KEY TRENDS AND STATISTICS OF THE NATIONAL CYBER SECURITY STATUS OF LITHUANIA

2021 – Q1 2022

MINISTRY OF NATIONAL DEFENCE
OF THE REPUBLIC OF LITHUANIA

Key Trends and Statistics of the National Cyber Security Status of Lithuania

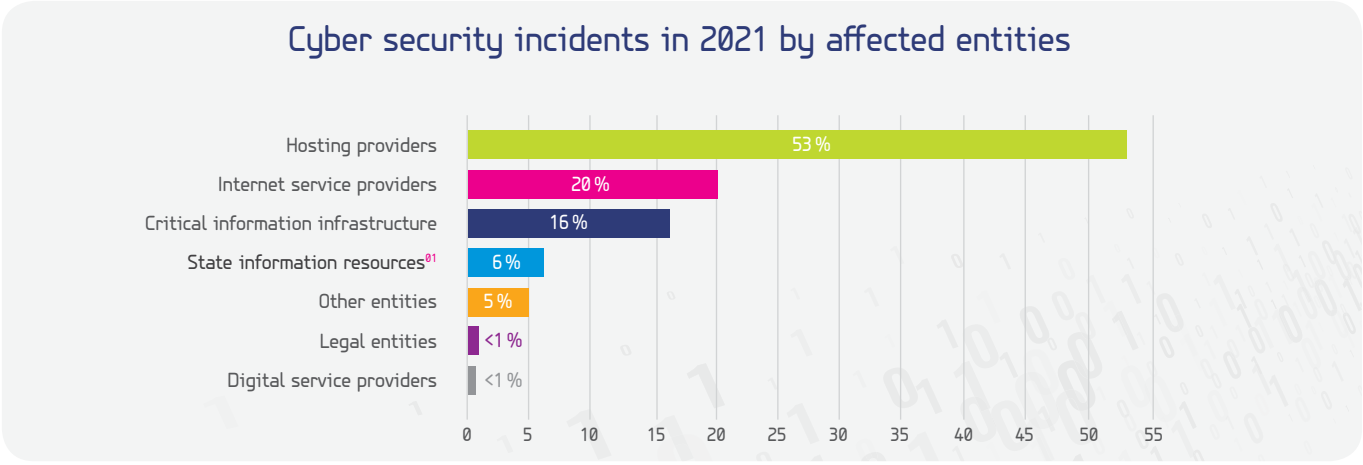
1. Lithuania is among the top ten countries according to the Global Cyber Security Index compiled by the United Nations' International Telecommunication Union (ITU).

Lithuania, with its score of 97.3, is sixth in the world and fourth in Europe according to the Global Cybersecurity Index (GCI) published by the ITU on 29 June 2021. Lithuania received highest assessment in the areas of legal regulation and the development of cyber security facilities. In the future, Lithuania will seek to maintain high level of the GCI by increasing the efficiency of cyber security technologies and organisational measures.

2. The total annual number of cyber security incidents registered by the Computer Emergency Response Team (CERT-LT) of the National Cyber Security Centre (NCSC) under the Ministry of National Defence (MoND) of the Republic of Lithuania remains similar as in the first year of the COVID-19 pandemic. In 2021, the number of cyber incidents that caused more intermediate damage increased, as they were more targeted and complicated. The intensity of cyber incidents remained high in the Q1 of 2022.

In 2021, CERT-LT recorded 4,088 cyber incidents. It is a 5% decrease compared with 2020, when CERT-LT recorded 4,330 cyber incidents. Notably, that 93 out of 4,088 incidents were classified as being of medium impact, and it is almost by one-third more than in 2020 when 67 cyber incidents of medium impact were recorded. A few notable incidents include a leak from the student database of the Vilnius College and hybrid attack on the Prienai Municipality's website.

Figure 1.
Cyber security incidents in 2021 by affected entities



More than half (53%) of all the cyber incidents recorded in 2021 by CERT-LT were related to the Lithuanian hosting service providers' infrastructure, which is used, e.g. for creating websites, virtual workstations, provision of email services and etc. Such a large percentage of cyber security incidents relates to the increasing activities of online fraudsters. For example, it is possible to pay for hosting services anonymously by cryptocurrencies; fraudsters have used these services to launch cyberattacks in Lithuania and other countries. The most malicious activities in 2021 were conducted on the hosting infrastructure of 'Interneto vizija' JSC (15%), followed by 'Host Baltic' JSC (10%), 'Hostinger International Limited' (7%), and 'Cherry Servers' JSC (6%).

01
State institutions that do not fall within the category of critical information infrastructure.

Ranking second are cyber incidents related to customers' terminal equipment (computers, smart devices etc.) that use Lithuanian Internet service providers. Due to insufficient protection, hackers often take over such equipment and use it for malicious activities. NCSC data shows that the majority of the intercepted consumer devices were mostly participating in *mirai* botnet attacks. In 2021, 20% of all recorded incidents were affecting customers of Lithuanian Internet service providers.

In the third position are cyber incidents recorded in the communications and information systems (CIS) of critical information infrastructure (CII) managers. It made 16% of all incidents in 2021.

The number of cyber incidents has remained high in the first three months of this year. The NCSC recorded 1,020 incidents during QI of 2022, which is more than in the same period last year (2021: 981). The number of incidents increased by one third in the eighth week of the year, when the war in Ukraine started. The increased focus on cyber security by both entities and individuals was the main reason for such spike. While the attention has subsided in the following weeks, vigilance remains essential, and both the authorities and the CII managers must be ready to ensure business continuity under various scenarios.

As in the previous years, most cyber incidents were related to the distribution of malware. Together with phishing, these are the main cyber incident threats in Lithuania. The numbers of both intrusion attempts of CIS (278) and successful intrusions (125) increased in 2021. One of the main reasons for the increase of intrusion attempts and successful intrusion attacks in 2021 is the infamous Microsoft Exchange zero-day vulnerability, which unfortunately some users did not patch in timely manner.

The number of Distributed Denial-of-Service (DDoS) attacks has decreased in 2021 (43 cyber incidents), which leads to an assumption that the interest in carrying out such attacks has lowered; however, due to their potential damage to the entities' availability, it should be treated as a possibly multiplying in volume and repetitive threat. The smaller number of registered spam emails (399 in 2021 and 739 in 2020) shows that the efficiency of cyber security measures implemented by the entities is gradually increasing.

Figure 2.
Number of cyber incidents by categories in 2021 and 2020

No.	Cyber incident category	2021	2020	Change
01	Malware	1,890	1,966	↓ 76
02	Phishing	1,187	962	↑ 225
03	Spam and misleading information	399	739	↓ 340
04	Intrusion attempts	278	171	↑ 107
05	Fraud	136	85	↑ 51
06	Intrusions	125	61	↑ 64
07	DDoS	43	75	↓ 32
08	Other incidents (not matching any of the aforementioned groups)	22	271	↓ 241
	Total	**4,088**	**4,330**	**↓ 242**

3. In 2021, the rising demand for stolen personal data and cases of ransomware increased.

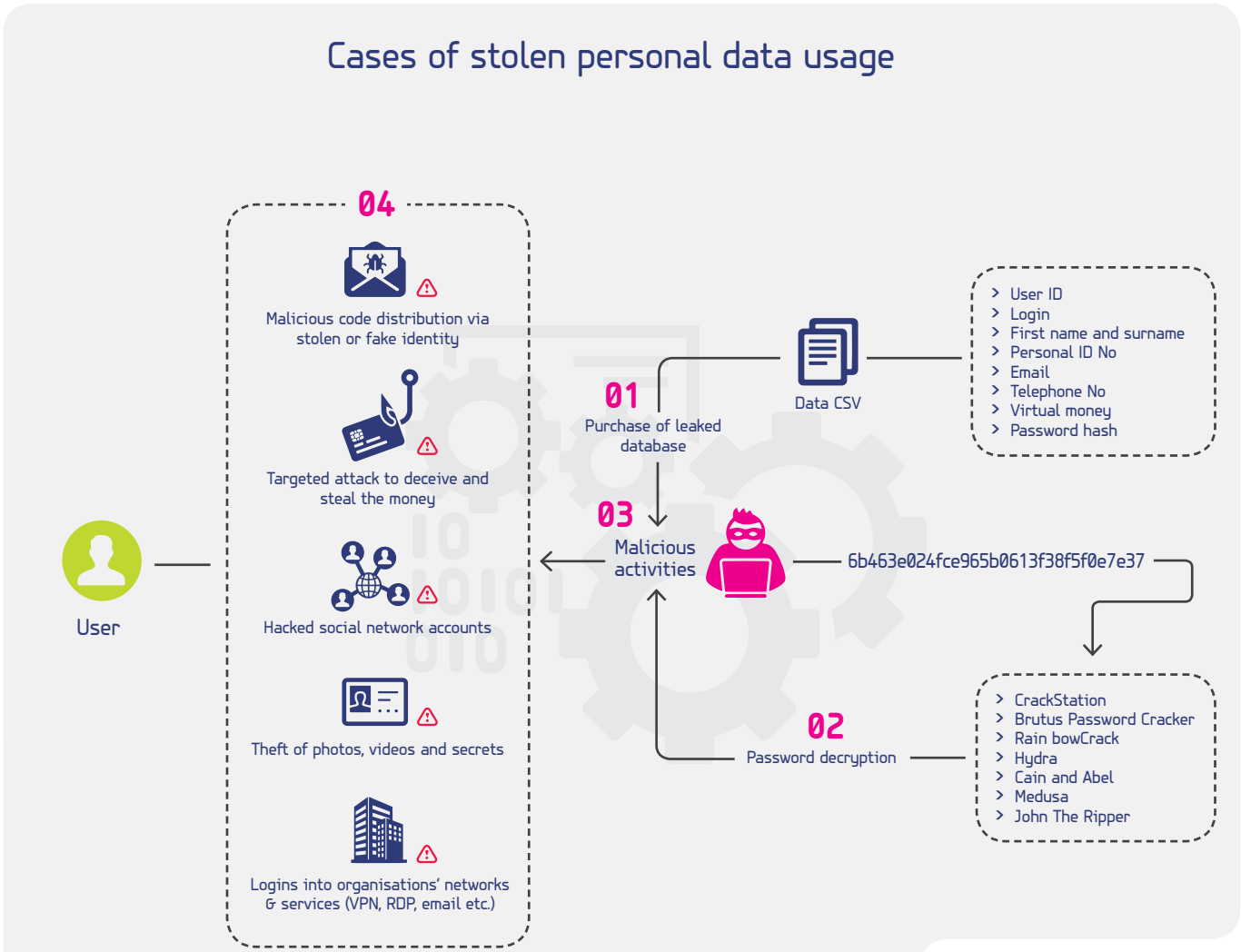
The demand for stolen personal data rose and determined an increase in such data theft and/or publication of previously leaked data. IBM in its annual report on data breaches[02] states that on average the estimated cost of one data breach for organisations was 4.24 million USD in 2021, which is a 10% increase compared with 2020.

According to IBM[03], approximately 60% of organisations moved their data to the cloud in order to continue their operations under restrictions imposed due to COVID-19 pandemic. However, there were no lateral application of relevant cyber security measures. Risks emerged because of the usage of cloud, since there were no control mechanisms implemented for data migration and storage.[04]

Such incidents were identified in Lithuania too. Irresponsible use of cloud resources and unregulated shadow IT practices have resulted in data leaks from 'Prime Leasing' JSC (linked to 'CityBee'), the Vilnius College and 'Kilobaitas' JSC.

02 IBM. **Cost of a Data Breach Report 2021**. https://www.ibm.com/security/data-breach.

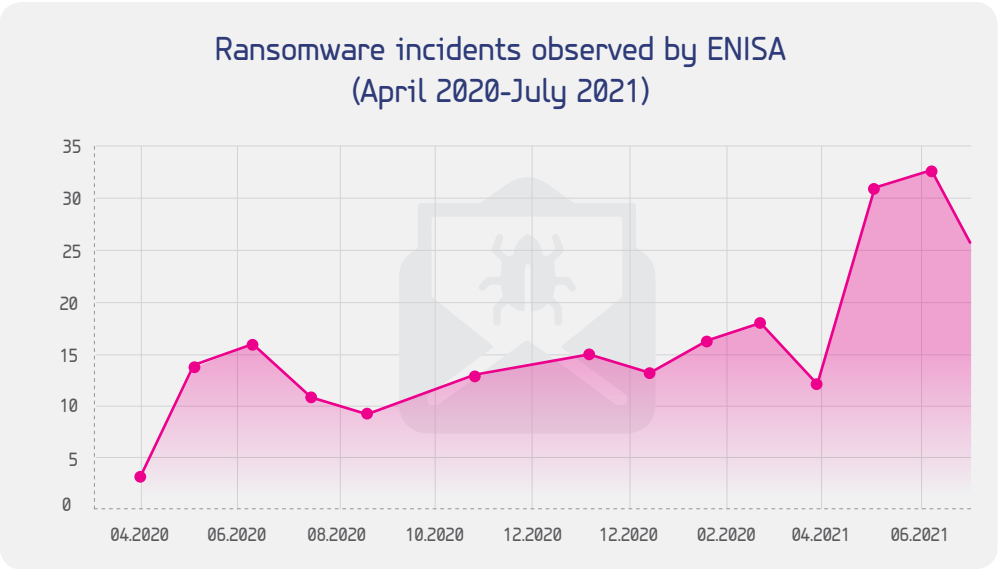
03 Charlie Osborne. **Enterprise data breach cost reached record high during Covid-19 pandemic** (2021-07-28). https://www.zdnet.com/article/enterprise-data-breach-cost-reached-record-high-during-covid-19-pandemic/.



^ **Figure 3.** Cases of stolen personal data usage (composed by NCSC)

04 David Puzas. **Cloud Security Risks, Threats, and Challenges** (2021-06-14). https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/.

According to the European Union Agency for Cyber Security (ENISA), ransomware attacks have been the highest threat since 2020.[05]



< Figure 4.
Ransomware incidents observed by ENISA (April 2020-July 2021) (Source: ENISA Threat Landscape 2021)

The European Union Agency for Law Enforcement Cooperation (Europol) has stated in its annual *Internet Organised Crime Threat Assessment 2021* (iOCTA)[06] that ransomware attackers exploit vulnerabilities arising from remote work: they scan networks of potential victims looking for insecure remote desktop protocol (RDP) and closely monitor published vulnerabilities for virtual private network (VPN). The report also notes that ransomware attacks aim at large organisations, public sector entities, and their supply chains. The United States identified this as a crucial threat, particularly considering the impact on the critical infrastructure after cyber incidents in May 2021 when the attacker targeted CIS of Colonial Pipeline, a US oil pipeline operator, and JBS, a North American division of the world's largest meat processing company. While this is a global threat, in Lithuania, by the end of 2021, NCSC recorded significant ransomware cyber incidents only in the infrastructure of a few private companies.

4. Website content management systems widely used in the public sector were the main target for information and communications supply chain attacks in Lithuania in 2021. Lithuania succeeded in avoiding significant damage to critical services from vulnerabilities such as SolarWinds, Microsoft Exchange, Pulse VPN and Log4J due to NCSCs, proactive dissemination of information and communication with cyber security subjects.

Supply chain attacks are well known to the cyber security experts, but their occurrences remarkably increased in 2020.[07] In Lithuania, this type of attacks were used against website content management systems that are provided by a few Lithuanian companies and are popular among the public sector institutions. These systems vulnerabilities were actively exploited for data thefts, fake news, and the hacking of organisations' information systems.

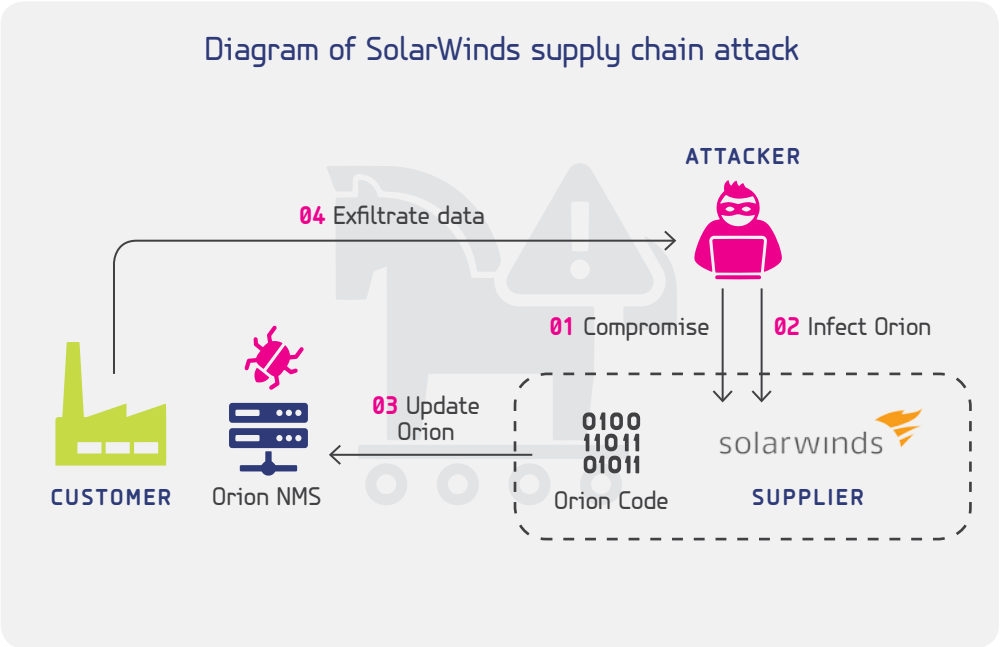
In response to the globally known vulnerabilities such as SolarWinds, Microsoft Exchange, Pulse VPN, Log4j etc., the NCSC took proactive measures to inform the cyber security subjects in 2021. Therefore, Lithuania avoided significant damage to critical service providers, although minor cyber incidents affected individual users, but Lithuania avoided significant damage to critical service providers. Still, cyber security experts warn that security issues related to Log4j vulnerabilities can last for a long time[08]. This will affect both data leaks and data thefts in the future.

05 **ENISA Threat Landscape 2021** (2021-10-27). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

06 Europol. **Internet Organised Crime Threat Assessment 2021**. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf.

07 **ENISA Threat Landscape for Supply Chain Attacks.** https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

08 Jonathan Greig. **Log4J update: Experts say log4shell exploits will persist for ‚months if not years'** (2021-12-13). https://www.zdnet.com/article/log4j-update-experts-say-log4shell-exploits-will-persist-for-months-if-not-years/.



< Figure 5.

Diagram of SolarWInds supply chain attack. The attackers compromised SolarWinds and modified the code of ORION software. The ORION instances in the customers were updated with malware, which allowed the attackers to access the data of customers (Source: ENISA Threat Landscape for Supply Chain Attacks 2021)

5. According to Lithuanian intelligence services, hacker groups coordinated by adversarial states remain the primary threat to security of information systems of Lithuanian institutions and organizations. There is an obvious correlation between major international political developments and hostile cyber activities targeting Lithuanian entities.

Russia-attributed cyber espionage groups are the most active comparing to other state-affiliated cyber actors. This is also a worldwide trend: Microsoft announced[09] that from July 2020 to July 2021 Russia had been responsible for 58% of all the detected state-sponsored cyber-attacks. The US, Ukraine and NATO nations are considered the primary targets of Russian cyber actors. The hackers not only collect data from the system they have compromised but also search for ways to get access to classified information, they analyse the system's architecture. While implementing this task, they try to get access to the targeted (usually state institution) networks undetected and create persistent mechanisms that allow espionage groups to access the system even if a malicious code is detected and partially removed. Over the recent years, espionage groups, traditionally known for their clandestine activity, have been used for more public operations – leaking of hacked information or destructive incidents. On certain occasions the information hacked is placed into a specific context or is mixed with fake information in order to discredit a person or organization, influence society's opinion in favour of Russia. Such Russian activity is detected in multiple states, including Lithuania.

Russian intelligence agencies not only use the tools associated with the criminal world but also cooperate with criminal hackers. Some of the criminal hackers provide ransomware-as-a-service. Such scheme further complicates the attribution. One of the examples of such activity possibly is a vast scale ransomware attack against the US oil product operator Colonial Pipeline and Japanese IT company Toshiba Tec Corporation unit in Europe, which were carried out by the group DarkSide in 2021.

In 2021, China also became increasingly active in using its cyber capabilities against Lithuania. China consistently increased the extent of its cyber espionage. China's aim to intensify the

09 **Microsoft Digital Defence Report 2021**. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/.

activities of cyber intelligence capabilities in Lithuania is considered as a threat to Lithuania's national security.

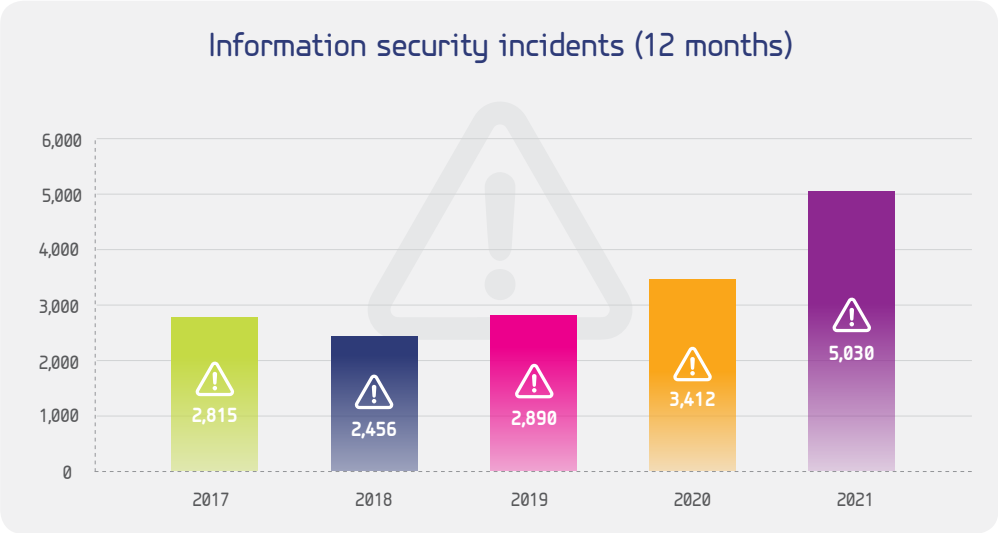
According to the information available to the Lithuanian intelligence agencies, the attractiveness for various adversarial states to use cyber means for subversive and espionage activities will very likely increase in the near term. Lithuania's institutions and related organisations will be among the main targets of cyber-attack groups coordinated by adversarial states.

6. 2021 was marked by the increased tension in the information environment

Dissemination of hostile information was deliberate in order to manipulate and influence public opinion in Lithuania, Russia and the Commonwealth of Independent States (CIS), Russian-speaking communities in other countries of Europe and the world, and EU and NATO member states.

Some of the European Union's Member States[10], including Lithuania, have been targets of Ghostwriter hacking operations linked to Russia. The EU and its Member States have unanimously condemned this malicious cyber activity in 2021[11] and demanded that Russia complies with the norms of responsible behaviour in cyberspace. At least nine information/cyber-attacks carried out in Lithuania's cyberspace in 2021 was part of Ghostwriters' campaign. Methods used for disseminating disinformation in the operations against Lithuania, other NATO Member States and Ukraine include: imitation of websites and (or) hacking them in order to change its content, spoofing e-mail sender information, hacking social network accounts and/or creation of fake accounts. It is very likely that in the future, the Ghostwriter activity will increase – both informational and cyber – in its efficiency.

The year 2021 was marked by an increase in the total number of cases of hostile informational activity: 5,030 unique cases (2020: 3,412).



< Figure 6.

Statistics of information security incidents by year (Source: Strategic Communication Department of the Lithuanian Armed Forces)

In the context of the past five years, 2021 was marked by a considerable increase in the hostile information activity aimed against the sectors of national defence, foreign policy, and protection of the Constitutional foundations. According to these sectors, the distribution of hostile activities in 2021 is as follows: defence – 29.93%, foreign policy – 29.86%, and protection of the Constitutional foundations – 22.88%.

10 As well as candidate countries (Republic of Northern Macedonia, Montenegro and Albania) and ELPA countries, that are members of the European Economic Area (Lichtenstein and Norway) and Ukraine and Sakartvelo.

11 Declaration by the High Representative on behalf of the European Union on Respect for the EU's Democratic Processes. https://www.consilium.europa.eu/lt/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/.

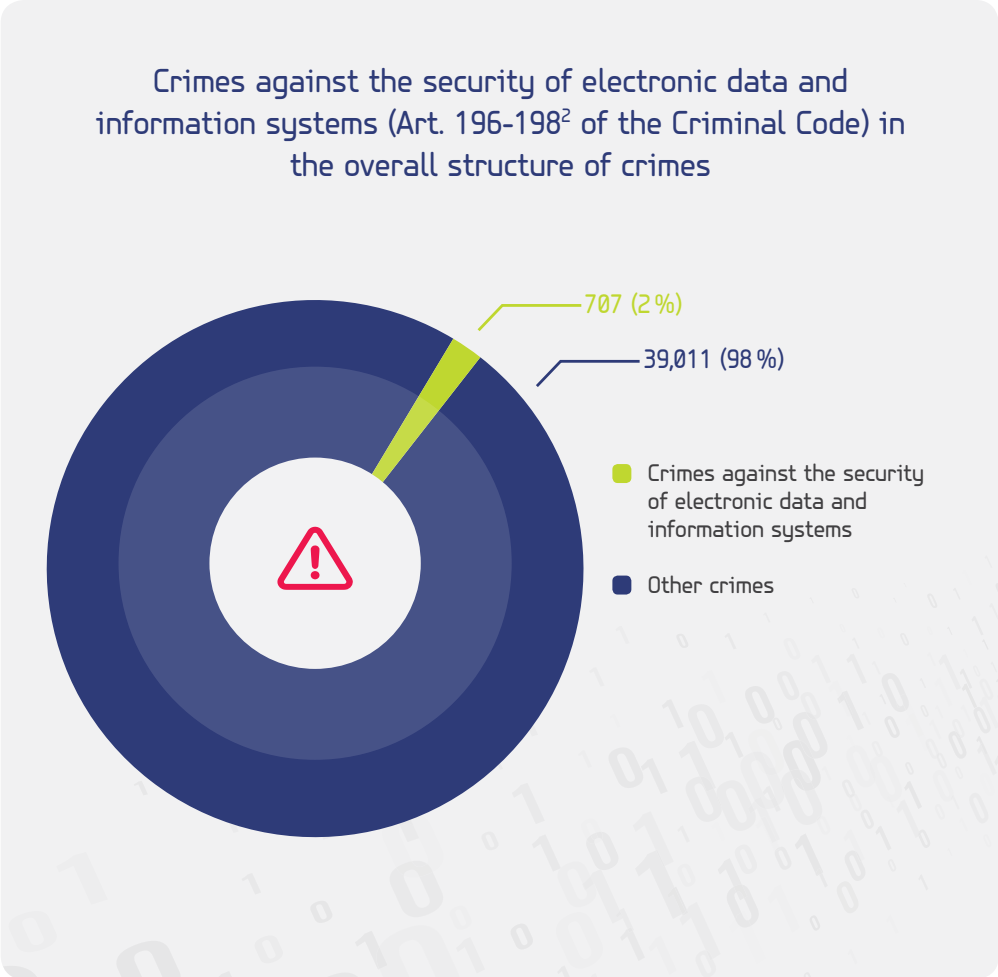
In 2021, the most frequently used hostile narratives aimed at the escalation of the defence subject. Compared with 2020, hostile narratives directly related to NATO, NATO-Russian relations, and Lithuania's membership in NATO have become even more prevalent:

(a) NATO is a threatening alliance that provokes Russia and Belarus and poses a threat to the security of these two countries.
(b) NATO will not defend the Baltic States in the event of war.
(c) NATO poses a threat to international peace and stability.

New hostile narratives related to illegal migration were identified in 2021. Such narratives were not present since 2017. A new topic - relations between Lithuania and China, appeared as well. Lithuania's decision to open Taiwan's representative office in Vilnius, which attracted the attention of the Chinese, Russian and Belarusian media, fuelled its escalation. Hostile actors disseminated manipulative message that national foreign policy is harmful to Lithuania.

7. In 2021, fraudsters lured 10.2 million EUR from Lithuanian residents and organisations – double the amount than in 2020 when 4.8 million EUR were lost to fraud[12].

In 2021, 707 crimes were recorded in Lithuania that breached the security of electronic data and information systems (Articles 196-198² of the Criminal Code of the Republic of Lithuania). In the overall structure of crimes, crimes against the security of electronic data and information systems amounted to 2% in 2021. Compared with 2020, such crimes increased by 51.7%, or by 241.



< Figure 7.
Crimes against the security of electronic data and information systems (Art. 196-198² of the Criminal Code) in the overall structure of crimes (Source: the Lithuanian Police)

12
Source: Lithuanian Banking Association. https://www.lba.lt/lt/apie-mus/asociacijos-naujienos/finansiniai-sukciai-is-gyventoju-ir-verslo-pernai-isviliojo-10-2-mln-euru.

Electronic fraud cases have remained dominant among crimes committed in cyberspace in 2021: they accounted for 71% of the total number of all cybercrimes. The structure of cyber fraud by types was as follows: telephone scams (vishing and smishing) – 70% of all cyber fraud cases, investment fraud – 17%, messenger scams – 8%, intercepting email communication and email scams – 5%.

A comparison between the years 2021 and 2020 shows that the largest increase (from 3 to 34 cases) has been in cybercrimes related to the search for data on information systems' vulnerability and/or electronic data theft.

An increasingly clear trend shows that the individuals committing criminal offences in the EU act as well-organised groups. Cybercriminals increasingly tend to select victims in a targeted way rather than randomly and hire hackers and malicious software developers to increase the scope and efficiency of ransomware attacks[13]. Criminals are constantly improving and frequently use state-of-the-art technologies to protect their anonymity. Criminal profiteering was the prevailing (84%) motive for cyber-crimes in 2021[14].

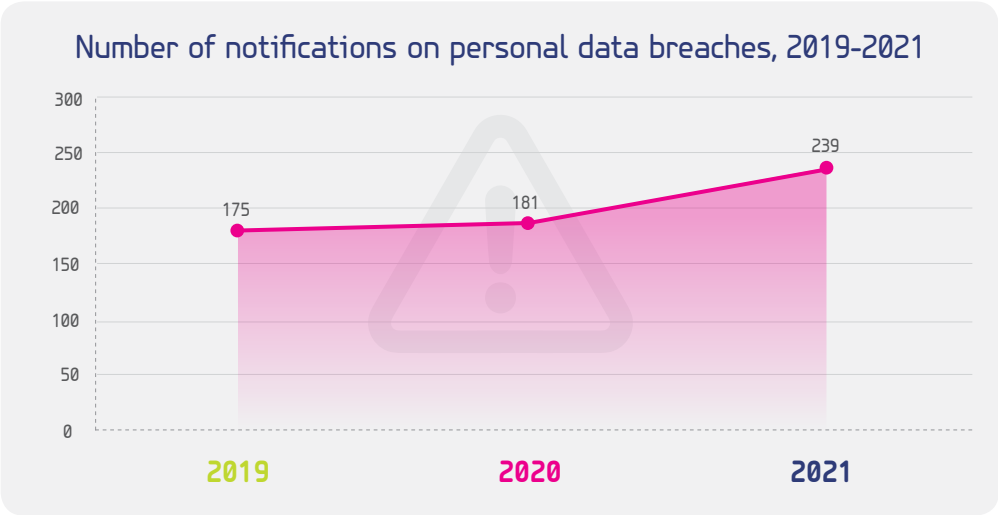
The Police Department paid attention to preventive measures that are the most efficient way to fight crime. In 2021, the Police Department held 13,772 meetings for the society where the participants were taught how to recognize crimes in cyberspace and how to protect against them. This measure reached the audience of 284,659 people. In addition, tremendous attention is devoted to collaboration with the banking sector. The Centre for Money Laundering Prevention Competencies, which was launched in May of 2021, formed a tactical collaboration unit within the Centre. The Ministry of Finance, the Bank of Lithuania and eight commercial banks operating in Lithuania, established the centre jointly.

8. A one-third increase in the number of notifications on personal data breaches (PDB) shows that both data controllers and data processors seek to perform their duties under the General Data Protection Regulation (GDPR) more responsibly. It also shows that the trust in the State Data Protection Inspectorate (SDPI) is increasing. However, to prevent serious personal data breaches related to cyber security incidents in Lithuania, it is necessary to enhance a unique data protection culture.

In 2021, the SDPI received 239 notifications on the PDB in Lithuania, which is one-third more than in 2020 (181 notifications). The majority of PBD cases in Lithuania are related to the confidentiality breaches; the number of PBD cases related to cloud services and leaked databases with the considerable amounts of personal data has also increased significantly. Notably, in November 2021, the SDPI imposed an administrative fine of EUR 110,000 on 'Prime Leasing' JSC, the operator of 'CityBee' short-term car rental platform. This is the most severe fine since the start of applying the GDPR in Lithuania due to a violation of the GDPR provisions regarding the security of personal data processing.

13 Organized Crime Threat Assessment (iOCTA). https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

14 Ibid.



< Figure 8.
Number of notifications on personal data breaches, 2019-2021 (Source: SDPI)

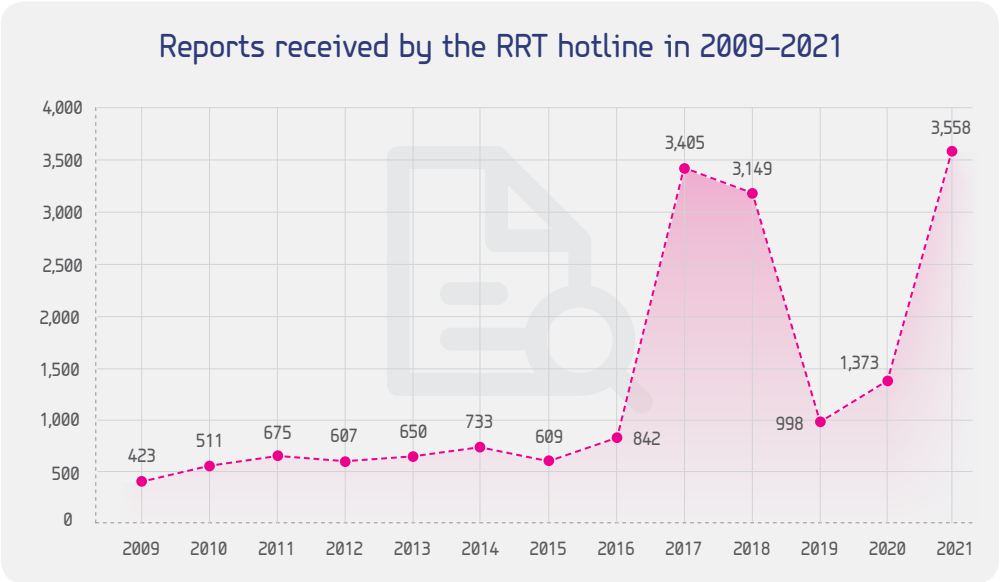
According to the SDPI, in 2021, Lithuania had 2,746 data protection officers appointed in the public and private sectors. However, their involvement in all activities of an organisation related to personal data processing is still insufficient; furthermore, top management often has an inadequate understanding of the importance of personal data protection.

Based on the results of the annual representative population survey in 2021, the SDPI calculated, for the first time, the level for personal data protection in Lithuania. It reaches 60% and allows to measure knowledge of citizens about the GDPR, the SDPI and their rights; trust in organisations that are involved in the processing of personal data; individual actions on encountering potential breaches; trust in the supervision system. Regarding the established level of conditions for personal data protection, the SDPI recommends promoting data protection culture in private and public sector organizations, and increasing public awareness of personal data protection in Lithuania.

9. In 2021, the continuing pandemic remained a considerable challenge due to the load in the electronic communications infrastructure. Nevertheless, according to the Communications Regulatory Authority (RRT), the capacities of public communications networks have been sufficient.

In 2021, the RRT received eight reports on public communications network integrity breaches from four service providers (2020: 10 reports). One of these breaches emerged by the scale of its impact on final service recipients. However, neither aforementioned, nor other breaches in 2021 resulted in an emergency that would require by law additional actions and/or to inform other institutions.

During the pandemic, internet users, who spent considerably more time online, sent to the RRT's Clean Internet hotline (**www.svarusinternetas.lt**) 3,558 reports about content found on the Internet that is prohibited to be disseminated or adversely affects minors. This is the most significant number of reports since the establishment of the hotline in 2007. The majority of the reports dealt with images of child sexual exploitation, which, after being investigated and approved by the RRTs' specialists, were referred for further investigation to the Police Department. In order to remove such content from their servers or to terminate access to it as soon as possible, the information hosting service providers in Lithuania as well as service providers or members of INHOPE, the International Association of Internet Hotlines, were informed about these reports too.



< Figure 9.

Reports received by the RRT hotline in 2009–2021

In order to carry out duties assigned by law, the RRT approves mandatory filtration measures that must be installed in public computer network (internet) access points, which are visited by minors. On annual basis, RRT conducts surveys on children's educational institutions and public libraries. The surveys show that the use of approved filtration measures at such institutions increases every year.

10. Public sector website periodic scanning increased in scope by including regional public sector institutions.

The scope of the public sector website scanning has increased by approx. 50% in 2021 from 996 scanned websites in 2020 to 1,497 in 2021. This has resulted in a much larger number of detected vulnerabilities (a 60% increase) – 12 per website on average (2020: 7.5). The scanning by the NCSC has shown that 58% of all the public sector domains checked had cyber security vulnerabilities mainly related to open administration access and not updated versions of content management systems.

In 2021, the NCSC issued special recommendations and a consolidated list of basic security requirements to enhance the security of the public sector websites[15] that applies to new and existing websites.

11. Lithuania is one of the four EU Member States that adopted laws legitimising 'ethical hacking', which increased the number of cyber security vulnerabilities, reported on a responsible disclosure basis.

On 28 June 2021, amendments to the Republic of Lithuania Law on Cyber Security entered into effect. These amendments establish a CIS vulnerability disclosure model. According to this model, the organisation concerned and/or the institution managing the disclosure process are the first to receive information about vulnerabilities detected. The NCSC is responsible for such coordination functions in Lithuania. In 2021, the Centre received 81 reports on various cyber security vulnerabilities submitted following the principle of responsible disclosure (2020: 40 reports). The majority of the reports deal with vulnerabilities of websites and internet systems, with a few reports on critical vulnerabilities of state information systems and widely used software.

15 Recommendations for Security Requirements for the Technical Specifications of Websites. https://www.nksc.lt/doc/biuleteniai/WEB-TS-Saugumo-reikalavimu-rekomendacijos.pdf.

12. Lithuania launched a sectorial military Computer Emergency Response Team (Mil-CERT) in order to prevent and respond to cyber incidents in the National Defence Network (NDM) more effectively.

At the beginning of 2021, NKSC started a joint effort with Lithuanian Armed Forces and formed the first sectorial CERT – Mil-CERT – led by NCSC experts. The new CERT ensures cybersecurity of the NDN by providing key services.

< Figure 10.
Cybersecurity Services in the National Defence Network

In 2021, Mil-CERT responded to 365 cyber incidents. In order to reduce incident numbers, Mil-CERT focused on the users, with the goal of spreading cybersecurity awareness and raising knowledge level across the network.

Sophistication of attacks increases annually in Lithuania, leading to higher impact incidents occurring more often. As Mil-CERT's experience proved in 2021, due to its adaptation to a specific environment, sectorial CERTs are better equipped to fight sophisticated and targeted attacks, leading to a safer cyberspace for everyone.

13. In 2021, enhancement of the Secure National Data Transmission Network (the Secure Network) continued by upgrading its infrastructure, introducing additional collective website security measures, and discontinuing the operation of irrelevant and insecure information resources.

2021 was marked by the enhancement of the Secure Network's user websites. In collaboration with network users, additional collective security measures were implemented in order to protect approx. 130 websites. Completing an entire inventory of the information resources resulted a removal of approx. 230 insecure and irrelevant resources that were still in use. Additionally, 2021 was marked by an implementation in processes and tools for continuous detection and elimination of vulnerabilities in particular information resources of the Secure Network. To ensure that the software and hardware correspond to the relevant cyber risks and remove such equipment provided by unreliable manufacturers, more than one-third of the terminal infrastructure network elements and part of the Secure Network's critical node infrastructure have been upgraded.

On 14 April 2022, the manager of the Security Network – the Core Centre for State Telecommunications – held exercises aimed at testing the continuous operations of the Security Network. During the exercise, it was checked how intercommunication facilities, websites and e-service portals (e.g. **www.lrv.lt**, **www.registrucentras.lt**, **www.epaslaugos.lt**) of 300 state and municipal institutions would operate in an emergency, on disconnection of the global internet communications, and how interoperability of public registers and information systems would be ensured.

NCSC continued to develop its Cyber Security Information Network, and used specific cyber threat prevention instruments for monitoring data traffic of 267 organizations within the area of control of state information resource (SIR) and CII managers.

14. The enhancement of the supply chain security of Lithuanian contracting authorities has continued. In addition, steps were made in order to ensure that state institutions and sectors that are critical in terms of national security, including 5G infrastructure, would not use products supplied by unreliable manufacturers.

MoND continued supervision over procurement procedures conducted by managers of CII. In 2021 MoND assessed approx. 200 objects of procurement (involving CII), and issued recommendations regarding technological risks that may arise during the procurement process and obligation to set security requirements set in the procurement documents.

State institutions and sectors that are critical for national security are prohibited from using Information and Communication Technology (ICT) equipment and technologies supplied by unreliable manufacturers; public sector organisations and CII managers are not allowed to purchase ICT goods and services if the country/territory of origin of the supplier or controlling person is deemed to be unreliable. The Seimas (Parliament) of the Republic of Lithuania on 17 March 2022 approved such amendments to the public procurement laws, which were initiated by the MoND in December 2021, as a matter of urgency. The amendments form part of the management of threats to national security arising from unreliable ICT goods and services. The new regulation applies to all contracting authorities that are CII managers, are users of the Secure Public Data Network, or operates in the defence sector or a sector critical for national security. There are almost 500 such entities in Lithuania.

5G communication is developing rapidly in Europe, and the GSM Association estimates[16] that Europe will have 276 million 5G connections in 2025. 5G can pose a threat to the public communication network infrastructure if criminals exploit the vulnerabilities of communications equipment and smart devices. Therefore, on 25 May 2021, the Seimas adopted amendments to the Republic of Lithuania Law on Electronic Communications and the Republic of Lithuania Law on the Protection of Objects of Importance to Ensure National Security that aims to ensure that only reliable manufacturers and suppliers provide ICT equipment and services in the development of the 5G communications infrastructure in Lithuania.

16 **GSMA Intelligence website.** https://www.gsmaintelligence.com/data/.

15. In selecting smart consumer devices, residents of Lithuania should take into account not just price criterion but also the results of manufacturer reliability assessments made by the NCSC and other organisations investigating cyber security issues on a periodic basis.

In 2021, the NCSC carried out a security investigation of smart 5G devices supplied by Chinese manufacturers Huawei P40 5G, Xiaomi Mi 10T 5G and OnePlus 8T 5G in order to ensure the safe use of 5G mobile devices sold in Lithuania as well as software implemented in such devices.

The NCSC research found four critical cyber security risks not recorded in the global cyber vulnerabilities database: two of them related to the apps installed in the devices by the manufacturer, one posing a personal data leakage threat, and one pertaining to potential restrictions on freedom of expression. Three risks found in Xiaomi mobile device and one in Huawei mobile device; no cyber security vulnerabilities identified in the OnePlus device.

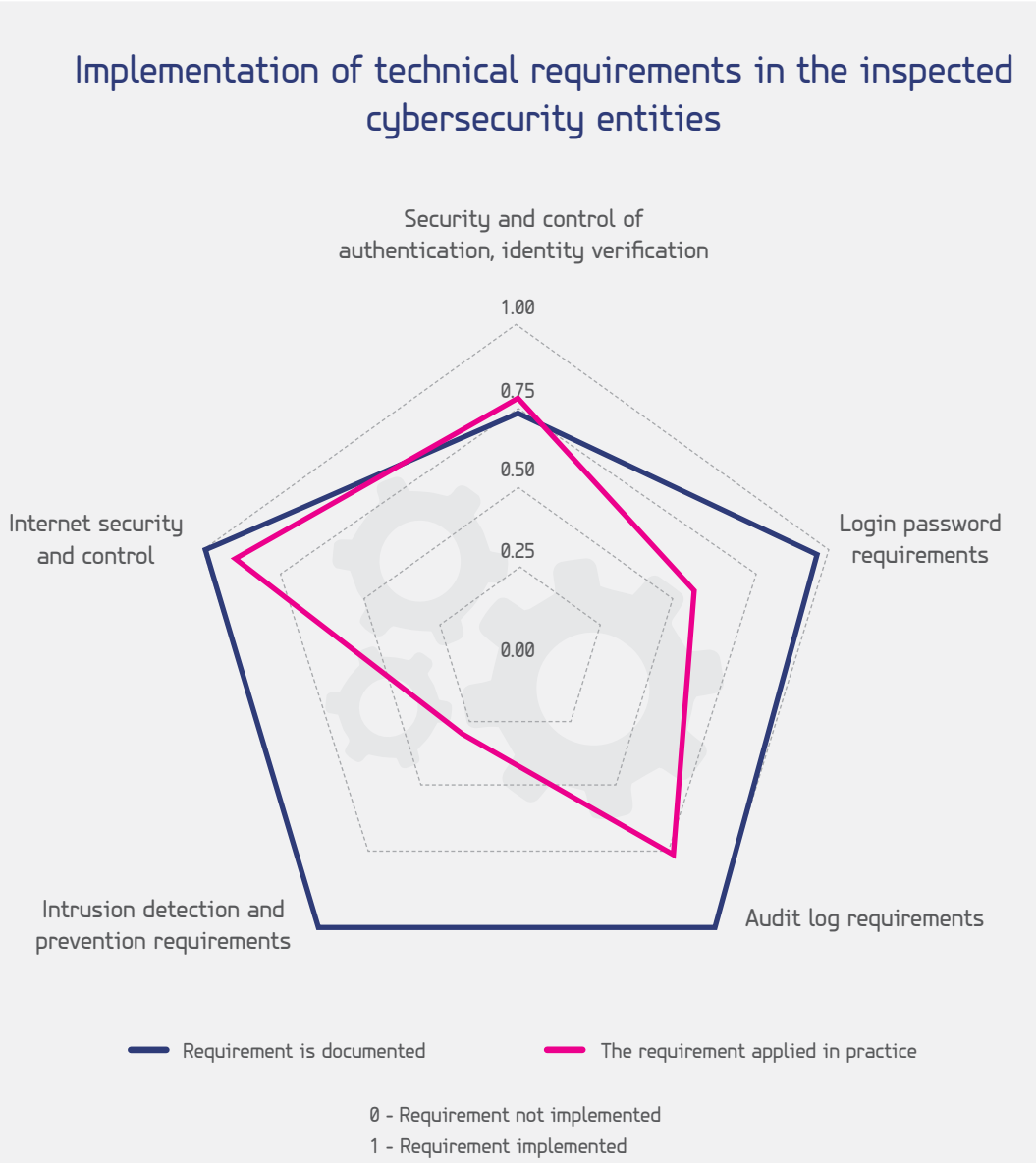
16. The level of implementation of organisational and technical cyber security requirements by SIR and CII managers and/or administrators remain insuficient. In order to foster positive changes in this area, the MoND is launching a new-generation cyber security requirements development project.

The attack surface is exponentially expanding due to the digital development. Complex cyber-attacks target EU institutions, state and municipal institutions, organisations of the Member States and CII managers. Smooth and timely implementation of the cyber security requirements at all such institutions and organisations ensures the efficiency of their activities in cyberspace as well as uninterrupted provision of services to the public.

According to the NCSC, 77% of all Lithuania's SIR managers have successfully completed the process of agreement on their security documentation with the NCSC by the end of QI of 2022 (51% as of the end of 2020). To speed up the process, in 2021, the NCSC started sending to relevant entities mandatory instructions for submitting security documents. During 2021 and QI of 2022, such instructions were issued to 52 entities; an administrative penalty – a warning was issued to three entities in accordance with the Administrative Code of the Republic of Lithuania.

After the start of the war in Ukraine in February 2022 and following the sharp rise in the cyber security risks, especially against Lithuania's CII and SIR, NCSC paid special attention to this area and provided instructions for the managers of CII and SIR. Other preventive measures were implemented too.

NKSC in order to determine the status of cyber security stakeholders conducts surveys and inspections (both scheduled and non-scheduled). In 2021, five scheduled and four non-scheduled inspections took place. The results show that the level of implementation of organisational and technical cyber security requirements has not changed in 2021. In many cases, requirements are formally implemented and implementation processes, although described, are carried out in a way that does not ensure continuity in the event of staff turnover.



In 2021, the MoND published the draft version of a project on the new-generation cyber security requirements in order to raise the level of implementation of organisational and technical cyber security requirements by the managers of SIR and CII. The New Generation Lithuania (NKL) measure of the Recovery and Resilience Facility (RRF) will finance the implementation of the project.

Acknowledging the varying levels of cyber security maturity among different stakeholders in the EU Member States, the European Commission seeks to resolve the issue by second directive on measures for a high common cyber security level across the Union ('NIS2 Directive'). The directive aims to eliminate the discrepancies in the cyber security implementation and requirements measures among the Member States. In addition, the directive aims to continue enhancing incident response capacities and the resilience of both public and private sectors as well as the EU as a whole. More stringent cyber security requirements and liability for failing to comply with them (including administrative penalties) are among some measures to achieve high common cyber security level.

^ Figure 11.
Implementation of technical requirements in the inspected cybersecurity entities in 2019-2021

17. Employees are one of the weakest links in ensuring cyber security. Therefore, enhancement of their cyber skills must be a continuous process in the public and private sectors.

Human, an employee is among the most frequent vectors of a cyber-attack. According to a research conducted by Verizon[17], 85% of cyber incidents occurs due to human error. The reasons for such errors vary from clicking on virus-infected links to the disclosure of passwords and accidental deletion of data.

Irrespective of who delivers cyber security training – the organisation itself or hired instructors, professionals recommend organizing around 11 cyber security-training events annually.[18]

KIBERNETINIS SKYDAS 2021

In 2021, the NCSC held basic one-day cyber security training for over 2,000 employees from over 20 public sector organisations in order to improve their cyber security knowledge. The employees who had completed the theoretical training course had an opportunity to check their knowledge in an annual national cybersecurity exercise *Cyber Shield 2021*. This major national cyber security exercise included 92 organisations from both the public and private sectors. Managers of SIR and CII accounted for the majority of the participants (87 organisations). NCSC, the Kaunas University of Technology (KUT), and the Lithuanian Research and Education Networks (LITNET) KUT technical center organized this event. The primary purpose of the exercise was to test the participants' practical abilities to respond effectively and manage cyber incidents of various types and scopes.

At the beginning of 2022, the NCSC launched a project entitled Integrated Cyber Security Training for Public Servants and Employees of State and Municipal Institutions and Organisations financed by the EU Structural Funds. Public servants and employees (total 1,200) took part in the training in QI of 2022, thus enhancing their theoretical and practical knowledge in the cyber security area. NCSC estimates that in 2022 the integrated three-day training will involve 2,000 participants.

18. International cooperation in the cyber security area remains Lithuania's priority in terms of building national, regional capacities and supporting the associated members of the Eastern Partnership, namely Ukraine and Sakartvelo in the cyber security area.

REGIONAL CYBER DEFENCE CENTRE

In July 2021, the Regional Cyber Defence Centre (RCDC) launched its activities. This Centre, a branch of NCSC, is a joint initiative of Lithuania and the US. Ukraine and Sakartvelo joined this initiative as well. In February 2022, RCDC launched a pilot project *Securing Cyber Space of Ukraine Together*. Its purpose is to share cyber information on Ukraine. Recently, Poland successfully joined RCDC members in this pilot project.

In 2021, the US support programme called the Counter Russian Influence Fund, allocated funding which will help the RCDC to implement new-generation high-efficiency cyber security facilities (sensors) and to establish a cyber range - training infrastructure - polygon.

17 **Verizon Data Breach Investigations Report**. https://www.verizon.com/business/en-gb/resources/reports/dbir/2021/results-and-analysis/.

18 **How often should businesses run cybersecurity awareness training?** (2021-05-20) https://www.idagent.com/blog/how-often-should-businesses-run-cybersecurity-awareness-training/.

Since 2018, Lithuania has been coordinating EU PESCO (Permanent Structured Cooperation) project, *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security* that includes representatives of six EU Member States: Estonia, Croatia, Poland, Lithuania, the Netherlands and Romania. The cyber rapid response teams (CRRTs) reached and tested their full operational capacity in May 2021 during Alarmex exercise in Vilnius and Warsaw. In February 2022, the CRRT was activated to provide support to Ukraine.

Issued by the Ministry of National Defence of the Republic of Lithuania,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
16/05/2022

Layout by the Visual Information Division of the General Affairs Department
of the Ministry of National Defence, Totorių g. 25, LT-01121 Vilnius
Illustrations from the Freepik.com graphic recource platform were used