
- IT was managed by cryptographic keys;
- protection against and detection of malicious software and patching were implemented;
- network security was ensured.

In the area of security support, the audit examined at the level of the systems selected whether, inter alia:

- users’ identity and accounts were managed;
- security technologies and sensitive data were protected.

Findings and conclusions

The degree of preparation and implementation of the Information Security System did not provide an acceptable level of security for the data collected in the IT systems intended for performing important public tasks. The information security processes were carried out in a disorderly manner and, in the absence of procedures – intuitive. Of the six units audited, but one had implemented the Information Security System,

and it should be noted that its operation had also been affected by significant faults. In all of the units audited, but one, the work to ensure suitable conditions of security for information processed in the IT systems had not reached the appropriate level because, having begun only recently, it was at the preliminary stage, which also involved drawing up the necessary formal foundations. It had been based on simplified or informal arrangements based on good practice or the IT staff's experience up to that time.

In accordance with COBIT 4.1 methodology, the maturity of the information-security management process in the various units audited ranged between (1) initial/ad hoc and (3) defined, on a scale of zero to five, where five is the maximum.

Responsibility for ensuring IT security in the units audited lay with the security coordinator, who, in practice, however, was not competent to manage the entire process. The tasks involved were also often carried out by just one person. Even though specialist teams had been appointed or agreements concluded with external contractors, the analysis necessary to establish whether the services provided meet a unit's security needs had not been made. The auditee units' understanding of the need to ensure IT security was fragmented and limited. Data security was seen mainly as the IT department's responsibility and domain, and not that of all organisational units with statutory tasks, which greatly hindered the development of coherent IT-security management systems for the entire institution.

When comparing the quality of the manner in which obligations to ensure information security were met with regard to both entire organisations and the systems selected, it is clear that the quality of implementation was higher in the second case. This may be due to the impact the practical knowledge and involvement of mid-level technical staff had on ensuring security, the increased use within the public administration of commercial IT systems based on market standards, and advanced security-assurance solutions. By applying such solutions, past experience and good practice, it was possible to maintain a certain level of security in the operation of the various systems in conditions of limited resources, organisational shortcomings or "non-functioning" regulation. This cannot be the target solution, however, since, in times of dynamic increase in threat level, the security of IT systems cannot be founded on measures managed in a disorderly fashion and geared solely to overcoming immediate difficulties.

Audit conclusions

General IT-security recommendations and requirements applicable to all public entities need to be developed and implemented at a central level. A systemic solution is needed whereby the results of IT security audits are disclosed in a way that allows citizens to access information on the activities of public entities, while access to knowledge of the measures and methods used to ensure the security of information processed is restricted.

Further reports in the area

Title of the report:	Information security management by regional authorities
Hyperlink to the report:	Report (Polish version)
Date of publication:	2019

Title of the report:	Cybersecurity in Poland (classified information)
Hyperlink to the report:	*Not publicly accessible*
Date of approval:	2019

Title of the report:	Ensuring the security of IT systems by regional authorities in Podlaskie Voivodeship
Hyperlink to the report:	Report (Polish version)
Date of publication:	2018

Title of the report:	Prevention and combat of cyber-bullying among children and young people
Hyperlink to the report:	Report (Polish version)
Date of publication:	2017

Title of the report:	Public bodies' performance of cybersecurity tasks in Poland
Hyperlink to the report:	Report (Polish version)
Date of publication:	2015

Title of the report:	Implementation of selected requirements on information systems, electronic information exchange and National Interoperability Framework based on the example of some municipality councils and cities with district rights.
Hyperlink to the report:	Report (Polish version)
Date of publication:	2015

Portugal
Tribunal de Contas

Audit on the Portuguese Electronic Passport

Publication date: 2014

Hyperlink to the report: Report (Portuguese version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2013

Summary of the report

Audit topic

The operational audit of the Portuguese Electronic Passport (PEP) was oriented towards the effectiveness of the information systems that support its granting, issuing and use, particularly in the automated screening of passengers by reading biometric data at the Portuguese borders[68].

The main audit objectives were:

- To verify compliance with EU and national law, international standards and guidelines for the granting, issuing and use of the PEP, including the adequacy of the national legal framework;
- To examine the effectiveness of key processes associated with the life cycle of the PEP, in particular those associated with the granting, issuing and use of the PE;

[68] We refer to Automated Border Control (ABC) Systems within Frontex (European Border and Coast Guard Agency).

- To examine critical aspects of the performance of information systems, in particular fulfilment of security requirements concerning PEP information systems (SIPEP).

The key risk areas included:

- Loss/theft of physical assets and/or electronic information;
- Misuse of confidential information;
- Compliance risk (failing to meet legal and regulatory requirements).

Audit period: 1 January 2013 – 31 December 2013 (where appropriate, to be extended to earlier and later years).

Findings and conclusions

The Portuguese Electronic Passport (PEP) covers three categories: common[69], diplomatic or special. There is also a passport for non-nationals, conferring reduced privileges.

The concession system has several applications and several data collection entities and granting bodies, but only one issuer (incorporating production, personalisation and delivery).

Several entities (PEP entities) take part in the process. The following entities collect data and grant passports:

- Mainland Portugal: the Serviço de Estrangeiros e Fronteiras (SEF)[70] and the registry services of the Instituto dos Registos e do Notariado (IRN)[71];

[69] About 99 % of the total.

[70] Immigration and Borders Service.

[71] Registration Office and Notary (receipt only).

- The Autonomous Regions of the Azores[72] and Madeira: services under the respective *Vice-Presidência do Governo Regional*[73]; abroad: the Portuguese consulates;
- The Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] issues and delivers the passports.

The main processes are mostly supported by SIPEP (central management application system for issuing Portuguese passports). SIPEP makes it possible to record, store, process, validate and provide the required information associated with the granting of the PEP, triggers the customisation process carried out by INCM, and ensures the interconnection with other system applications, coordinating all PEP entities involved in the physical and logistical registration of the data collected.

The PEP entities have an organisational structure that enables them to meet the legal goals associated with the PEP. The system still relies heavily on human resources at request and collection levels. However, SIPEP includes several automatic processing functions and validation controls.

Since the procedures ensure control functions and manipulation of data, some of which can be conducted independently, without human intervention, SIPEP has a significant impact in terms of organisation and the information system, particularly as regards: (i) the understanding and definition of the standards, processes and required data; and (ii) the definition of the information system's own requirements.

The efficiency and effectiveness of the data collection process are ensured by the interaction of SIPEP with other information systems[75], in accordance with legal regulations.

A framework of overall control for IT activities (governance, development and acquisition, IT operations, business continuity and disaster recovery, information

[72] And the service points of the *Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* – Agency for Modernisation and Quality of Service to the Citizen, public institute (receipt only).

[73] Vice Presidency of the Regional Government.

[74] The Official Printing Office and the Mint, public company.

[75] Namely: Integrated Information System of SEF (SIISEF); National Part of the Schengen Information System (NSIS); Civil identification database, Criminal records database.

security) has been established, although not extensively documented, and ensures the development, operation, management and maintenance of the SIPEP system.

Activity indicators (2013):

- Around 500 000 PEPs were granted, of which about 63 % by SEF, 33 % by Portuguese consulates and 4 % by the Regional Governments;
- The income from issuing the PEP totalled about €37 million, predominantly from the INCM (43 %), the SEF (32 %) and the *Ministério dos Negócios Estrangeiros (MNE)*[76] (17 %).

For 2013, tests performed in SIPEP did not confirm compliance with the maximum delivery time legally established (from the date of the request to the availability of the PEP for collection from the delivery point) because the actual delivery date at the delivery point was not always registered in a timely manner.

Investments relating to the acquisition of equipment for collecting biometric data and signature (kiosks), equipment for automated border control (ABC) systems and the purchase and maintenance of IT systems, services and technical assistance were made by the SEF, MNE, RIAC and INCM for the sum of €11 million, with the highest amount spent by the SEF.

Prior to the PEP, the price of the (non-biometric) Portuguese Republic Passport was €22.44; in 2006, the common (biometric) PEP was priced at €60, rising to €65 in 2011.

PEP applications

PEP applications are processed in person by the competent services, which receive the application documents, collect applicants' biographical and biometric data, collect the fees and, later, deliver the PEP issued.

The underlying system (SIPEP) validates data correctness and quality through virtual controls and cross-referencing with other information systems, namely the Civil Identification Database, in order to ensure that the application is compliant and suitable for granting and issuing the PEP.

The associated status changes are recorded in log files, ensuring the auditability, integrity and non-repudiation of the transactions.

[76] Ministry of Foreign Affairs.

Data transmission between the data collection bodies (in Portugal and abroad) and the SEF takes place via VPN (Virtual Private Network), implemented on the basis of access management in accordance with credentials controlled by SEF[77].

The application for the common PEP is processed differently when submitted by citizens whose rights are limited or restricted, including: (i) those who cannot exercise their rights (minors, incapacitated or prohibited persons); (ii) persons precluded judicially or by the police (criminal record, pending lawsuit or seizure of documents); and (iii) when the applicant for a second PEP invokes a national or legitimate interest.

Granting the PEP

The decision to grant the common PEP may be:

- Automatic – automatic approval by the SIPEP application system after validation of the identity of the applicant and the absence of a criminal record (through cross-referencing with the IRN's civil identification and criminal records databases) and pending lawsuits. Only occurs in the SEF, for PEP applications on the mainland[78].
- Subject to individual acceptance/ approval by other entities (Regional Governments and Consular Posts) or, in the case of the SEF, requirements not covered by the automatic granting[79].

[77] The SIPEP is accessible (via the web) at national/regional and international level to services located on the mainland, in the autonomous regions of the Azores and Madeira, and abroad (Portuguese consulates).

[78] This is an automated functionality of the SIPEP application system for granting (internally referred to as "authorising") an application (except for a second PEP) for a citizen of legal age, with a valid citizen card, with no pending lawsuits and who is not banned or disqualified. Common PEPs granted by SEF, about 60 %, were covered by automatic validation procedures and granting decisions, and the rest were subject to examination and approval by the *Direção Central de Imigração e Documentação (DCID)*.

[79] Particularly in the cases of applicants unable to exercise their rights (minors, incapacitated or prohibited persons), precluded judicially or by the police or, in the case of a second PEP, whose application is considered on a case-by-case basis by the DCID.

Issuing the PEP

Issuing the PEP, which covers production, personalisation and delivery, is under the competence of the INCM. When delivery of the PEP is recorded in the SIPEP, the passport status is changed to “Valid”.

PEP rates differ depending on the level of service required. To measure the level of service, SIPEP needs to consider the actual delivery date of the PEP.

PEP delivery is carried out by a contracted transport service.

PEP termination

Whenever an applicant delivers a prior, still valid, PEP, it should be disabled to prevent re-use, corresponding to the passport record status “unusable”, in the SIPEP application system.

Finland
Valtiontalouden tarkastusvirasto

Cyber protection arrangements

Publication date: 2017

Hyperlink to the report: Report (Finnish version)

Audit type and period

Type of audit: Performance Audit

Audited period: 2016-2017

Summary of the report

Audit topic

The purpose of the audit was to investigate whether cyber protection in central government had been arranged as effectively and cost-efficiently as possible. The audit focused on how central government cybersecurity was organised and managed. The results of the audit could be used to develop the effectiveness and efficiency of cybersecurity in central government. The audit was carried out from 22 September 2016 to 4 September 2017. The follow-up was carried out in autumn 2019. In the follow-up, the National Audit Office examined the actions taken on the findings and recommendations of the audit.

The audited entities included the authorities in charge of cyber protection in central government (the Prime Minister's Office, the Ministry of Finance, the Ministry of Transport and Communications) and the authorities responsible for centralised cyber protection tasks and centralised IT services in central government (the National Cyber Security Centre of the Finnish Transport and Communications Agency, the Government ICT Centre Valtori, the Digital and Population Data Services Agency). The effectiveness of the guidance was also assessed by examining central government units providing electronic services (the Digital and Population Data Services Agency, the Finnish Transport and Communications Agency Traficom, the National Administrative Office

for Enforcement and its supervisor the Ministry of Justice, and the ICT Service Centre of the Ministry of Justice).

Audit questions

The following audit questions were used in the audit of the organisation of cybersecurity:

- Did the audited entity give the economic aspect sufficient consideration when organising cybersecurity?
- Does the cybersecurity situational awareness of the audited entity support the cybersecurity of systems?
- Is the audited entity's ability to respond to cyber violations sufficient?

The audit topic of cyber protection arrangements was part of the audit theme "Ensuring the operational reliability of the information society" in the National Audit Office of Finland's 2016-2020 audit plan. From the point of view of importance to central government finances, the audit topic can be justified by the disadvantages related to service interruptions and data breaches, as well as the negative effects of poor cybersecurity on business activities. The audit was carried out in parallel with the audit "Steering the operational reliability of electronic services", which belongs to the same theme. The key audit material consisted of documents and interviews with the authorities responsible for the activity in question.

Findings and conclusions

Finland's cybersecurity strategy defines the key objectives and policies for meeting the challenges facing the cyber environment and ensuring its functioning. Efforts have been made to implement the cybersecurity strategy through an implementation programme, the progress of which is evaluated annually. The Security Committee is a cooperation body within the Ministry of Defence that monitors and coordinates the implementation of the cybersecurity strategy.

Effective organisation of cybersecurity is risk management, which, in order to be successful, requires effective management structures and arrangements that integrate risk management into operations at all levels of the organisation. Like many other countries, Finland and its central government are not self-sufficient in cyber protection resources. European Union legislation has increased over time and become more

binding. In the Finnish government, the responsibility for cyber protection is decentralised, with each corporate body responsible for its own cybersecurity. In central government, the assignment of responsibilities in respect of the nature, extent and implementation of possible cyber violations is complex.

Due to this complexity, the response to an anomaly may be too slow, and scarce funding has limited the implementation of Finland's cybersecurity strategy. Based on the audit findings, the National Audit Office reached the following conclusions and made the following recommendations regarding the organisation of cybersecurity in central government:

Operative management of extensive cybersecurity violations was not defined

Planning the operational management of extensive cybersecurity violations and division of related responsibilities could allow for faster reactions and appropriate coordination and resource allocation for countermeasures. In the current operating model, each agency is responsible for its own cyber protection. However, there is not enough expertise in cyber protection available, which impedes the creation of cyber protection either internally or via outsourcing.

Some Cybersecurity Strategy goals were not achieved

The implementation programme for the Finnish Cybersecurity Strategy had improved cyber protection. Some of the goals of the first implementation programme were not achieved, because the level of commitment to the actions varied and could not be improved in a centralised manner. The new implementation programme only included actions to which the competent authorities and other actors had expressed their commitment. Commitment and available resources depended on each other.

Appropriateness of cyber protection funding solutions was unclear

The differences in the development of cyber protection were partially due to the differences in the amount of development resources the organisations had at their disposal. No procedures to ensure that funds were allocated to the most important targets for cyber protection were identified in the regulations on the preparation of the State budget or the preparation process. Agencies and institutions budgeted the appropriations for cybersecurity as an unspecified part of the operating expenditure of the agency or institution. Measures described in Finland's cybersecurity strategy were implemented only to the extent allowed by the appropriations.

Cyber protection should also be taken into account in changes to the ICT organisation

Changes in central government ICT organisation had influenced cyber protection arrangements. Developing cybersecurity centralised by Valtori had proven difficult. There were deficiencies in assessing the adequacy of the practical cyber protection procedures and in the implementation of new arrangements.

Situational awareness of cybersecurity operations should be improved

The Cyber Security Centre maintained nationwide situational awareness of cybersecurity. At the time of the audit, there was no obligation to report cybersecurity violations to the Cyber Security Centre. Requiring government organisations to report violations would improve the situation, as would increasing the coverage of centralised cyber violation detection procedures.

Based on the above statements, the National Audit Office recommends that the Ministry of Finance defines and implements an extensive operational management model in case of cybersecurity incidents in central government ICT services. The Ministry of Finance should also find out how the cybersecurity of services should be taken into account in the funding of services throughout their lifecycle and improve operative situational awareness by instructing authorities to report cyber violations to the Cyber Security Centre. It was recommended that Valtori should improve the implementation, evaluation and development of cybersecurity procedures and the detection of cyber violations.

The follow-up audit examined how the recommendations given during the audit had been implemented. The Audit Office considered that the Ministry of Finance, as the competent authority for the implementation of the recommendations, had not taken sufficient measures in response to the recommendations made. However, cybersecurity had also been reinforced in Finland through measures taken by authorities other than the Ministry of Finance. A change in the strategic management of cybersecurity to the cybersecurity director model was underway. In the budget proposal for 2020, the government increased appropriations for the central government authorities that play a key role in strengthening cybersecurity. In addition, Valtori was taking measures in line with the National Audit Office's recommendation. In conclusion, the National Audit Office stated that follow-up auditing was necessary due to unimplemented recommendations, and a completely new audit in the area was justified by the ongoing changes in the cybersecurity arrangements and digital operating environment, and the related risks, as well as the importance of cybersecurity to central government finances and society.

Sweden
Riksrevisionen

Obsolescent IT systems – an obstacle to effective digitalisation

Publication date: 2019

Hyperlink to the report: Summary of report (English version)
Report (Swedish version)

Type Audit type and period

Type of audit: Performance Audit

Audited period: 2018-2019

Summary of the report

Audit topic

Obsolescent business-critical IT systems involve a major risk of efficiency problems because, proportionally, organisations are forced to put more resources to use just to maintain the system. There is therefore good reason to assume that obsolescent IT systems imply a high risk of mismanaging public funds. They also imply some diversion of an agency's innovative capacity in terms of developing new IT systems. However, not only do obsolescent IT systems lead to risks for individual agencies, problems at one agency may mean major consequences for its ability to coordinate operations with another agency or private stakeholder. Obsolescent IT systems also involve risks from an information security perspective.

Definition of the main audit subject/ Audit questions/ Context

The purpose of the audit was to examine the incidence of obsolescent IT systems in central government administration and to see whether the authorities and the government had taken suitable measures to prevent these systems from becoming an obstacle to effective digitalisation. The audit questions addressed were:

- Have the authorities taken suitable measures to deal with the problems associated with obsolescent IT systems?
- Has the Government taken suitable measures to deal with the problems associated with obsolescent IT systems?

Findings and conclusions

- The audit showed that obsolescent IT systems were present in a large number of government agencies. At many agencies, moreover, one or more business-critical IT systems were obsolescent. As far as the Swedish NAO is aware, this is new information and no-one was previously aware of the extent of the problem in central government administration. Around 80 % of the agencies stated that they found it difficult to maintain the level of information security in one or more of their business-critical systems. More than one in ten authorities replied that this applied to all, or to a majority, of the systems.
- A large proportion of the agencies examined did not have the correct approach to development and administration of IT support. They did not use existing tools for operational development in order to determine how IT support could best contribute to achieving the objectives of core operations. A large proportion of the agencies audited therefore lacked an overall description of how strategies, operational processes and systems were linked. This, in turn, meant that they had difficulty analysing and understanding how changes affected the objectives of the organisation, and it was therefore more difficult to define a desirable future situation.
- More than half of the authorities stated that there was no approved model for dealing with and taking decisions on their IT systems from the system development stage to phase-out, usually termed life-cycle management. According to the Swedish NAO, this indicated that life-cycle management was not undertaken in a structured and methodical manner. There were also

shortcomings in risk analysis work and in the ability to break down IT costs at the detailed level necessary for sound decision-making.

- Almost 60 per cent of the authorities lacked system development life cycle plans for any systems other than one or a few business-critical systems. The lack of life-cycle plans and other planning documentation at many agencies, combined with shortcomings in the life-cycle management actually carried out, meant that the agencies in general could not be regarded as having developed a conscious, explicit position around their IT systems.

- The Swedish NAO's assessment is that the ministries involved, and thus also the government, lacked sufficient knowledge on both the incidence and the consequences of obsolescent IT systems.

The overall conclusion was that, at the time of the audit, most agencies had not really managed to deal effectively with the problems involved in obsolescent IT systems. The Swedish NAO considered that the problem was so serious and widespread that it constituted an obstacle to the continued efficient digitalisation of the State's administration. The audit also showed that the government lacked knowledge about the existence and consequences of the problems of obsolescent IT systems. Furthermore, the government had not taken any measures to target the problem of obsolescent IT systems more directly. The Swedish NAO's assessment was therefore that the government could not be considered to have taken sufficient measures to ensure that the problems were reduced or eliminated.

Further reports in the area

Title of the report:	Making it easier to start a business – government efforts to promote a digital process (RiR 2019:14)
Hyperlink to the report:	Summary of report (English version) Report (Swedish version)
Date of publication:	2019
Title of the report:	Digitalisation of public administration – Simpler, more transparent and effective administration (RiR 2016:14)
Hyperlink to the report:	Summary of report (English version) Report (Swedish version)
Date of publication:	2016
Title of the report:	Information security work at nine agencies (RiR 2016:8)
Hyperlink to the report:	Summary of report (English version) Report (Swedish version)
Date of publication:	2016
Title of the report:	Cybercrime – police and prosecutors can be more efficient (RiR 2015:21)
Hyperlink to the report:	Summary of report (English version) Report (Swedish version)
Date of publication:	2015

European Union
European Court of Auditors

Briefing paper: Challenges to effective cybersecurity policy

Publication date: 2018

Hyperlink to the report: Report (23 languages versions)

Audit type and period

Type of audit: Policy review

Audited period: April – September 2018

Summary of the report

Review topic

The objective of this briefing paper, which is not an audit report, was to provide an overview of the EU's complex cybersecurity policy landscape and identify the main challenges to effective policy delivery. It covers network and information security, cybercrime, cyber defence and disinformation.

The ECA's analysis was based on a documentary review of publicly available official documents, position papers and third party studies. The fieldwork was carried out between April and September 2018, and developments up to December 2018 were taken into account. The ECA complemented its work with a survey of the Member States' national audit offices, and through interviews with key stakeholders from EU institutions and private sector representatives.

There is no standard definition of "cybersecurity". Broadly, it is all the safeguards and measures adopted to defend information systems and their users against unauthorised access, attack and damage to ensure the confidentiality, integrity and availability of data. Cybersecurity involves preventing, detecting, responding to and recovering from cyber incidents. Incidents may be intended or not and range, for example, from accidental disclosures of information to attacks on businesses and critical infrastructure, to the theft of personal data, and even interference in democratic processes.

The cornerstone of the EU's policy is the 2013 Cybersecurity Strategy. It aims to make the EU's digital environment the safest in the world, while defending fundamental values and freedoms. It has five core objectives: (i) increasing cyber resilience; (ii) reducing cybercrime; (iii) developing cyber defence policies and capabilities; (iv) developing industrial and technological cybersecurity resources; and (v) establishing an international cyberspace policy aligned with core EU values.

Findings

It was difficult to capture the impact of being poorly prepared for a cyber attack due to the lack of reliable data. The economic impact of cybercrime rose fivefold between 2013 and 2017, hitting governments and companies, large and small alike. The forecast growth in cyber insurance premiums from €3 billion in 2018 to €8.9 billion in 2020 reflects this trend. Although 80 % of EU businesses experienced at least one cybersecurity incident in 2016, acknowledgement of the risks is still alarmingly low. Among companies in the EU, 69 % have no or only a basic understanding of their exposure to cyber threats, and 60 % have never estimated the potential financial losses. According to a global survey, one third of organisations would rather pay the hacker's ransom than invest in information security.

The ECA's findings were as follows:

- The EU's cyber ecosystem is complex and multi-layered, involving numerous stakeholders. Bringing together all of its disparate parts is a considerable challenge.

- The EU intends to become the world's safest online environment. Achieving this ambition requires significant efforts from all stakeholders, including a sound and well-managed financial footing. Figures are hard to come by, but EU public spending on cybersecurity is estimated to range between one and two billion euros per year. In comparison, US federal government spending is budgeted at around $21 billion for 2019.

- Information security governance is about putting structures and policies in place to ensure data confidentiality, integrity and availability. More than just a technical issue, it requires effective leadership, robust processes, and strategies aligned with organisational objectives.

- Cybersecurity governance models differ between Member States, and within them responsibility for cybersecurity is often divided among many entities. These

differences could obstruct the cooperation needed to respond to large-scale, cross-border incidents and exchange threat intelligence nationally and even more so at EU level.

- Devising an effective response to cyber attacks is fundamental to stopping them as early as possible. It is especially important that critical sectors, Member States and EU institutions be able to respond in a swift and coordinated way. Early detection is essential to this.

Recommendations

The ECA's review shows that a shift towards a performance culture with embedded evaluation practices is needed to ensure meaningful accountability and evaluation. Some gaps in the law remain, and existing legislation is not consistently transposed by Member States. This can make it difficult for legislation to reach its full potential.

Another challenge identified concerns the alignment of investment levels with the strategic goals, which calls for the scaling-up of investment levels and impact. This is more challenging when the EU and its Member States do not have a clear overview of EU spending on cybersecurity. There were also reported constraints in the adequate resourcing of the EU's cyber-relevant agencies, including difficulties attracting and retaining talent.

Acronyms and abbreviations

APT: Advanced Persistent Threat

CEF: Connecting Europe Facility

CERT-EU: Computer Emergency Response Team

COBIT: Control Objectives for Information and Related Technology

Covid-19: Coronavirus Disease 2019

cPPP: contractual Public-Private Partnership

CSDP: Common Security and Defence Policy

CSIRT: Computer Security Incident Response Team

DDoS: Distributed Denial of Services

DEP: Digital Europe Programme

EC3: Europol's European Cybercrime Centre

ECA: European Court of Auditors

EDA: European Defence Agency

EEAS: European External Action Service

ENISA: European Union Agency for Cybersecurity

ESIF: European Structural and Investment Funds

ESRB: The European Systemic Risk Board

EU: European Union

EUROPOL: European Union Agency for Law Enforcement Cooperation

GDP: Gross Domestic Product

GDPR: General Data Protection Regulation

HR: Human resources

ICT: Information and Communications Technology

IoT: Internet of Things

ISACA: Information Systems Audit and Control Association

ISF-P: Internal Security Fund – Police

IT: Information Technology

MERS: Middle East Respiratory Syndrome

MFF: Multiannual Financial Framework

NAO: National Audit Office

NATO: The North Atlantic Treaty Organization

NCSS: National Cybersecurity Strategy

NIS Directive: Network and Information Security Directive

PESCO: Permanent Structured Cooperation Framework

RDP: Remote Desktop Protocol

SAIs: Supreme Audit Institutions

SARS: Severe acute respiratory syndrome

UK: United Kingdom

URL: Uniform Resource Locator

USA: United States of America

Glossary

Access data: Information on a user's log-in and log-out activity to access a service, such as time, date and IP address.

Adware: Malicious software displaying advertising banners or pop-ups that include code to track victims' online behaviour.

Advanced persistent threats: An attack in which an unauthorised user gains access to a system or network and remains there for an extended period of time without being detected. Particularly dangerous for enterprises, as hackers have ongoing access to sensitive company data, however generally do not cause damage to company networks or local machines. The goal - data theft.

Artificial intelligence: The simulation of human intelligence in machines that are programmed to think like humans and mimic their actions; any machine that exhibits traits associated with a human mind such as learning and problem-solving.

Availability: Ensuring timely and reliable access to and use of information.

Biometric data (biometrics): Physical (such as fingerprints and eyes) or behavioural calculations related to human characteristics. Authentication is used in computer science as a form of identification and access control.

Bitcoin: A digital or virtual currency created in 2009 that uses peer-to-peer technology to facilitate instant payments.

Cloud computing: The delivery of on-demand and IT resources – such as storage, computing power or data-sharing capacity – over the internet, through hosting on remote servers.

Confidentiality: The protection of information, data or assets from unauthorised access or disclosure.

Critical information system: Any information system, existing or envisaged, which is regarded as being essential to the efficient and effective running of the organisation.

Critical infrastructure: Physical resources, services and facilities of which the disruption or destruction would have a serious impact on the functioning of the economy and society.

Cryptocurrency: A digital asset which is issued and exchanged using encryption techniques, independently of a central bank. It is accepted as a means of payment among the members of a virtual community.

Cyber attack: An attempt to undermine or destroy the confidentiality, integrity and availability of data or a computer system through cyberspace.

Cybercrime: Various criminal activities involving computers and IT systems as either a primary tool or primary target. These activities include: traditional offences (e.g. fraud, forgery and identity theft); content-related offences (e.g. online distribution of child pornography or incitement to racial hatred); and offences unique to computers and information systems (e.g. attacks against information systems, denial of service attacks, malware or ransonware).

Cyber defence: A subset of cybersecurity aiming to defend cyberspace with military and other appropriate means in order to achieve military-strategic goals.

Cyber diplomacy: The use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to cyberspace. It is conducted in all or in part by diplomats, meeting in bilateral formats (such as the US-China dialogue) or in multilateral fora (such as in the UN). Beyond the traditional remit of diplomacy, diplomats also interact with various non-state actors, such as leaders of internet companies (such as Facebook or Google), technology entrepreneurs or civil society organisations. Diplomacy can also involve empowering oppressed voices in other countries through technology.

Cyber ecosystem: A complex community of interacting devices, data, networks, people, processes, and organisations, and the environment of processes and technologies influencing and supporting these interactions.

Cyber espionage: Cyber spying is the act or practice of obtaining secrets and information without the permission or knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using the Internet, networks or individual computers.

Cyber incident: An event that directly or indirectly harms or threatens the resilience and security of an IT system and the data it processes, stores or transmits.

Cyber resilience: The ability to prevent, prepare for, withstand and recover from cyber attacks and incidents.

Cybersecurity (cyber-protection): All the safeguards and measures adopted to defend IT systems and their data against unauthorised access, attack and damage to ensure their availability, confidentiality and integrity.

Cyberspace: The intangible global environment in which online communication occurs between people, software and services via computer networks and technological devices.

Cyber threat: A malicious act that seeks to damage data, steal data, or disrupt digital life in general.

Data breach: The intentional or unintentional release of secure or private/confidential information to an untrusted environment.

Data processing: The carrying out of operations on data, especially by a computer, to retrieve, transform, or classify information.

Digital asset: Anything that exists in digital format, owned by an individual or company and comes with the right to use (e.g. images, photos, videos, files containing text, etc.).

Digital content: Any data – such as text, sound, images or video – stored in a digital format.

Digital service provider: Is anyone who provides one or more of these three types of digital service – online marketplace, online search engines, cloud computing services.

Digital platform: An environment for interactions between at least two different groups—with one typically being suppliers and the other consumers/user. It may be the hardware or the operating system, even a web browser and associated application programming interfaces, or other underlying software, as long as the program code is executed with it.

Digitalisation: The process of converting information into a digital format, in which the information is organised into bits. The result is the representation of an object, image, sound, document or signal by generating a series of numbers that describe a discrete set of points or samples.

Disinformation: Verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.

Distributed Denial of Service (DDoS): A cyber attack preventing legitimate users from accessing an online service or resource by flooding it with more requests than it can handle.

Electoral infrastructure: Includes campaign IT systems and databases, sensitive information on candidates, voter registration and management systems.

Encryption: The transformation of readable information into unreadable code for its protection. To read the information, the user must have access to a secret key or password.

Ethical hacker: A person (a computer security expert) who penetrates a computer network in order to test or evaluate its security, rather than with malicious or criminal intent.

Hacker: An individual who uses computer, networking or other skills to gain unauthorised access to data, computer system or network.

High-performance computing: The ability to process data and perform complex calculations at high speeds.

Hybrid threat: An expression of hostile intent which adversaries make using a mix of conventional and non-conventional warfare techniques (i.e. military, political, economic and technological methods) in forceful pursuit of their objectives.

Information security: The set of processes and tools protecting physical and digital data from unauthorised access, use, disclosure, disruption, modification, recording or destruction.

Integrity: Guarding against the improper modification or destruction of information, and guaranteeing its authenticity.

Internet of Things (IoT): The network of everyday objects fitted with electronics, software and sensors so that they can communicate and exchange data over the internet.

Malware: Malicious software. A computer programme designed to harm a computer, server or network.

Network security: A subset of cybersecurity protecting data sent via devices on the same network, to ensure that the information is not intercepted or changed.

Operator of essential services: A public or private entity that provides a service which is essential for the maintenance of critical societal and economic activities.

Patching: Introducing a set of changes to software to update, fix, or improve it, including fixing security vulnerabilities.

Personal data: Information relating to an identifiable individual.

Phishing: The practice of sending emails purporting to originate from a trusted source in order to deceive recipients into clicking malicious links or sharing personal information.

Public utilities installations: Any pole, tower, overhead or underground conduit, any other supporting or sustaining structure, and any trench, together with accessories, susceptible of use for the supply or distribution of electrical, telephone, telegraph, cable delivery or signalling service or any other similar service.

Ransomware: Malicious software that denies victims access to a computer system or makes files unreadable, usually through encryption. The attacker then normally blackmails the victim by refusing to restore access until a ransom is paid.

Remote desktop protocol (RDP): A technical standard (issued by Microsoft), for using a desktop computer remotely. Remote desktop users can access their desktop, open and edit files, and use applications as if they were actually sitting at their desktop computer.

Sabotage: An action to deliberately destroy, damage, or obstruct, especially for political or military advantage.

Social engineering: In information security, psychological manipulation to deceive people into performing an action or divulging confidential information.

Spyware: A software with malicious behaviour that aims to gather information about a person or organisation and send such information to another entity in a way that harms the user; for example by violating their privacy or endangering their device's security.

Text vectorisation: The process of converting words, sentences or entire documents into numeric vectors so that machine-learning algorithms can use them.

Trojan: A type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

Web-based attacks: Defined Users trust that the sensitive personal information they divulge on the website will be kept private and safe. Intrusion (attack) can mean that their credit card, Social Security, or medical information might become public, leading to potentially grave consequences.

Worms: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it.

5G: Is the fifth generation technology standard for broadband cellular networks, which cellular phone companies began deploying worldwide in 2019, and is the planned successor to the 4G networks which provide connectivity to most current cellphones. The increased speed is achieved partly by using higher-frequency radio waves than previous cellular networks.