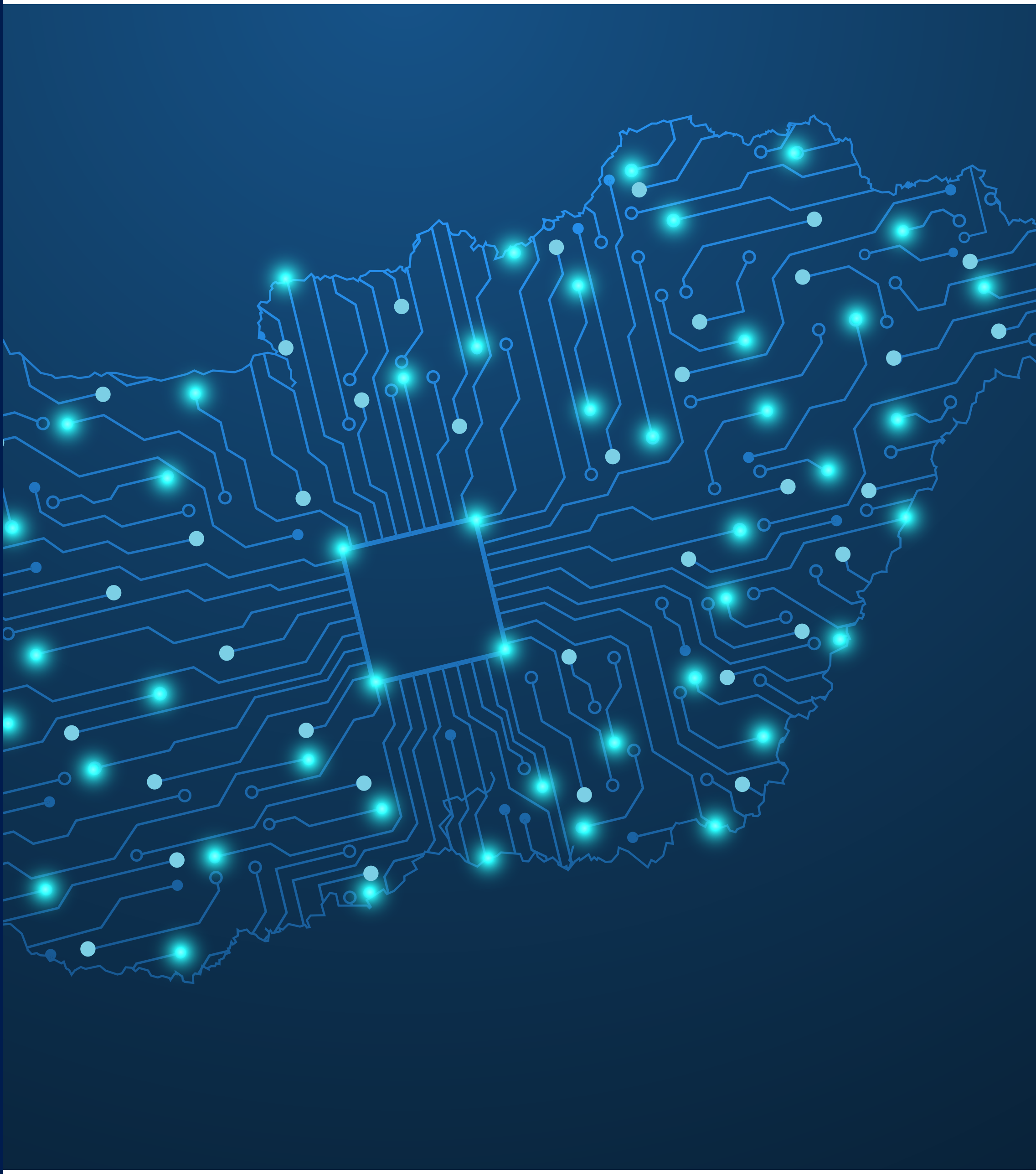
CYBER THREAT LANDSCAPE REPORT OF THE HUNGARIAN FINANCIAL SECTOR 2022



2022

DECEMBER

“Total security has never been available to anyone. To expect it is unrealistic; to imagine that it can exist is to invite disaster.”

Edward Teller

CYBER THREAT LANDSCAPE REPORT OF THE HUNGARIAN FINANCIAL SECTOR 2022

2022

DECEMBER

Cyber Threat Landscape Report of the Hungarian Financial Sector 2022

(December 2022)

The publication was approved by: Financial Stability Board

Funded by
the European Union

Published by the Magyar Nemzeti Bank

Publisher in charge: Eszter Hergár

Editor: Gabriella Biró

H-1013 Budapest, Krisztina körút 55.

www.mnb.hu

ISSN 2939-7758 (on-line)

Act CXXXIX of 2013 on the Central Bank of Hungary sets the achievement and preservation of price stability as the primary and continuous objective of the Central Bank of Hungary. Without endangering this objective, the Central Bank of Hungary supports the preservation of the stability of the financial intermediary system, the increase of its resilience, the assurance of its sustainable contribution to economic growth and the economic policy of the Government with the instruments at the disposal of the Central Bank.

The supervisory strategy of the Central Bank of Hungary, thereby reinforcing the objective set out in Act CXXXIX of 2013 on the Central Bank of Hungary, has identified the support and deepening of the stability of the financial system as its main objective until 2025. Thanks to digitalisation, the importance of and dependency on ICT solutions and digital services in the financial sector are continuously increasing, therefore achieving the resilience of the financial system requires particular attention to the digitalisation processes, their security, and their threats.

In this publication, the Central Bank of Hungary presents the cybersecurity threat landscape of the financial sector in Hungary for the period February-August 2022. The aim of the report is to provide an adequate and comprehensive picture of current threats and to identify the main trends, thereby supporting the participants of the financial sector to identify and prepare for the threats that are relevant to them. With this publication, the CBH contributes to developing and ensuring the cybersecurity resilience of the financial sector and supervised institutions, and the general improvement of cybersecurity awareness and preparedness.

The “Cyber Threat Landscape Report of the Hungarian Financial Sector 2022” was prepared under the project “Developing a methodology for the analysis of cyber threats in the financial sector and the preparation of a threat landscape”, supported by the European Commission’s (Commission) Directorate-General for Structural Reform Support (DG REFORM). The analysis was prepared by the Information Technology Supervision Department of the CBH.

In the report, the CBH’s experts mainly used information for the period from 1 February to 31 July 2022, with particular attention to the analysis of emerging cyber threats within the financial sector and incident data received during the pilot project within the project on the preparation of the cyber threat landscape report.

Contents

I Executive summary

This publication, the "Cyber Threat Landscape Report of the Hungarian Financial Sector 2022", published by the Central Bank of Hungary (hereinafter: CBH), provides a comprehensive view of the key cybersecurity threats affecting the Hungarian financial sector, the main trends observed in relation to these threats and a high-level overview of the incidents experienced in the Hungarian financial sector.

This publication was produced with the support and funding of the Technical Assistance Instrument 2021 programme of the European Commission's (hereinafter: Commission) Directorate-General for Structural Reform Support (DG REFORM). Following the Commission's decision, the Hungarian office of Ernst & Young Consulting Ltd. assisted the CBH in the implementation of the project.

The project started in September 2021, with a survey of the national incident reporting obligations in the financial sector and an international outlook. Taking these into account, a methodology for reporting incidents has been developed and a six-month Pilot Project involving 39 institutions (including 12 insurance undertakings, 5 banks, 10 funds) was carried out between 1 February and 31 July 2022 to collect and analyse detailed incident data – supplemented by some additional data – on which the report is based.

After the introduction of the whole project, the report is divided into four main parts: the general overview – international and domestic, including other sectors – is followed by the description of threat trends identified based on all incidents and in particular critical incident data, then an analysis of the technical data of the potential attack surfaces visible from the Internet and externally accessible security settings of the institutions participating in the project, and finally the reader is given a methodological overview of the tools and approaches used during the pilot.

The key conclusions of the report can be summarised as follows:

- the international trends appear with a slight (few months) delay in Hungary as well; the risks and threats are virtually identical, so it is worth paying attention especially to European events and to base domestic defence priorities on them,

- the vast majority of the incidents collected within the pilot (70%) were traditional malfunctions, so prevention and timely response is currently a more efficient way to maintain cyber security than defensive measures focused on cyber-attacks,

- evidence from multiple sources suggests that during the summer months, especially during periods when there are fewer changes/upgrades to IT systems, there are significantly fewer incidents affecting the operation of systems, therefore more careful change management may play an important role in preventing malfunctions,

- actual cyber-attacks – typically various forms of phishing – primarily target customers, so in addition to technical control measures, it is important to raise customer security awareness while defending against attacks and preventing damage,

- during the pilot, the CBH received far more detailed and significantly better quality incident data than under the mandatory supervisory reporting and the institutions participating in the project themselves gave positive feedback on the reporting process,

- there is no detectable correlation between the incidents collected during the pilot and the externally accessible Internet security settings of the institutions.

With the publication of the *Cyber Threat Landscape Report of the Hungarian Financial Sector 2022* the project itself is not the end of the project, the methodological work will continue, and it is foreseen that after the refinement of the incident reporting procedures, the CBH will regularly, annually produce a similar analysis based on the available data.

II Introduction

The financial sector is particularly affected by global digital transformation pressure and the need to move to online and paperless solutions. The CBH's FinTech and Digitalisation Report 2022 also revealed that "*The digital transformation of the financial sector gained new momentum in 2021. The COVID-19 pandemic, and the surge in digitalisation that accompanied it in the expanding range of financial services, has led to an increasing openness—and in many cases, increasing expectations—on the part of customers to use digital solutions.*" This indicates that a financial service provider that is unable to respond in a timely manner to changing customer needs may fall irrevocably behind. To achieve business goals in a highly competitive environment, IT solutions that have been in use for decades need to be complemented by continuous improvement, innovation, and the introduction of new solutions. In order to adequately serve diverse and varied customer needs, the broadening use of traditional solutions and the rapid integration of innovative technologies make cyber risks and cybersecurity a high priority, and accelerated digitalisation developments mean that institutions and their IT security experts are also facing a greater number and complexity of information security risks and threats.

The implementation and operation of efficient protection systems is positively supported if the institution knows based on its services and activities which are the current key threats that it most certainly needs to guard against. This can be greatly aided by comparing and summarising recent incidents and the main identified threats. It is now a common expectation in the financial sector that institutions monitor, promptly detect, manage, and record their incidents; in fact, the European Union (hereinafter: EU) is further deepening and tightening this set of requirements through its Digital Operational Resilience Act (DORA), to make financial sector institutions gain more digital resilience uniformly across the EU.

However, most institutions process information related to detected incidents internally, inter alia because of their confidential nature. This could lead to the creation of excellent micro-knowledge centres in the sector at institutional level. At the same time, the isolated operating model means that the possibilities of the participants of the financial sector in Hungary have a limited possibility to collate, analyse and share threat data and identify possible correlations at sectoral level.

The CBH has identified this gap and recognised the potential of exploiting the scattered knowledge base available within institutions and has initiated the EU-funded project *"Developing a methodology for the analysis of cyber threats in the financial sector and the preparation of a threat landscape"*.

Within the project, the CBH, leveraging on the existing incident and threat information and the EU's objective as stated in the DORA Regulation that incidents and potential threats in the financial sector should be collected by the national authorities, initiated the development of a methodology that enables the use and feedback of this data to the institutions of the financial sector. In other words, with the use of the available data, the CBH aims to fill the gap with Hungary's first sector specific cyber threat landscape publication. With the creation and publication of this threat landscape it is the express aim of CBH to support the entire domestic financial sector with a comprehensive, realistic, and sector specific threat analysis for a specific time period. According to the CBH, this will help institutions to plan, operate and fine-tune their protection and risk management tasks more effectively and to set cybersecurity priorities appropriately. Preventing and preparing for current threats supports the efficient operation, stability and integrity of financial services and helps institutions to prevent loss, damage, and disruption of services due to incidents.

A sub-task of the project was to collect and process incident reports sent in by the institutions participating in the project over a period of six months. The analyses presented in the publication are based on data from incidents identified in the day-to-day business operations of the participants of the financial sector. As a result of this, a data structure has been built up during the project that was not previously available in Hungary. The processing of the data provided the opportunity to look for deeper, sector level correlations, which are explained in more detail in Chapter IV (Presentation of identified threat trends).

The cyber threat landscape provides a summary of the characteristics of incidents in the financial sector, their different features and, in some cases, how they are managed.

The publication aims to reach a wide audience:

Primarily it contains important and useful information and data for senior managers, decision makers, and IT security experts in financial sector institutions. For senior managers, the publication presents a comprehensive cyber threat landscape to help them understand and gain a general overview of the threats their institution may face. For decision makers it may provide a good overview of the main threats and incidents in the sector in a given period (the previous year or semester), allowing them to identify which areas to focus on (even in the context of risk assessment) while considering trends (and their own development). IT security professionals will be able to apply the information presented in this publication and in Chapter VI, which also presents the issues, when designing, preparing, or modifying security solutions.

On the other hand, the publication may also orient service providers providing services to the institutions of financial sector, giving them useful information on the most typical incidents in each sector or type of institution.

1. INTRODUCTION OF THE CBH'S CYBER THREAT LANDSCAPE PROJECT

Based on the above, the CBH, in line with the EU's objectives to enhance digital resilience, has recognised the importance and need to develop an adequate and comprehensive landscape of the current threats to the financial sector, to identify and focus on key trends, and to enable the CBH to assist and support institutions in preparing for the main threats.

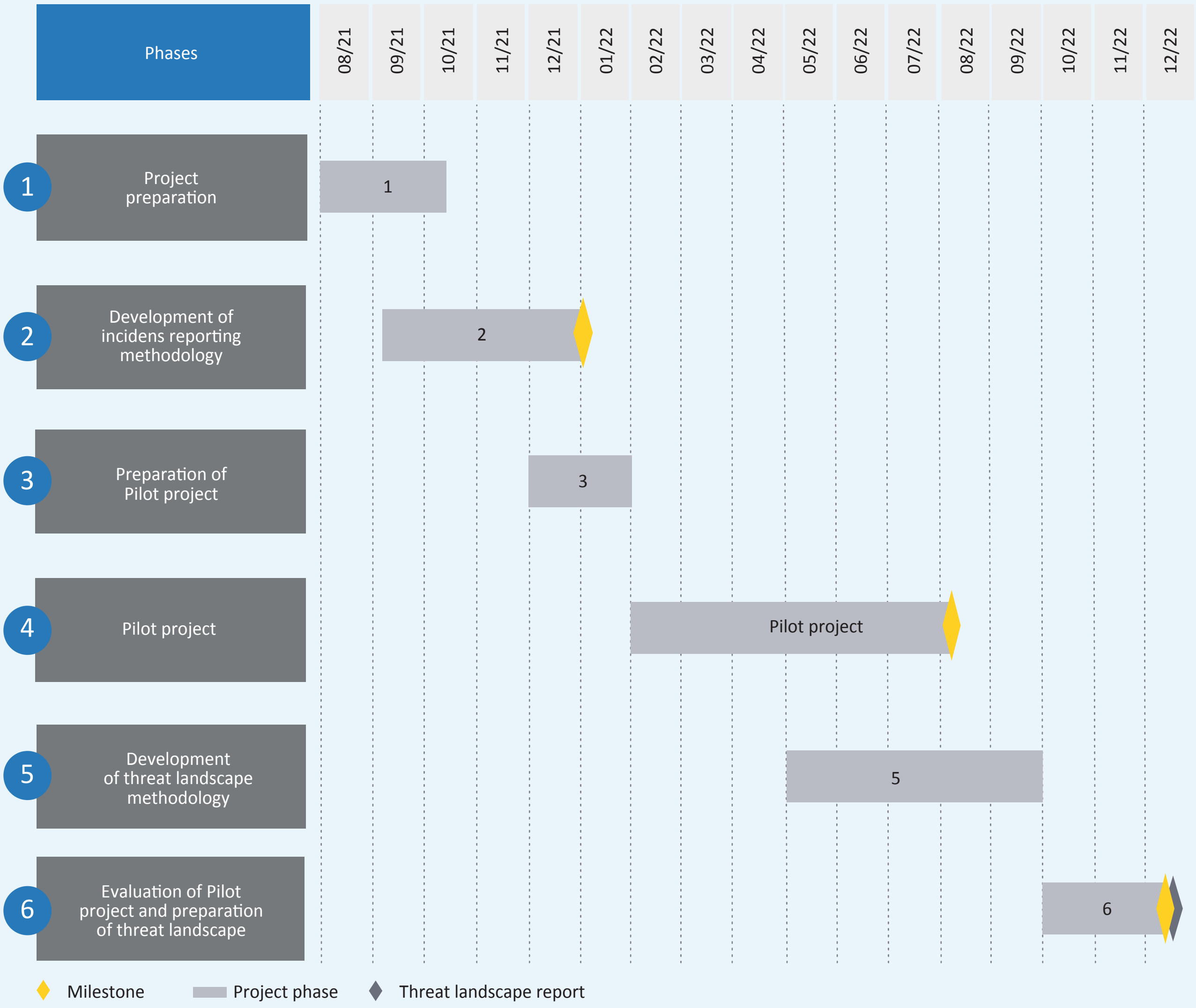
Unfortunately, currently only partial information on attacks, incidents and major threats to the financial sector in Hungary is available to stakeholders, as there is currently no comprehensive mandatory incident reporting obligation for all institutions (neither by the CBH, nor by the National Cyber Security Center of the Special Service for National Security (hereinafter: SSNS-NCSC) operating the Computer Security and Incident Management Group (hereinafter: SSNS-NCSC CSIRT), which supports incident management in the financial sector).

Considering existing and emerging EU and national legislative requirements and international best practices, the CBH aims to develop a methodology that provides an adequate overview of cyber-attacks, incidents, and key threats to the financial sector. This allows the CBH to focus more on addressing significant threats with the instruments at its disposal. An overview of the main cyber risks and threats in general and the identification of sector specific trends can support the formulation of institution level risk management action plans to help market participants respond more efficiently to events in cyberspace.

To achieve the above objective, the CBH decided to prepare a cyber threat landscape of the financial sector, which was supported by the Technical Assistance Instrument for 2021 programme of the Commission's Directorate-General for Structural Reform Support (DG REFORM). Following the Commission's decision, the Hungarian office of Ernst & Young Consulting Ltd. assisted the CBH in the implementation of the project. The project started in September 2021, with an assessment of national incident reporting obligations in the financial sector and an international outlook. During the three-month preparatory phase, several European authorities were consulted. Based on these experiences, it was concluded that the planned sectoral cyber threat landscape will require the development of a fundamentally new incident reporting framework. The preliminary information requirements were defined taking into consideration a number of existing and planned reporting frameworks, leveraging on international experience and best practices. Subsequently, the CBH developed a new, broader incident reporting framework, which was tested in a pilot project (hereinafter: Pilot).

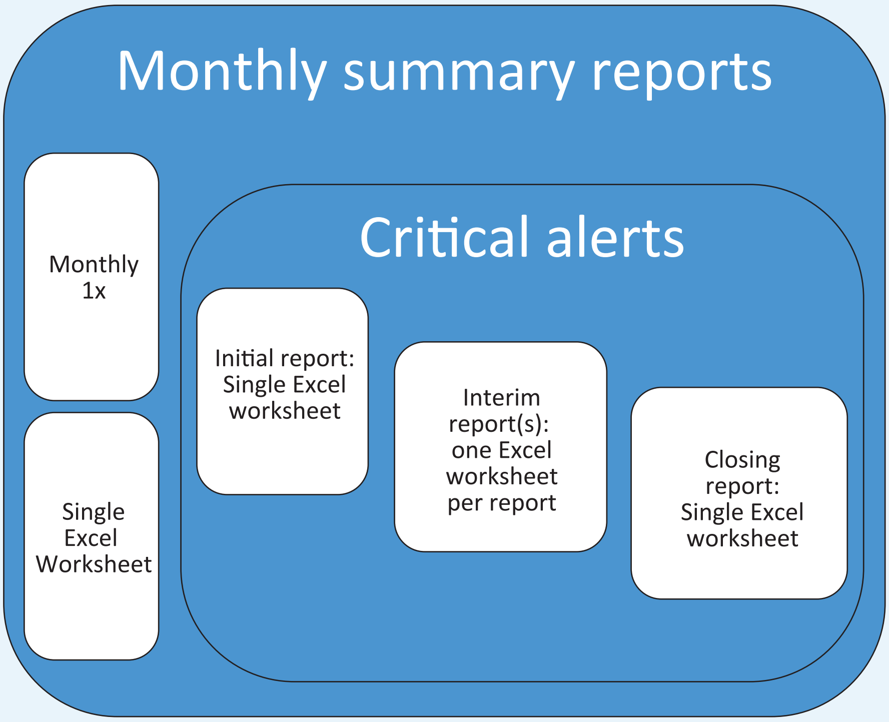
An important aim of the Pilot Project was to enable the widest possible range of institutions to join the programme. The aim was also to collect, organise and analyse as much formalised data as possible. Therefore, a six-month pilot period (1th February 2022 – 31th July 2022) was defined, during which the institutions participating in the Pilot Project informed the CBH of their incidents with all the details according to the newly developed methodology. The Pilot Project was joined on a voluntary basis by 39 institutions providing various financial services. Five banks, twelve insurance undertakings, financial markets infrastructures, investment companies, fund managers, insurance brokers and funds participated in the Pilot Project. The 39 institutions signed an agreement with the CBH at executive level, then their experts received methodological training on the incident reporting process.

Figure 1
Project plan of the CBH's "Cyber Threat Landscape" publication



The institutions that joined the Pilot Project undertook two types of reporting tasks, using bespoke reporting forms: on the one hand, they sent monthly reports summarising all critical and non-critical incidents that occurred during the month, and on the other hand, in addition to the monthly reports, they sent immediate, detailed alerts on critical incidents. This incident reporting framework, which included the specially developed reporting forms, enabled the data-driven conclusions that form the main part of this publication.

Figure 2
Types of reports and their components


Monthly summary reports
Monthly 1x
Single Excel Worksheet
Critical alerts
Initial report: Single Excel worksheet
Interim report(s): one Excel worksheet per report
Closing report: Single Excel worksheet

Institutions were required to communicate in their monthly reports any IT security incident that, as a result of an unforeseen event, had an adverse impact on their IT network or information systems and the data stored within or processed by them. Furthermore, a number of incidents may be considered critical on the basis of the criteria developed by the CBH (involvement of systems supporting critical functions, disclosure of customer data or financial sector secrets such as bank or securities secrets), and these incidents had more detailed reporting requirements. Critical incidents were subject to three levels of reporting: the initial report, the interim report, and the final report. The following incidents were to be considered critical in all cases:

- events that attract the attention of the press,
- unauthorised access to personal data of multiple customers involving bank secrets, payment secrets, insurance secrets, securities secrets, or fund secrets (e.g., data leakage, successful phishing),
- unauthorised activity in the IT system (e.g., external or internal fraud) resulting in data modification involving multiple customers,
- services considered critical based on the institution's Business Impact Analysis (BIA), that are expected to be down for more than 1 hour or below normal service levels, with a specific focus on:
  - electronic channels (online sales channels, payment cards, Internet banking and electronic payments),
  - account management in the case of credit institutions, investment companies and investment funds.

The explicit aim of the project was that the results of the analysis of the data collected and processed through the new structure and wider incident reporting would provide a more accurate picture of threat areas and trends, where sufficient data was not available in the previous period. Another objective was to test the new form of the reporting process in a live environment. This will provide valuable practical "field experience" to support future efforts and initiatives to improve incident reporting systems and processes. During the Pilot Project, the participating institutions reported incidents in the new structure and on a broad scale. With the end of the Pilot Project, the next phase of the "Cyber Threat Landscape" publication project was the development of this report.

III General overview

In 2020, the COVID-19 pandemic strengthened the acceleration the digitalisation of the financial sector as well worldwide. The transformation processes continued to intensify in 2021, as the lockdowns imposed by the authorities and the uncertainty that hampered business processes encouraged financial service providers to be flexible and innovative. Pandemic-related cyber security threats and attempts to exploit the "new normal" became common. Nevertheless, as the CBH's FinTech and Digitalisation Report points out, in 2021 payment processes in many respects returned to the pre-pandemic tracks, and although COVID-19 continued to be present in everyday life, payment service providers[1] learned to manage the aftermath of the pandemic situation in their processes.[2] It is fair to say that all financial service providers behaved in a similar way to payment service providers, i.e., they started to return to their familiar pre-pandemic processes after the pandemic. Of all payment service providers, bank payment service providers are the most numerous, and the digitalisation behaviour of bank payment service providers can therefore forcast the adaptation processes of the entire financial sector.

1 GENERAL THREAT TRENDS

Table 1
ENISA top threats for 2021

Rank	Threats	Trend
1	Ransomware	↑
2	Malware	↓
3	Cryptojacking	↑
4	E-mail-related threats	↑
5	Threats against data	↑
6	Threats to availability and integrity	↑
7	Disinformation – misinformation	↑
8	Non-malicious threats	↑
9	Supply chain attacks	↑

The main objective of the ENISA Threat Landscape (hereinafter: ETL) prepared by the European Union Agency for Cybersecurity (hereinafter: ENISA) is to present the cybersecurity environment for the reference year. The ETL identifies the primary threats, the main trends observed in relation to threats, attackers, and attack techniques. The ETL has limited information and data on trends and events affecting the financial sector in the past, presenting general (non-sector-specific and non-comprehensive) threat analyses.

According to previous ENISA ETL publications[3], the most common threats in 2017, 2018 and 2020 were malware attacks, web-based attacks, and attacks against web applications. The well-known Distributed Denial of Service (DDoS) and phishing attacks were among the six most common threats. The ETL was not published in 2019, but the data was included in next year's report.

The ETL for 2021 took into account the threat information originated between April 2020 and July 2021, during which the ENISA ETL working group identified nine main threats (Figure 1). The first on the list in 2021 is the category of

[1] Under the current legislation, among the institutions relevant for the threat landscape, payment service providers include banks, payment institutions and electronic money institutions.

[2] MNB – FinTech and Digitalisation Report, June 2022 (https://www.mnb.hu/letoltes/mnb-fintech-and-digitalisation-report-2022-final.pdf)

[3] ENISA Threat Landscape through the years (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape) and ENISA Threat Landscape 2021 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021)

ransomware, considered the top threat of the year by the ETL. A new item on the top list is supply chain attacks, which ENISA considers to be of particular importance for 2021. The reason given is that external service providers represent extremely valuable targets for cybercriminals. ENISA also analysed this threat in a separate report[4], further underlining its importance. According to ENISA, the key cybersecurity risks of the coming years will be in supply chains – a prediction that has been proven correct, as this threat is among the top priorities in next year's ETL.

The ENISA Threat Landscape for 2022[5] builds on threat information originated between July 2021 and July 2022 to analyse global and European threat trends. According to the 2022 edition, ransomware and malware continued to be the most prevalent threats (Table 2), but new in 2022, social engineering threats were now ranked 3rd.

Table 2
ENISA top threats for 2022

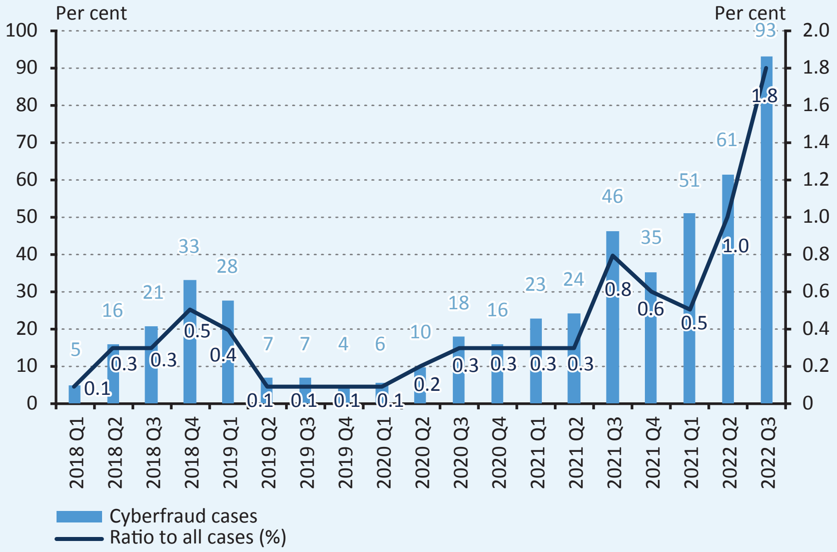
Rank	Threats	Trend
1	Ransomware	→
2	Malware	→
3	Social engineering	↑
4	Threats against data	↑
5	Threats against availability: DDoS	↑
6	Threats against availability: Internet threats	→
7	Disinformation - misinformation	→
8	Supply chain attacks	↑

Regarding the evolution of threat trends, ENISA highlights for the reporting period that attackers continue to carry out their attacks in an increasingly sophisticated and targeted manner. Increasingly, critical infrastructures are being attacked or affected and artificial intelligence is being used. Government agencies have therefore enhanced their role, cooperation, and protection capacities at national and international level.

Cybercriminals are often motivated by the goal of monetising their activities, for example by using ransomware. In 2018, when so-called cryptocurrencies (e.g., BTC, ETH) started to spread worldwide, a new threat emerged, cryptojacking, i.e., the unauthorised mining of cryptocurrencies using other people's IT devices. In 2018, it was already ranked 13th on the list of the top 15 threats, and in 2020 it was ranked 15th. Cryptocurrency continues to be the most common payment method for cybercriminals, reaching a record high of attacks in 2021 and ranking 3rd in the top threat list, but it is no longer on the top list in 2022. With successful attacks gaining media attention and the proliferation of Ransomware-as-a-Service (RaaS), the monthly value of attacks nearly doubled by June 2021 and this growth trend remains unbroken in 2022. Several factors could be behind the sudden surge in ransomware attacks. A particular risk is that malicious code components are relatively easy to access and purchase, so the technical barrier to entry for cybercrime has been greatly reduced in recent years. Examples include ransomware, denial of service, phishing, and misinformation services. Criminals without high technical skills may successfully attack individuals or even institutions. Two out of three ransomware attacks use "ransomware as a service".

[4] Threat Landscape for Supply Chain Attacks (https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks)
[5] ENISA Threat Landscape 2022 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022)

Figure 3
Evolution of the number of cyber fraud reports at the CBH customer relations information center



Cyber fraud (Figure 3), phishing and social engineering threats are on the rise, and fraudsters are using increasingly sophisticated solutions to hide their attempts. Attacks have become more credible, abuses have become better adapted to the context of the different channels of perpetration, and the number of phishing attacks reported in a given month tripled between the beginning of 2020 and the end of 2021, with phishing being the most common attack vector – also as a starting point for other types of attacks – according to the ETL 2022. Attackers often take advantage of the fact that users are by now tired of increased remote working (user fatigue). The targets are often members of the financial sector or their customers.[6] The CBH's experience of cyber abuse incidents (Figure 19) shows that, by the first half of 2022, the most common form of attack have been the fake bank phone calls, in other words, voice phishing attacks. This is in line with the experience of the SSNS-NCSC concerning financial institutions providing essential services (Figure 3). Thus the 19 incidents identified during the Pilot Project include advanced phishing attacks of the masquerade type. COVID-19 continues to be a predominant theme in phishing attack campaigns, and business e-mail compromise (BEC) and CEO fraud (i.e., abuse of executive or business e-mail addresses) have also increased in number, sophistication, and scope during 2021 and 2022. These abuses involve using fake supplier or management messages to induce the victim to transfer large sums of money to the accounts provided by the criminals.[7]

[6] APWG – Phishing Activity Trends Report 1st Quarter 2021. (https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf?_ga=2.100477661.234220476.1663894927-96135508.1660773867&_gl=1*1sfq8wd*_ga*OTYxMzU1MDguMTY2MDc3Mzg2Nw..*_ga_55RF0R-HXSR*MTY2Mzg5NDkyNy4yLjAuMTY2Mzg5NDkyNy4wLjAuMA..)

[7] See, e.g., the article on false management instructions by e-mail or telephone on the "Pénzügyi Navigátor" (Financial Navigator) site of the CBH (https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/hamis-vezetoi-utasitas-e-mail-ben-vagy-telefonon).

Table 3
Incidents observed by the SSNS-NCSC concerning financial institutions providing essential services, 1 February – 31 July 2022

Threats	Number of incidents
DDoS	3
DoS	1
Information security	1
Information gathering	9
Malicious code of unknown origin	3
Masquerade	1
SPAM	3

According to the 2021 report, a decrease in the use of malware was already observed in 2020. This trend continued in 2021, but at the same time there was a significant improvement in the sophistication of malicious code. Traditional DDoS campaigns have also become more targeted and persistent in 2021, affecting an increasingly broad area. In line with international trends, Hungary was also hit by the first relatively significant, newsworthy DDoS attack wave at the end of 2020. Interestingly, in 2020 and 2021, there was a strong increase in incidents attributable to non-malicious root causes.

Intsights LLC. (hereinafter: Intsights) regularly produces a threat landscape analysis and report (Banking & Financial Services Cyber Threat Landscape Report) for the financial sector, summarising the most common types of attacks. According to their report analysing 2018 data, 25.7 percent of all malware attacks of that year targeted banking and financial services (Intsights, 2019[8]) and this trend is continually increasing. This poses a serious risk to the financial sector, as the most common threats at EU level (according to ENISA reports issued in previous years) were malware attacks.

According to the Intsights 2019 threat report, the number of incidents related to the leakage of user credentials (username, password) increased by 129 percent on an annual basis, while incidents related to stolen credit card data increased by 212 percent and the number of mobile banking attacks using malicious apps increased by 102 percent.

Intsights' next threat report (2021)[9] revealed the most common attack vectors used by cyber attackers. According to the report, successful cyber-attacks on banking and financial services institutions provide evidence that hackers are increasingly collaborating to carry out attacks. Intsights' experience showed that the most significant threats to the banking and financial sector in 2020 and 2021 were attacks against compromised credit cards and banking networks, carried out by attackers using, among others, Trojan viruses. In line with the ENISA publication, the report identified an increasing number of attacks against third parties operating in other industries, which indirectly threaten the financial sector.

[8] Intsights – Banking & Financial Services Cyber Threat Landscape Report (April 2019) (https://intsights.com/resources/banking-financial-services-cyber-threat-landscape-report-april-2019)

[9] Insights – Banking and Financial Services Industry Cyber Threat Landscape Report 2021 (https://intsights.com/resources/2021-banking-and-financial-services-industry-cyber-threat-landscape-report)

Ongoing cyber threats are increasingly part of the way the financial sector operates. The spread of the use of digital channels for various services, accelerated by the COVID-19 pandemic, has significantly increased the exposure of institutions and customers in the financial sector. As users of digital financial services, customers can easily find themselves in the focus of cyber threats. Increasingly sophisticated malicious attacks seek to exploit this increased attack surface for profit, both from the institutional and the customer side. National and international regulatory efforts are concentrated on countering these risks, and the threat landscape is changing every year as security controls continue to evolve.

2 INTERNATIONALLY IDENTIFIED ATTACK GROUPS

Nation-state sponsored actors (intelligence, hacker groups, collectives) were already the biggest cyber risk actors in 2021, according to the ENISA threat landscape. In addition to pandemic related intelligence activities (such as attacks on pharmaceutical manufacturers or the World Health Organization), the largest supply chain attacks are believed to have been carried out by nation-state sponsored actors. According to ENISA data, different APT (Advanced Persistent Threat) groups were responsible for more than half of the supply chain attacks that occurred between 2020 and 2021. The activities of these actors in cyberspace are shaped by state strategies, geopolitical realities and last but not least, armed conflicts.

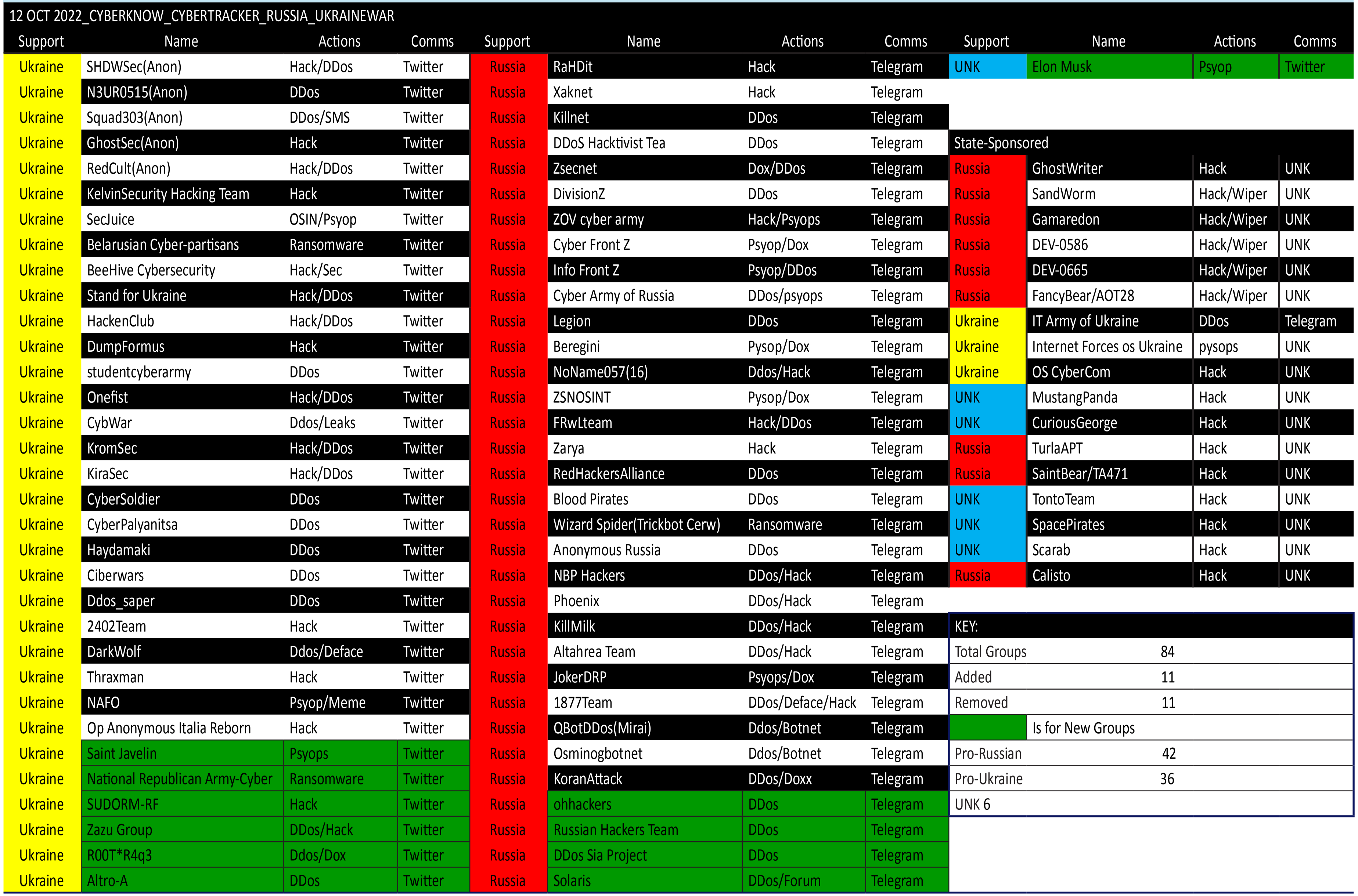
One of the defining events of 2022 is the Russian-Ukrainian war that broke out on 24 February, which has also led to significant changes in cyberspace. Cyberspace can be considered the fifth operational domain of war[10]; and in addition to physical conflict, there have been significant war-related attacks and disinformation operations in cyberspace, while new defence mechanisms such as the so-called “hunt forward”[11] used by the United States of America have also emerged. While a significant number of hacker groups (including criminal groups) have taken sides in the war and are/have been admittedly assisting the Russian or Ukrainian sides, there has been a shift in the past months, with some groups leaving the conflict or disappearing completely, while new actors have emerged, according to data from the Cyberknow portal[12] (Figure 4).

[10] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017. (https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9)

[11] BBC: Inside a US military cyber team’s defence of Ukraine (https://www.bbc.com/news/uk-63328398)

[12] https://twitter.com/Cyberknow20

Figure 4
Pro-Russian and pro-Ukrainian hacker groups according to data from the Cyberknow portal, as of 12 October 2022

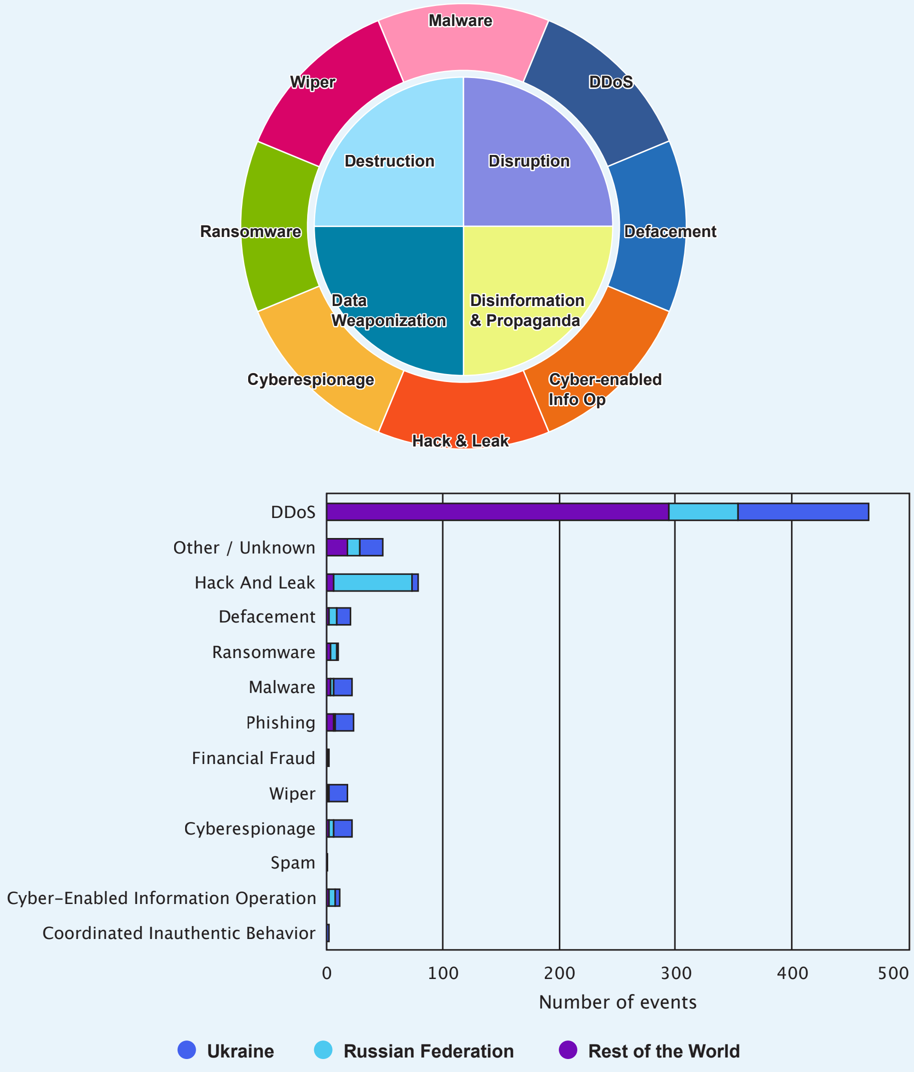


12 OCT 2022_CYBERKNOW_CYBERTRACKER_RUSSIA_UKRAINEWAR

Support	Name	Actions	Comms	Support	Name	Actions	Comms	Support	Name	Actions	Comms
Ukraine	SHDWSec(Anon)	Hack/DDos	Twitter	Russia	RaHDit	Hack	Telegram	UNK	Elon Musk	Psyop	Twitter
Ukraine	N3UR0515(Anon)	DDos	Twitter	Russia	Xaknet	Hack	Telegram				
Ukraine	Squad303(Anon)	DDos/SMS	Twitter	Russia	Killnet	DDos	Telegram				
Ukraine	GhostSec(Anon)	Hack	Twitter	Russia	DDoS Hacktivist Tea	DDos	Telegram	State-Sponsored			
Ukraine	RedCult(Anon)	Hack/DDos	Twitter	Russia	Zsecnet	Dox/DDos	Telegram	Russia	GhostWriter	Hack	UNK
Ukraine	KelvinSecurity Hacking Team	Hack	Twitter	Russia	DivisionZ	DDos	Telegram	Russia	SandWorm	Hack/Wiper	UNK
Ukraine	SecJuice	OSIN/Psyop	Twitter	Russia	ZOV cyber army	Hack/Psyops	Telegram	Russia	Gamaredon	Hack/Wiper	UNK
Ukraine	Belarusian Cyber-partisans	Ransomware	Twitter	Russia	Cyber Front Z	Psyop/Dox	Telegram	Russia	DEV-0586	Hack/Wiper	UNK
Ukraine	BeeHive Cybersecurity	Hack/Sec	Twitter	Russia	Info Front Z	Psyop/DDos	Telegram	Russia	DEV-0665	Hack/Wiper	UNK
Ukraine	Stand for Ukraine	Hack/DDos	Twitter	Russia	Cyber Army of Russia	DDos/psyops	Telegram	Russia	FancyBear/AOT28	Hack/Wiper	UNK
Ukraine	HackenClub	Hack/DDos	Twitter	Russia	Legion	DDos	Telegram	Ukraine	IT Army of Ukraine	DDos	Telegram
Ukraine	DumpFormus	Hack	Twitter	Russia	Beregini	Pysop/Dox	Telegram	Ukraine	Internet Forces os Ukraine	pysops	UNK
Ukraine	studentcyberarmy	DDos	Twitter	Russia	NoName057(16)	Ddos/Hack	Telegram	Ukraine	OS CyberCom	Hack	UNK
Ukraine	Onefist	Hack/DDos	Twitter	Russia	ZSNOSINT	Pysop/Dox	Telegram	UNK	MustangPanda	Hack	UNK
Ukraine	CybWar	Ddos/Leaks	Twitter	Russia	FRwLteam	Hack/DDos	Telegram	UNK	CuriousGeorge	Hack	UNK
Ukraine	KromSec	Hack/DDos	Twitter	Russia	Zarya	Hack	Telegram	Russia	TurlaAPT	Hack	UNK
Ukraine	KiraSec	Hack/DDos	Twitter	Russia	RedHackersAlliance	DDos	Telegram	Russia	SaintBear/TA471	Hack	UNK
Ukraine	CyberSoldier	DDos	Twitter	Russia	Blood Pirates	DDos	Telegram	UNK	TontoTeam	Hack	UNK
Ukraine	CyberPalyanitsa	DDos	Twitter	Russia	Wizard Spider(Trickbot Cerw)	Ransomware	Telegram	UNK	SpacePirates	Hack	UNK
Ukraine	Haydamaki	DDos	Twitter	Russia	Anonymous Russia	DDos	Telegram	UNK	Scarab	Hack	UNK
Ukraine	Ciberwars	DDos	Twitter	Russia	NBP Hackers	DDos/Hack	Telegram	Russia	Calisto	Hack	UNK
Ukraine	Ddos_saper	DDos	Twitter	Russia	Phoenix	DDos/Hack	Telegram				
Ukraine	2402Team	Hack	Twitter	Russia	KillMilk	DDos/Hack	Telegram	KEY:			
Ukraine	DarkWolf	Ddos/Deface	Twitter	Russia	Altahrea Team	DDos/Hack	Telegram	Total Groups	84		
Ukraine	Thraxman	Hack	Twitter	Russia	JokerDRP	Psyops/Dox	Telegram	Added	11		
Ukraine	NAFO	Psyop/Meme	Twitter	Russia	1877Team	DDos/Deface/Hack	Telegram	Removed	11		
Ukraine	Op Anonymous Italia Reborn	Hack	Twitter	Russia	QBotDDos(Mirai)	Ddos/Botnet	Telegram	🟩	Is for New Groups		
Ukraine	Saint Javelin	Psyops	Twitter	Russia	Osminogbotnet	Ddos/Botnet	Telegram	Pro-Russian	42		
Ukraine	National Republican Army-Cyber	Ransomware	Twitter	Russia	KoranAttack	DDos/Doxx	Telegram	Pro-Ukraine	36		
Ukraine	SUDORM-RF	Hack	Twitter	Russia	ohhackers	DDos	Telegram	UNK 6			
Ukraine	Zazu Group	DDos/Hack	Twitter	Russia	Russian Hackers Team	DDos	Telegram				
Ukraine	R00T*R4q3	Ddos/Dox	Twitter	Russia	DDos Sia Project	DDos	Telegram				
Ukraine	Altro-A	DDos	Twitter	Russia	Solaris	DDos/Forum	Telegram				

In the context of the Russian-Ukrainian war, the key question for 2022 is how the events of the Russian-Ukrainian war in cyberspace will affect the cybersecurity of different sectors; what consequences and possible attacks can be expected by the members of different sectors in the countries at war and worldwide. By analysing the events, as of 18th October 2022, the CyberPeace Institute[13] has identified 564 cyberattacks (an average of 13.8 per week), with 61 different perpetrators. DDoS predominates among the attack types (Figure 5), but presumably most attacks aimed at data theft or interception are not disclosed.

Figure 5
Threats and attacks observed in the context of the Russia-Ukraine war



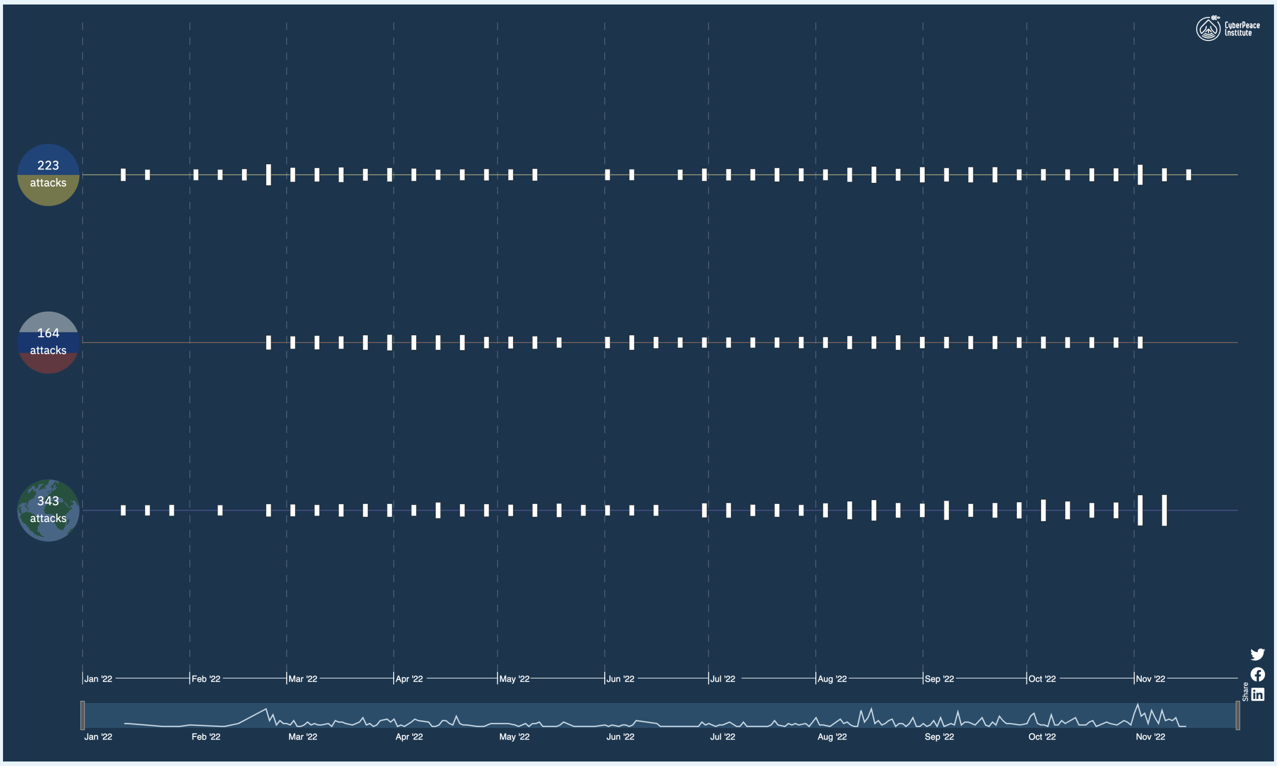
Source: https://cyberconflicts.cyberpeaceinstitute.org/threats

The start of the war in physical space prominently coincides with the increased activity in cyberspace (Figure 6). However, the analyses also show that it is not primarily the financial sector that has been targeted, neither on the Russian nor on the Ukrainian side (Figure 7), as also confirmed by the ETL 2022 data. At the European level, most supervisory authorities have also called for increased vigilance, but only relatively few institutions have suffered an actual cyberattack as a result of the war; moreover, apparently the number of other attacks in the financial sector has decreased as well. The reason

[13] https://cyberconflicts.cyberpeaceinstitute.org/

for this is difficult to establish without doubt, but the analysis of the activity of the various hacker groups suggests that the voluntary involvement in the war by groups specialising in cybercrime was a major drain on their resources, especially in the first weeks of the war.

Figure 6
Timeline distribution of cyber-attacks related to the Russia-Ukraine war by targets for all sectors



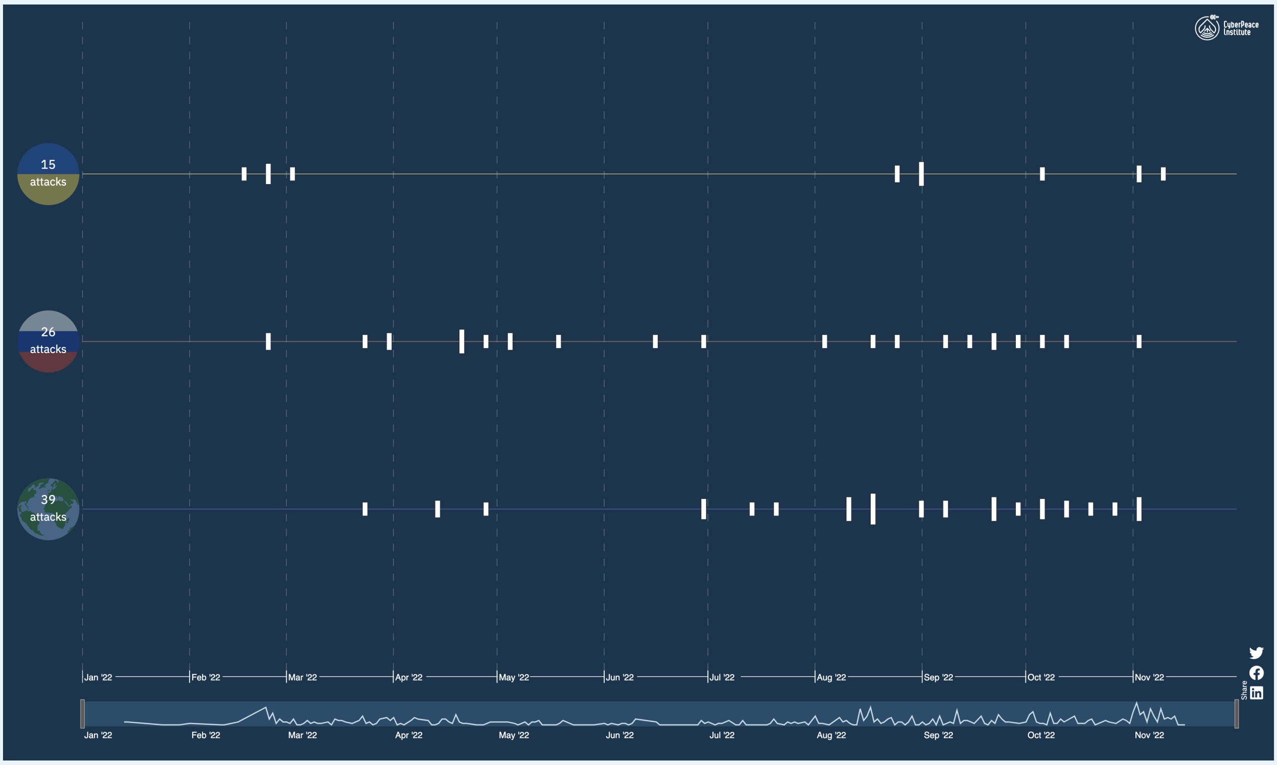
Source: https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

Understanding trends related to cybercriminal actors and their motivations and targets greatly assists the planning in developing cybersecurity defence and risk mitigation strategies. The ENISA threat landscape identified the following cybersecurity threats:

- state-sponsored actors,
- cybercrime actors,
- hacker-for-hire actors,
- hacktivists.

Data from both CyberKnow and CyberPeace Institute show that both the largest pro-Ukraine and pro-Russia cyberspace actors fall into the category of hacker collectives and actors presumably sponsored by nation-states. This makes it likely that their activities – at least in relation to the war – are not motivated by material gain, and this may be the reason why financial institutions are not their primary targets.

Figure 7
Timeline distribution of cyber-attacks related to the Russia-Ukraine war by targets in the financial sector



Source: https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

The international outlook and the review other available statistics, as well as an assessment of the main political and geopolitical developments over the period covered by the report and the identification of actors is an integral part of the threat assessment, as it allows the contextualisation of the trends identified in Hungary, the prioritisation security controls and the development of a dedicated strategy to prevent potential threats and impacts from occurring.

3 INTERNATIONAL REGULATORY INITIATIVES

The EU has also recognised the importance of intense digitalisation and the growing number and complexity of cybersecurity challenges it poses and responded by proposing a number of legislative measures and initiating the review and modernisation of several previous EU requirements.

On 24 September 2020, the Commission presented its Digital Finance Package (DFP) proposal, which includes a Digital Finance Strategy for the EU that facilitates innovation and competition, aims to strengthen consumer protection and reduce risks[14], a Retail Payments Strategy to create a fully integrated retail payments system at EU level, and three legislative proposals to support the implementation of the strategies and the objectives of the overall Digital Finance Package:

- Proposal for a regulation on markets in crypto-assets (MICA)[15]. The aim of MICA is to establish unified EU-wide requirements for the issuance of crypto-assets and the provision of services related to them, which are not yet covered by existing EU legal standards, and to mitigate, as far as possible, the risks for users of these crypto-assets.

[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU (https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0591&from=EN)

[15] Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937 (https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52020PC0593)

- Proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT).[16] The DLT pilot establishes a pilot regime for the issuance and clearing of blockchain-based financial instruments, including securities, for authorised securities settlement systems and multilateral trading facilities.

- Proposal for a regulation on digital operational resilience for the financial sector (DORA).[17] The main objectives of the DORA are to further enable and support the harnessing of the potential of digital financial services in terms of innovation and competition, while mitigating the risks and strengthening the digital resilience of the financial sector, and to harmonise and standardise the different supervisory practices currently existing in the Member States. In line with the above objectives, DORA defines a detailed set of requirements for information and communication technology (ICT) risk management, testing and the management of ICT third-party service providers of financial institutions. Furthermore, DORA creates a general incident reporting requirement and threat reporting opportunities for the regulated financial entities, which will enable national and European supervisory authorities to have a good overview of major incidents, major threat and incident trends within the financial sector.

The negotiation and early adoption of the DORA was made a priority by the forced and rapid digital transformation experienced during the COVID-19 pandemic and the many cybersecurity challenges because of the Russian-Ukrainian war this year.

Meanwhile, the review of the Network and Information Security Directive (NIS Directive), which also affects certain designated members (essential service providers) of the financial sector, has also started, and in May 2022, the Council of the European Union, the European Parliament, and the Commission agreed to amend the Network and Information Security Directive (NIS2 Directive). The aim of the legislators is to align the provisions of the NIS2 Directive with sector specific legislations, such as the DORA and the Critical Entities Resilience Directive (CER Directive), in order to create legal certainty and ensure coherence between the NIS2 Directive and other relevant legal acts.

Overall, EU legislators have also responded to the increased threats and emerging challenges of recent years, so in the coming years we will be able to increase the cybersecurity resilience of the financial sector by implementing these EU-level regulations and expectations, and we can get a more up-to-date and accurate picture of the current challenges and threats.

[16] Proposal for a regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology (https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52020PC0594)

[17] Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (https://eur-lex.europa.eu/legal-content/hu/TXT/PDF/?uri=COM:2020:595:FIN&rid=1)

IV Presentation of identified threat trends

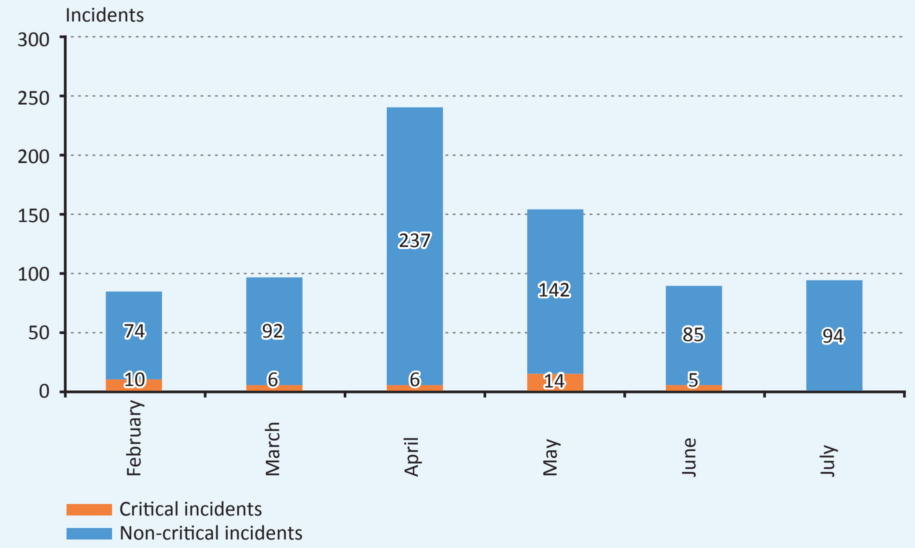
During the preparatory phase of the project creating the Cyber Threat Landscape Report, the data to be recorded and reported by institutions using the incident reporting form was defined. On the one hand the aim was to provide the respective institutions with the simplest possible data reporting process during the incident response, and therefore, particular attention was given to designing the data structure of the form to request only the most necessary data. At the same time, it was also important to ensure that the data provided would be sufficient for follow-up, processing and drawing conclusions for future learning.

The results of the analyses carried out on the data collected during the Pilot Project phase are presented in the following subsections. The incident data were supplemented with data from other sources, such as data supplied by the CBH Customer Relations Information Centre and the regulatory reporting data with the identification code P58, as defined in CBH Decree 54/2021 (23.11.2011) on the obligations to report data to the central bank's information system primarily to enable the Central Bank of Hungary to carry out its fundamental duties. Separate subsections deal with the general analysis of the processed incident reports, the analysis of incident reports by type of institution, the in-depth analysis of reported incidents and the analysis of authority notification and external service provider involvement. The chapter ends with a summary of the conclusions on the threat trends identified from the analyses. Within each section, separate analysis was performed for the total incident population, which includes all reports (both critical and non-critical incidents). Where meaningful, separate analysis was carried out for the reported critical incident data. For ease of comparison, separate graphs represent the analyses for the total incident population and for the critical incident population carried out in the same area.

1 GENERAL ANALYSIS OF INCIDENT REPORTS

During the six-month data collection period of the Threat Landscape Report, the CBH received reports of a total of 765 incidents from the institutions participating in the project (Figure 8).

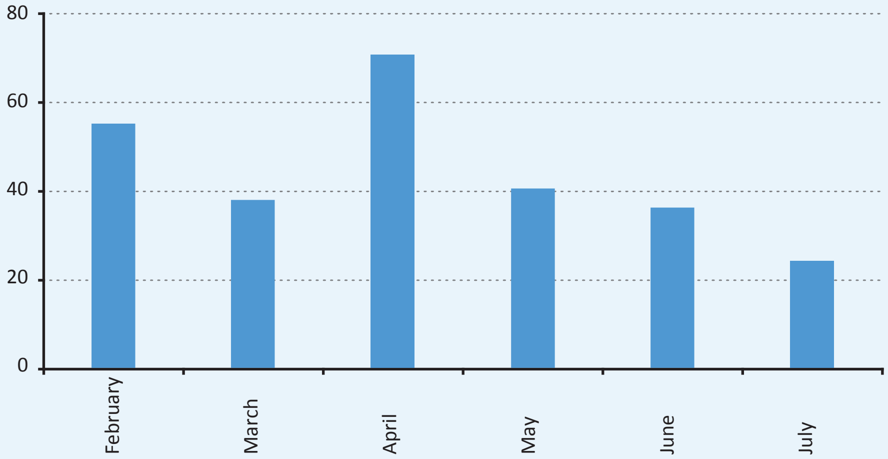
Figure 8
Number of incidents per month of reporting



An important objective of the analysis was to look at the spikes in April and May following the February and March introductory phase, where a significant increase in the number of reported incidents was identified. The subsequent period in June and July again saw fewer reports.

One possible explanation for the peak period, which was also identified as a risk during the project preparation, is a possible start-up phase, during which the new incident reporting process is introduced and formalised as an internal routine by the participating institutions. However, the analysis of the raw data revealed that such increased incident reporting activities, resulting in the April and May incident numbers, can only be attributed to a few institutions.

Figure 9
Monthly distribution of payment service disruptions (based on CBH regulatory reporting P58)

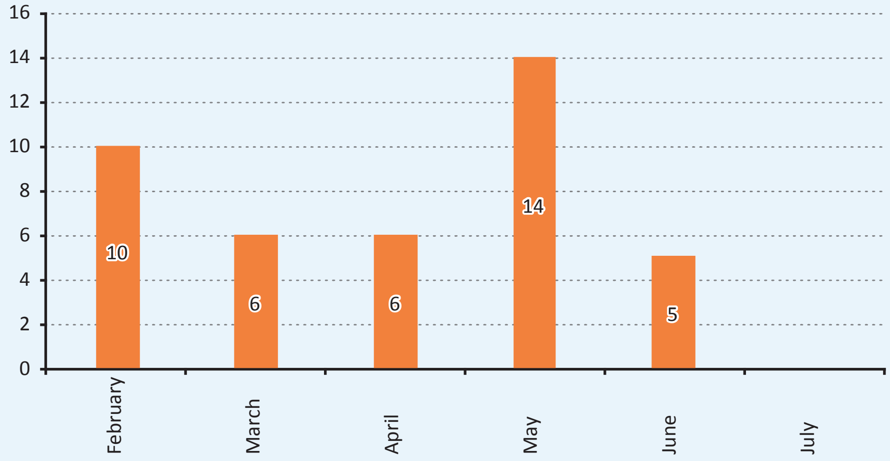


As to the lower number of events in the months of June and July, it may be assumed that the summer and holiday season have reduced the number of development and major software upgrade tasks, which were rather scheduled for the autumn months. This hypothesis is also supported by the monthly distribution of the data reported under the Incident Reporting on Payment Service Disruption P58 (Figure 9), which shows a similar pattern to the incident reports. Excluding the outliers in April and May from the statistics, the average number of monthly reports was not significantly affected by the summer period. Overall, it may be concluded that during the first two months of the start-up phase, reporting did not cause any apparent difficulties for the institutions participating in the Pilot Project.

The comparison of the proportion of critical incidents to the total population of reported incidents shows that the overall proportion of critical incidents was below four percent.

The pattern of the number of critical incidents matches the aggregated monthly reporting results. A stable monthly average number of reports may also be observed for critical incidents during the Pilot Project (Figure 10).

Figure 10
Number of incidents per month of reporting (for critical incidents)



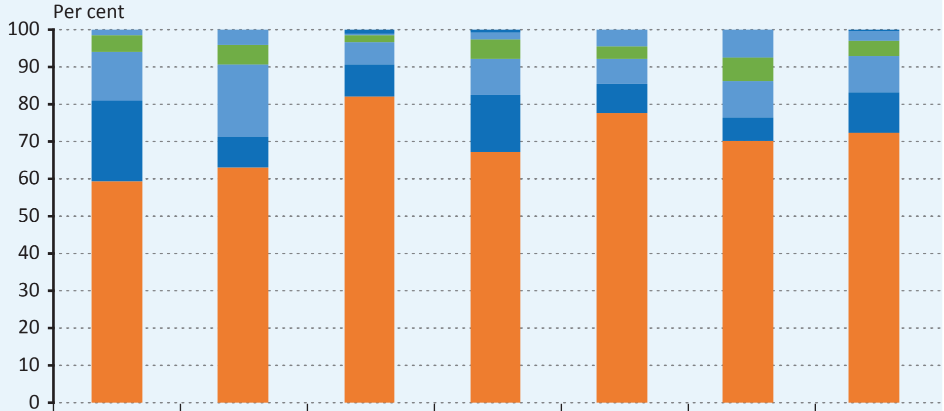
An outstanding number of incidents were reported in May, no critical incidents were reported in July, and in the other months there were between six and ten critical incidents reported, which can be considered typical. The significantly different number of critical incidents reported in May, which is similar in tendency to the aggregated statistics including both critical and non-critical incidents, may be traced to an increased number of reports for some specific institutions after the data analysis. The other significant difference is the closing figure for July, with no critical incidents reported in this month. This is probably due to lower system development activities during the summer period.

Overall, a similar pattern is observed in the total incident reporting population and in the critical incident statistics over the Pilot period. A stable monthly number of reports in a well identifiable range is clearly visible, with slightly lower summer values, which initial observations may be confirmed, supplemented, or corrected by data analysis in subsequent years.

2 ANALYSIS OF INCIDENT REPORTS BY TYPE OF INSTITUTION

The monthly aggregation of incident reports (Figure 11) shows that banks reported an outstanding number of incidents, reaching 72 percent of the total number of incidents reported by all types of institutions over the entire six-month period of the Threat Landscape Report. This is especially prominent in view of the fact that banks represented only 12 percent of all the institutions participating in the Pilot Project.

Figure 11
Incident reports by type of institution per month

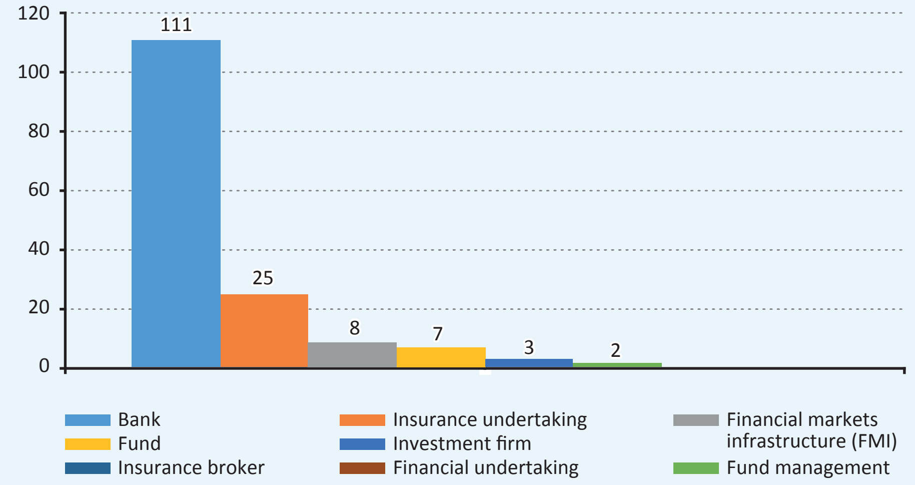


	February	March	April	May	June	July	Total
🟧 Bank	50	62	200	105	70	66	553
🟦 Insurance undertaking	18	8	21	24	7	6	84
🟦 Financial markets infrastructure (FMI)	11	19	14	15	6	9	74
🟩 Fund	4	5	5	8	3	6	31
🟦 Investment firm	1	4	1	3	4	7	20
🟦 Fund management	0	0	2	1	0	0	3
🟦 Insurance broker	0	0	0	0	0	0	0
🟫 Financial undertaking	0	0	0	0	0	0	0

In terms of institutions, the average number of incidents detected by banks was 110, while for the type of institution with the highest participation rate, i.e. funds, the number was only 2.82 (Figure 12). Next to banks, insurance undertakings and financial markets infrastructures were the ones reporting higher number of incidents.

Fewer incidents took place among fund managers, funds and investment firms, while insurance brokers and financial undertakings did not report any incidents during the period.

Figure 12
Average number of incidents by type of institution



For the institutions reporting fewer incidents mentioned above, there is no downward trend in the number of incidents for the summer months of June and July, but it should be noted that the institutions reporting fewer incidents also have fewer customers and less complex IT systems, so they have a smaller attack surface and a lower probability of failures in systems with fewer IT assets.

Based on the data, a further conclusion may be drawn from the first chart that the majority of reports were not hindered by the start-up period of the first two months. We deliberately speak of the majority of reports and not the majority of institutions, as it appears that the majority of reports were not impeded and as the majority of reports were mainly submitted by banks, it may be concluded that banks did not have any perceivable difficulties in implementing the reporting process, while for example for insurance brokers and financial undertakings the same cannot be declared. For the majority of reporting banks, the incident reporting process was already familiar, in most cases internal fine-tuning of the process was sufficient, and they were ready to provide information according to the procedure defined by the Pilot Project. This explains the result that, for the Pilot Project as a whole, there was no marked shortage in the number of reports in the first two months.

This observation is supported by the fact that banks participating in the Pilot Project currently also have a reporting obligation regarding payment services disruptions. Although the reporting frameworks of the Pilot Project and the reporting of major operational and security incidents under the Act on the Provision of Payment Services (hereinafter Pft.[18]) transposing the Directive on Payment Services in the Internal Market (hereinafter PSD2[19]) into domestic law differ to such an extent that no meaningful conclusions can be drawn from their comparison, it is nevertheless worthwhile to examine the number of significant incidents that adversely affect payment systems.

[18] Act LXXXV of 2009 on the Provision of Payment Services (Available: https://njt.hu/jogszabaly/2009-85-00-00)

[19] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC (Available at: https://eur-lex.europa.eu/legal-content/HU/TXT/? uri=celex%3A32015L2366)

Pursuant to PSD2, the Pft. requires payment service providers to notify the CBH without undue delay of any disruptions affecting payment transactions and payment services, which obligation the payment service providers can fulfil by reporting data under the regulatory reporting form P58. This incident reporting also covers events that are considered to be major operational and security incidents. These reports describe to incidents that are unplanned by the payment service provider and have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment systems.

Box 1
Banking 24/7: new rules for bank holidays

The amendment to the Act on Credit Institutions and Financial Undertakings[20], which entered into force on 1 July 2022, fundamentally changed the conditions for the suspension of credit institutional services. In contrast to the previous legislation, credit institutions may now suspend their services not only on working days (Monday to Friday) for five working days per year, but also on any calendar day, for any length of time, if they would otherwise have a working day for the service in question. The aim of the legislator in introducing the new rules was to support the digitalisation of credit institutions. In other words, to ensure that in all cases there is sufficient time for both the credit institution and its customers to prepare for any downtime, and that the maximum of five days of downtime per year is not a strict limitation to any potential IT developments.

Under the new rules, if a credit institution has a planned shutdown of any financial or ancillary financial service or any part of its activities when it should be providing that service under the relevant legislation or contracts, it will have to announce a banking holiday in respect of the planned shutdown. Therefore, a bank holiday may be an outage of a shorter duration, during which only a part of the service is unavailable (e.g. a 15-minute downtime during which only the credit scoring within the overall lending process is interrupted).

It is important to note that the downtime must be planned, i.e. a service outage due to an incident and its subsequent recovery does not constitute a banking holiday. A good example would be instant payments, where the legislation[21] requires credit institutions to observe a business day from 0-24 hours, seven days a week. Therefore, any planned service outage for instant payments can only take place during a bank holiday. However, if a particular service is not provided by a credit institution at the weekend but only on a weekday (e.g. if a deposit can only be placed with a credit institution between 8 a.m. and 5 p.m. from Monday to Friday), a planned outage of that service (or part of the service) can only be a bank holiday if it takes place on a contractually agreed working day (e.g. based on the previous example, a planned outage on a Wednesday between 12 and 13 hours may be executed during a bank holiday, whereas a planned outage on a Saturday or Sunday does not need to follow the rules of a bank holiday).

As a guarantee rule, a credit institution must inform its customers directly (e.g. by push message) 30 days in advance of the bank holiday and must also report to the CBH. The CBH may still impose a bank holiday as an exceptional measure, i.e. order a credit institution to shut down its service or services. In order to support the interpretation of the law, the CBH also published an executive circular[22] on the subject on 5 October 2021 on its website. From 1 January 2023, the Act on Certain Payment Service Providers[23] will also be amended to allow payment service providers and electronic money institutions to have a bank holiday in the same way credit institutions do.

The incidents and disruptions processed during the preparation of the Cyber Threat Landscape Report are not covered by the bank holiday provisions, as all cases occurred in an unplanned manner.

[20] Act CCXXVII of 2013 on Credit Institutions and Financial Undertakings (Hpt.) (Available at: https://njt.hu/jogszabaly/2013-237-00-00)]

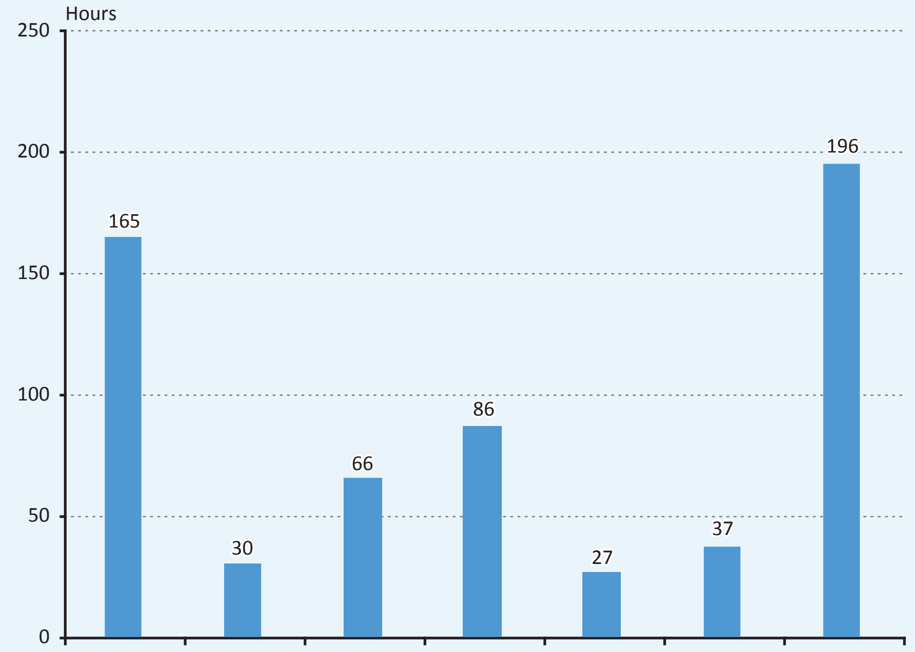
[21] Decree No. 35/2017 (14.12.2017) of the Governor of the Magyar Nemzeti Bank on the implementation of payments services (Available at: https://njt.hu/jogszabaly/2017-35-20-2C)

[22] Executive Circular on the interpretation of the concept of a working day in relation to a bank holiday in credit institutions (Available at: https://www.mnb.hu/letoltes/vezetoi-korlevel-bankszunnap-honlapra.pdf)

[23] Act CCXXXV of 2013 on Certain Payment Service Providers (Fszt.) (available at: https://njt.hu/jogszabaly/2013-235-00-00)]

Among the institutions in the Pilot Project, the banks that were required to report outages reported more than fifty disruptions to the CBH between February and August (the figure shows the data of the large banks). In fulfilling their reporting obligations, the banks accounted for almost one hundred and fifty hours of service outages (Figure 13).

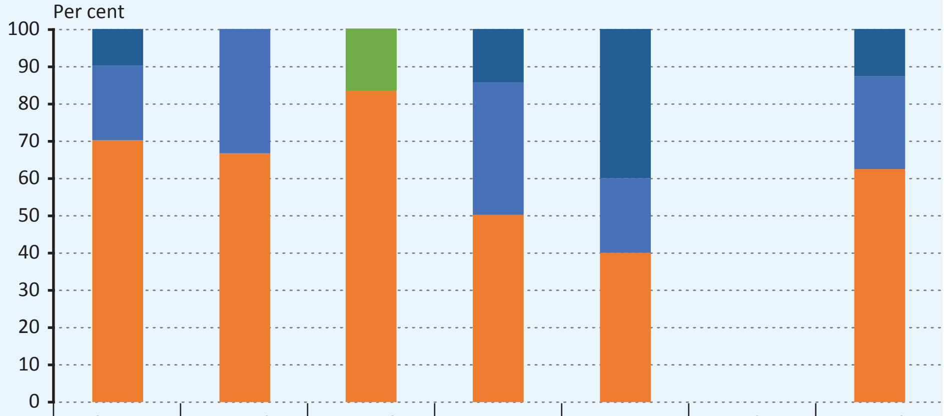
Figure 13
Outages affecting payment systems of large banks in Hungary during the period of the Pilot Project



A comparison of the reports received in the Pilot and the results of the CBH P58 regulatory reporting did not lead to any meaningful conclusions, but the detailed data showed less overlap between the two sets than expected. Payment service providers participating in the pilot (typically small and large banks) provided more detailed data on operational incidents affecting payment services within the pilot than in the regulatory reporting. One possible reason for this is that in the pilot there was a much tighter time frame (90 minutes for the initial report) for the report to be sent to the CBH, so the information was generally provided by IT security and/or business continuity specialists directly involved in the management of the incident, while the regulatory reporting, especially for larger organisations, is mostly handled by different competence areas.

When analysing critical incident data in the breakdown by type of institution, there is no significant difference compared to the total population, as banks reported the large majority of the incidents (Figure 14).

Figure 14
Incident reports by type of institution per month (for critical incidents)



	February	March	April	May	June	July	Total
🟦 Fund management	0	0	0	0	0	0	0
🟧 Bank	7	4	5	7	2	0	25
⬜ Investment firm	0	0	0	0	0	0	0
🟨 Insurance broker	0	0	0	0	0	0	0
🟦 Insurance undertaking	2	2	0	5	1	0	10
🟩 Fund	0	0	1	0	0	0	1
🟦 Financial markets infrastructure (FMI)	1	0	0	2	2	0	5
🟫 Financial undertaking	0	0	0	0	0	0	0

In addition to the type, size and complexity of institutions, an important factor in analysing incident reporting data for each type of institution may be the extent to which a particular type of institution is an attractive target for potential attackers. The related analysis will be discussed in depth in the next chapter, as it is primarily the content of the incidents that could yield additional information.

3 IN-DEPTH ANALYSIS OF REPORTED INCIDENTS

The most common causes of incidents are failures and malfunctions, followed by nefarious activities and abuse (Figure 15)

Figure 15
Distribution of root causes by main categories

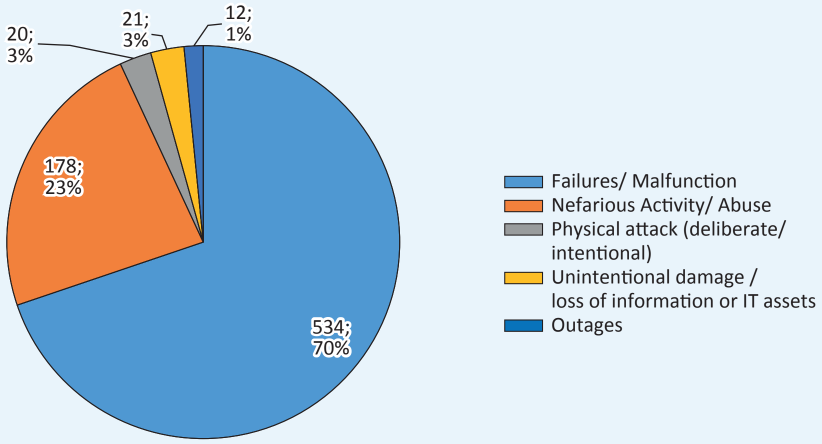
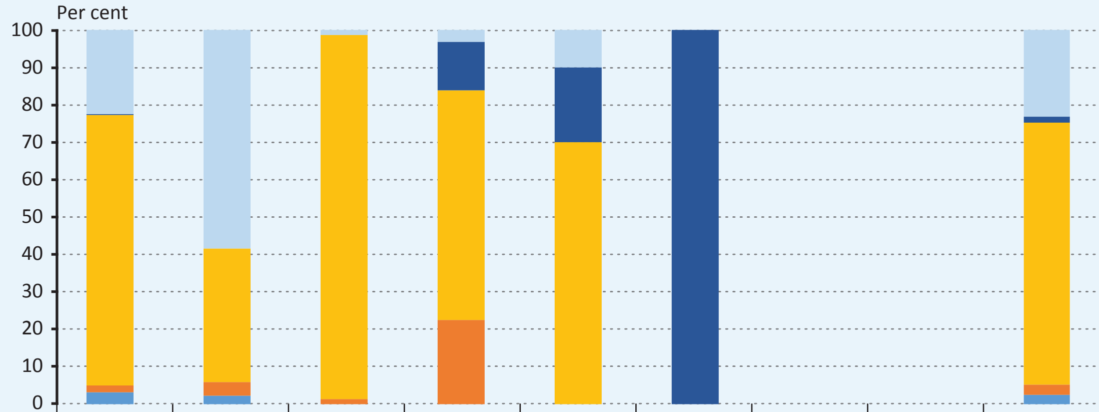


Figure 15 shows that the vast majority of incidents reported to the CBH were incidents that could be classified as failures and malfunctions. Therefore, the root cause analysis raises the question of why the failures and malfunctions category is so over-represented. A review of the technical descriptions of the reports suggests that the reason behind the eminent values may be that a large proportion of malfunctions are detected by sophisticated monitoring tools (i.e. they are less likely to go unnoticed) and thus form a constant subset of the incidents identified. It is also worth noting that the large majority of the data comes from banking environments, where prudent operations require the use of advanced monitoring and detection tools, and institutions already have current requirements to report outages affecting payment services. Nevertheless, the results confirm the hypothesis that the Hungarian financial sector is not one of the most prominent targets for fraudsters. We can only speculate as to the reasons for this, but apart from the difficulty of the Hungarian language (which may make it more difficult for phishing attacks to be carried out), the relatively small size of the sector compared to the rest of Europe and its overall good preparedness in the field of IT security may play a role. A more detailed chart is available for the analysis of the other categories.

Below is a detailed breakdown of the root causes of incidents grouped by type of institution (Figure 16).

Figure 16
Distribution of root causes by type of institution and month of reporting



	Bank	Insurance undertaking	Financial markets infrastructure (FMI)	Fund	Investment firm	Fund management	Insurance broker	Financial undertaking	Total
🟦 Physical attack (deliberate/ intentional)	18	2	0	0	0	0	0	0	20
🟧 Unintentional damage / loss of information or IT assets	10	3	1	7	0	0	0	0	21
⬜ Disaster (natural, environmental)	0	0	0	0	0	0	0	0	0
🟨 Failures/ Malfunction	399	30	72	19	14	0	0	0	534
🟦 Outages	1	0	0	4	4	3	0	0	12
🟩 Eavesdropping/ Interception/ Hijacking	0	0	0	0	0	0	0	0	0
🟦 Nefarious Activity/Abuse	125	49	1	1	2	0	0	0	178
🟫 Legal	0	0	0	0	0	0	0	0	0

After the first place category of failure and malfunction, the second ranking category is nefarious activity and abuse, which accounts for almost 25% of all reported incidents. When looking at this category, it is important to note that a significant proportion of the reported nefarious activity was not targeted against institutions, but against customers, or possibly it was some general (non-targeted) malicious activity. The cumulative data shows that the malicious attacks were mainly reported by banks and insurance undertakings. This confirms that, as previously discussed, these types of institutions are preferred by attackers, as they are the most likely targets to yield direct financial gains.

In the physical attacks subcategory of the nefarious activities category, the most common threat is the loss or theft of employee hardware (e.g. laptops, mobile phones). Most of these incidents coming from loss and theft result in a police report. Encryption of back-up storage media can significantly reduce the associated risks for these types of incidents.

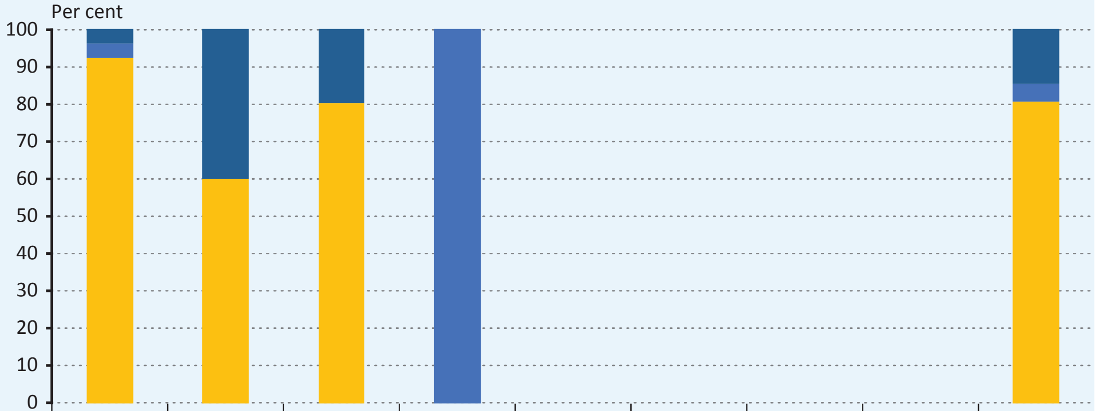
There were no environmental incidents (e.g. water leak, fire) in the participating institutions. This fact can be explained by the high safety requirements specific to the sector (around which the facilities they use are designed), but may also be related to the weather conditions during the Pilot period (dry, droughty weather). At international level, for example in the UK, the extreme heat caused problems in cooling data centres, leading to outages. In Hungary, even in the extreme summer heat, there were no similar disruptions.

Three categories are included in the methodology defined during the Pilot Project, which are not linked to an incident. These are, respectively, disasters, eavesdropping and legal incidents. There were no environmental disasters in the country during the course of the project. Moreover, eavesdropping incidents can result in unauthorised access to highly sensitive data, so robust protection against wiretapping is a well-understood interest of sectoral institutions. Although precise data are not available, it can only be assumed based on expert judgement that the specific situation of the Hungarian language and the adequate level of protection may have played a role in the low occurrence of wiretapping incidents. In addition, in such cases, if the purpose of the eavesdropping is not blackmail or disclosure, the latency is likely to be much higher, as the interceptors do not reveal themselves. The encryption of data transmission has been a regulatory requirement[24] for a long time. The foregoing consideration is also valid in case of legal incidents, where a legal incident may cause significant financial and reputational losses. The strict data protection and legal environment strongly supports keeping the number of incidents at a minimum in the field.

[24] See Government Decree 42/2015 (12.03.2015) on the protection of the information system of financial institutions, insurance and reinsurance undertakings, investment firms and commodity exchange service providers (Available: https://njt.hu/jogszabaly/2015-42-20-22) and, among others, MNB Recommendation 8/2020 (22.06.2020.) on the protection of the information system, which helps to interpret the provisions of the said Decree (Available: https://www.mnb.hu/letoltes/8-2020-informatikai-rendsz-vedelmerol.pdf).

In the case of reported critical incidents, the root causes of the most frequent incidents – similarly to the pattern of the overall incident population – are overwhelmingly due to failures and malfunctions (Figure 17).

Figure 17
Breakdown of root causes by type of institution and month of reporting (for critical incidents)



	Bank	Insurance undertaking	Financial markets infrastructure (FMI)	Fund	Investment firm	Fund management	Insurance broker	Financial undertaking	Total
🟦 Physical attack (deliberate/ intentional)	0	0	0	0	0	0	0	0	0
🟧 Unintentional damage / loss of information or IT assets	0	0	0	0	0	0	0	0	0
⬜ Disaster (natural, environmental)	0	0	0	0	0	0	0	0	0
🟨 Failures/ Malfunction	23	6	4	0	0	0	0	0	33
🟦 Outages	1	0	0	1	0	0	0	0	2
🟩 Eavesdropping/ Interception/ Hijacking	0	0	0	0	0	0	0	0	0
🟦 Nefarious Activity/ Abuse	1	4	1	0	0	0	0	0	6
🟫 Legal	0	0	0	0	0	0	0	0	0

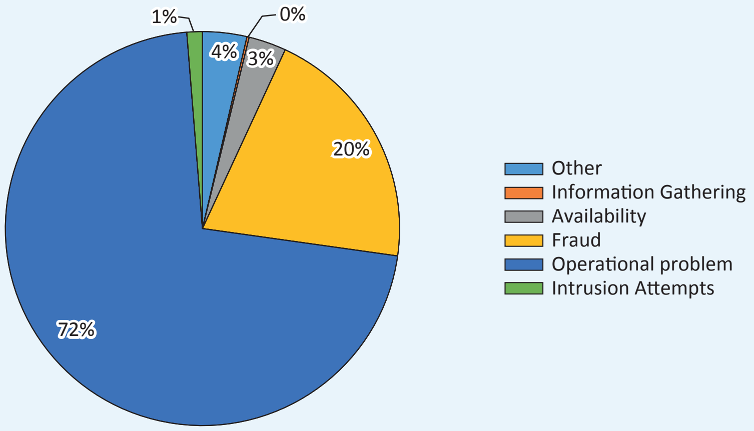
Incidents originating from the institutions' own infrastructure and from third parties providing services to them fall under the category of failures and malfunctions.

For critical incidents, a smaller number of incidents were caused by abuse, due the exploitation of weaknesses in systems not updated properly.

Given that more than two-thirds of the incidents were reported by banks, we have more detailed information on this type of institution, so on the following charts incident data coming solely from banks will be presented.

The following figure shows the distribution of the types of incidents reported by banks (Figure 18).

Figure 18
Distribution of types of incidents occurring in banks



In case of banks, the large majority of the reported operational problem type incidents, around 72 percent, are also due to failures and malfunctions. When the category of bank failures and malfunctions is further broken down, the vast majority of incidents, 95 percent, were caused by operational problems. In a smaller proportion, five percent, other failures or disruptions at so-called third-party ICT service providers[25] other than the bank were the cause of the banking failures and malfunctions. A more detailed analysis of the technical data in the failures and malfunctions category reveals that system failures in banking environments are much less common than in the overall sample. The lower failure rate is due to the higher fault tolerance of the systems and the stricter availability requirements. For example, the continuous availability required for the instant payment system is ensured by the majority of payment service providers through maintaining two active sites. It is interesting to note that, while failures or interruptions of communication networks have been identified in non-banking systems, no such failures have been reported in banking systems during the Pilot Project. It is likely that the higher fault tolerance and increased redundancy of banking communication networks is responsible for the absence of failures or interruptions in their communication networks.

Nefarious activity was also the second leading cause of incidents in the banking segment during the period under review, with 23% of incidents linked to nefarious activity. More than half of the malicious incidents were caused by targeted attacks (e.g. APT, DDoS, etc.). During the Pilot Project period, non-bank participants also identified targeted attacks. This shows that other institutions in the financial sector are also being targeted, albeit to a lesser extent. The abuse of information and information systems (including mobile applications) was also limited to banking actors, with a total of 15 cases during the period under review. There were 25 reported cases of attacks based on deception identified in case of banks, while for other types of institutions the number was negligible. A possible explanation may be that it is much more difficult to initiate a transaction with a direct financial gain in the case of insurance undertakings or pension funds. It should also be underlined that phishing attacks typically target bank customers rather than banks. In the category of malicious code and malicious software, only two incidents were reported by banks. Institutions reported eight times more incidents than that just in the insurance sector. There were 12 cases of Denial-of-Service (DoS) attacks at banks, and apart from banks only investment firms suffering DoS attacks during the Pilot period. It is important to note that banks have been the targets of DoS and DDoS attacks for several years and most of them have by now established professional defences. Attacks on banks therefore typically do not result in any real outage. Unauthorised activity (not in the financial sense, but in the

[25] Examples of such services include telecommunications services.

ENISA sense) – as a primary root cause[26] occurred only once for banks during the course of the Pilot Project, while the same category was identified multiple times for funds and insurance undertakings.

Although the number of physical attacks appears to be significant, there were several cases of bomb threats, which fortunately did not involve actual physical attacks. The theft of laptops, mobile phones from various locations (e.g. office, public transport, car) is the most prevalent form of physical attack. There was only one case of vandalism of an automated teller machine (ATM) during the Pilot Project period.

Unintentional damage/loss of information or IT assets is the last category that can be measured in percentage terms and includes the following: damage caused by a third party; erroneous use or administration of devices and systems; information leakage or sharing due to human error. There were precedents for the incidents listed in the Pilot Project, but their number was not significant. In the category of third-party damage, various attempts to penetrate banking systems were reported.

There was only one reported case of outage or loss of resources, which happened due to a technical problem with the uninterrupted power supply following a power failure in the data centre.

The fraud category was characterised by phishing and voice phishing (vishing) attempts. With one or two exceptions, phishing and vishing attempts were mainly directed against bank customers. Banking institutions reported five times as many fraud incidents in the Pilot period as insurance undertakings and funds combined, which demonstrates the higher exposure of banks to these types of attacks and attempted fraud.

Box 2
The CyberShield (KiberPajzs) initiative

On 7 November 2022, the CBH, the Hungarian Banking Association, the National Media and Infocommunications Authority (NMHH), the National Cyber Security Center of the Special Service for National Security (SSNS-NCSC) and the National Police Headquarters (ORFK) launched a joint educational and communication cooperation called CyberShield. Nowadays digital fraudsters mainly attack by the emotional manipulation and deception of consumers, so the participants will collaborate to strengthen financial awareness among consumers and to help them effectively manage cyber risks.

KiberPajzs
Védelem a pénzügyekben

Under the CyberShield project, which will run until 31 January 2024 and can be extended at the request of participants, institutions and market players will launch a comprehensive education programme to improve customers' digital financial awareness. As a means of this, a broad and coordinated communication campaign has been launched on cybersecurity risks and how to defend against them.

The CyberShield project will also analyse regulatory and market processes, and through cooperation, participating law enforcement agencies will further develop their cybercrime prevention and investigative capabilities, while cyber defence authorities will improve their effective incident management procedures and practices. The project will pay particular attention to minors and vulnerable groups (such as the elderly), but will also provide preventive messages to consumers, small and medium-sized enterprises and other corporate clients.

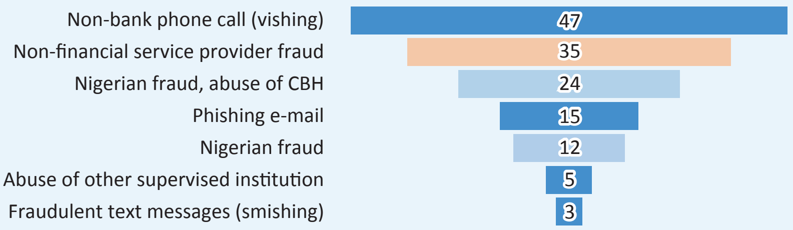
[26] See for example the ENISA threat taxonomy (Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy)

Digitalisation is increasing the importance of electronic payments, and at the same time – while the domestic financial system is considered to be one of the most secure in Europe – the increase in the number and proportion of successful fraudulent transactions is apparent. Criminals do not attack financial institutions or infrastructure, but primarily target consumers (who are sometimes not cognizant of the rapid changes) by deceiving them and manipulating their emotions. This is the reason why it has become essential to raise the financial awareness of customers, who are the "first line of defence", and to prepare them to deal with cyber risks.

The participating institutions of the CyberShield will present uniformly designed, simple messages about the key models of fraud, such as different forms of phishing, fake bank calls or text messages (SMS), fake bank websites, fake transaction approval forms, fraudulent investment modes or online offers, and personal data theft through social media. The billboards and messages feature three "everyday role models" who are coping with these risks in a similar situation to most digital financial consumers in Hungary.

The above trend is also confirmed by the cyber fraud related experience of the Customer Relations Information Centre of the CBH in their role of customer service, which shows that based on customer complaints received by the CBH, the most common form of attack during the period under review was vishing, followed by cyber fraud on behalf of non-financial service providers (Figure 19). The summary also shows that phishing attacks via classic banking e-mail are only the fourth most common form of attack. The majority of customer notifications were received from customers who had already suffered financial loss (62 percent), but the customer service of the CBH also received alerts from customers who reported a cyber fraud attempt. In a number of cases (20 percent), customers reported that they had also filed a police report in connection with the cyber fraud.

Figure 19
Types of cyber fraud based on customer reports received by the CBH Customer Relations Information Center, February - August 2022



Continuing with the analysis of reported incidents in banking systems, there were no reports of successful network intrusions, but there were a number of attempted intrusions. In accordance with recently published vulnerabilities and publicly available codes exploiting those vulnerabilities (so-called exploits), unknown perpetrators have attempted intrusions based on known vulnerabilities in Log4j[27], Spring Cloud[28] and IIS servers[29]. For some of these vulnerabilities, we know from the data available to the CBH that the supervised institutions took the necessary protective measures shortly after the vulnerabilities were disclosed.

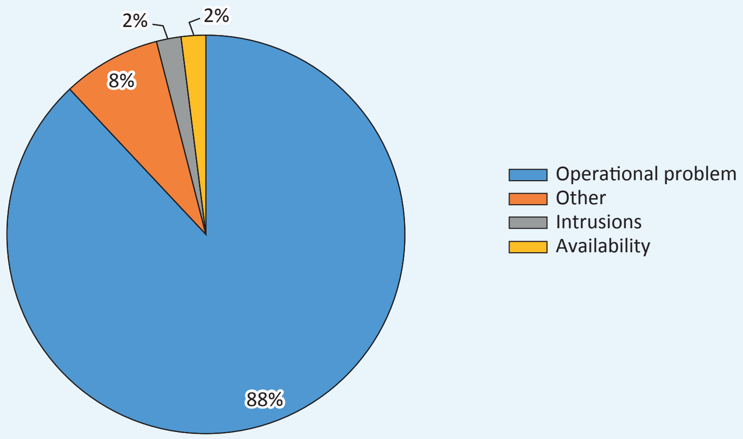
There was only one report of an information gathering type of incident, when customers of one bank received an e-mail containing a link to a site resembling the bank's Internet banking portal, but leading to a phishing site.

Other types of incidents, which cannot be classified by the institutions, accounted for approximately four per cent of the incidents reported, typically due to incidents that restricted the availability of information.

[27] Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228
[28] Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963
[29] Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907

For critical incidents, the distribution of incident types is analysed first (Figure 20).

Figure 20
Breakdown of critical incidents by incident type, based on customers affected



For each incident, the supervised institutions had the opportunity to provide the number of customers affected. If we suppose that there is no overlap in the number of clients affected by each incident, we can add up the number of clients affected to estimate the *total number of clients affected*. The types of incidents can also be ranked by the proportion of customers affected: the ratios of the total number of customers affected by an incident type to the total number of customers affected by incidents are shown in Figure 20. It is apparent here, that the most prevalent incidents are operational problems based on the proportion of affected customers as well.

After analysing the subcategories given under the root cause categories of the reported incidents, it can be seen that incidents flagged as either operational problems, availability problems or problems falling into the “other” category, the events were reported because of systems becoming unavailable. In total, the number of user accesses affected by an availability problem during the six months of the Pilot period was approximately 150,000. This is the number of customers who may have experienced a problem accessing a service for a longer or shorter period of time. This does not imply that the incidents were actually perceived by such large numbers. Customers who did not attempt to access the services affected by the outages in question during the critical period may not have experienced the problem at all.

The analysis of the third category also provides important results: the incidents in the intrusion subcategory are all the results of a single incident at a single financial institution, affecting more than 3,500 customers. The incident highlights that the institution participating in the Pilot Project successfully managed an advanced, serious attack that also involved a system intrusion. The primary point of intrusion in the attack was an application server. Although the incident may raise questions about the weaknesses in internal patch management processes, investigations by the institution itself and authorities found that several less well known vulnerabilities were exploited by the attackers. Thus, no clear conclusions can be drawn as to whether a security update of the application server could have prevented the attack. In addition to the CBH, the National Authority for Data Protection and Freedom of Information (hereinafter: NAIH) and the SSNS-NCSC have also been notified of the incident. The institution responded quickly and effectively to the intrusion, in line with the best practices of its incident management plan. It also reinforced the affected system before the vulnerability could have had further negative consequences on the institution’s IT systems. The case illustrates the importance of both incident detection and the existence of incident management plans. Without these two elements, the management of an incident resulting from a successful attack would be significantly more difficult.

The critical incident analysis looked into the number of people affected in relation to the main root causes of incidents (Figure 21).

Figure 21
Number of customers affected by root cause of critical incidents

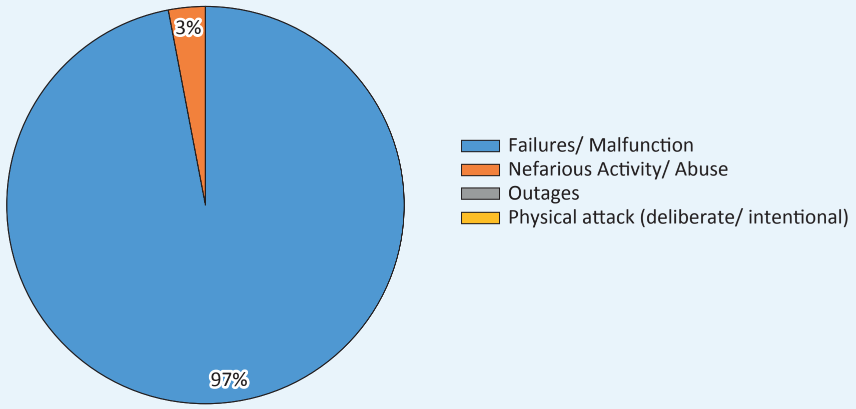


Figure 21 – similarly to Figure 20 – compares the root causes based on the number of customers affected. If we suppose that there is no overlap between the customers affected by each incident, we can add up the number of customers affected respectively, to estimate the *total number of customers affected*. The root causes of incidents can also be ranked by the proportion of customers affected: the ratio of the number of customers affected by a given root cause compared to the total number of affected customers is shown in Figure 21.

Most customers were affected by failures and malfunctions. Within this, the most significant impact was limited to customers of one of the largest banks in Hungary who would have made a card payment on a given day. The incident affected tens of thousands of customers, illustrating the potentially significant impact of a minor failure.

Incidents involving customers were typically linked to banks: for incidents reported by other non-bank institutions involving customers, the total number of people affected was 3,400, while for bank customers the total number of people affected was approximately 150,000.

Despite the fact that the current threat landscape shows that the majority of incidents during the period under review was attributable to root causes related to operational problems, the risk of attacks still remains. Financial services providers in Hungary have robust defensive controls and strong professional background and support to reduce the chances of malicious activities directly targeting institutions being successful. Despite this, attempted attacks remain a high risk, both for financial institutions and their external suppliers. Vulnerabilities were identified as a root cause in two of the critical incident reports. For example, one of the incidents reported to the CBH involved the discovery of a software vulnerability that required an institution providing extensive financial services to shut down a business website until the risk was eliminated by the deployment of security patches. Had the vulnerability not been discovered, the vulnerability could have posed a significant risk in the event of a potential targeted attack.

Still looking at critical incidents, nefarious activities were identified in case of two critical incidents that affected customers as well. One of these was the previously mentioned outdated software running in an incorrect configuration, the other was a distributed denial of service (DDoS) attack that also affected over a thousand customers. Other nefarious activities include phishing attacks, which remain common and widespread, particularly in the financial sector. In the wake of the phishing waves of recent years, the security awareness of supervised institutions has improved considerably in this area. Nevertheless, in the Pilot Project, critical incidents were identified where the root cause was a phishing attack.

Box 3
Case study of a critical incident causing an outage

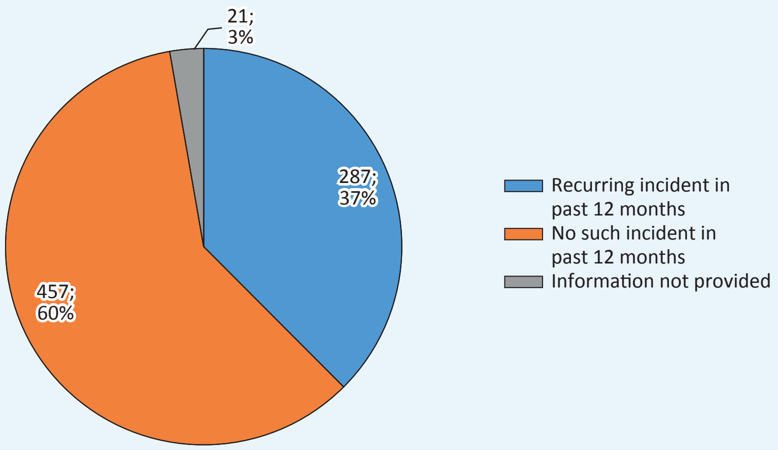
Reading the news on cyber incidents, it would be wrong to think in that critical incidents only constitute attacks by nation-state sponsored hacking groups affecting the most significant financial service providers. In reality, the experience of the Pilot Project has shown that any root cause may trigger a critical incident. In general, incidents and their root causes may be related to the scope of activity, size or other characteristics of the institution concerned. By comparison, in our breakdown of critical incidents, we found that few of these incidents align with patterns identified from monthly reports. As an example, we highlight a critical incident at a financial service provider that resulted in a service outage, where the root cause can be traced to a power outage. The criticality of the incident was caused by a secondary event, the failure of uninterrupted power supplies. Moreover, this event during the Pilot is not unique, the CBH has encountered similar incidents before. Compared to incidents with the same root cause that have not had a negative impact on the proper running of services, it is clear that any root cause, however trivial, may have a major impact on the functioning of an organisation when multiple factors simultaneously influence the effective management of an incident. Furthermore, the incident illustrates that any incident root cause may have a significant impact on an institution of any size if security controls are not properly in place, and thus it is not possible to significantly mitigate the impact of the incident in a timely manner. Incident management should not end with the restoration of the service, in all cases the root causes of the incident should be identified and measures must be taken to address the root causes to prevent a recurrence of the incident.

Of the incidents due to outages, only one affected a really small number of users. Staff at one financial institution were unable to access the Internet due to the service provider’s involvement. Thus, the category of incident root causes affecting a total of 19 people highlights that the incident reporting practices of the institutions that provided reports during the Pilot Project varied widely in their understanding of what constitutes customer exposure and whether they consider internal users as customers.

In the detailed analysis of the incident data, the last area examined was what the institutions see when identifying incidents, whether they have encountered the cause of the incident in the preceding 12 months or whether the incident identified was attributable to a cause new to them.

The following chart shows whether the cause of the incident has occurred before or was identified for the first time by the reporting institution in the last 12 months. In summary, two thirds of the incidents are attributable to a new root cause not encountered in the last 12 months (Figure 22).

Figure 22
Recurrence rate of incidents



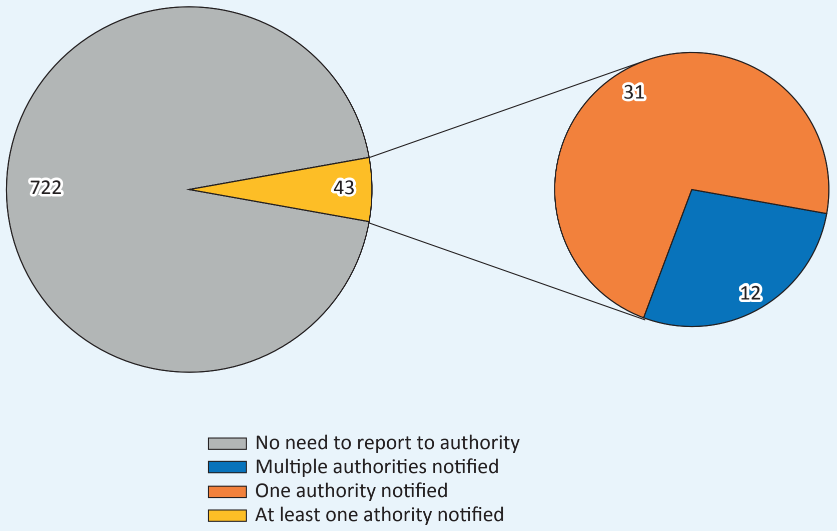
The vast majority of incidents attributed to a new cause in the six-month reporting period were non-critical, operational type issues affecting individual systems and components. Among the failures encountered, updates and configuration file incompatibilities stand out as non-malicious activity. Based on the data, it is of utmost importance to prepare a recovery plan as part of the change management process for changes affecting IT systems, as this could potentially minimise downtime. The majority of incidents attributed to new causes resulted in system malfunctions, which led to service outages. During the incident resolution process, updates, enhancements and exceptions were added to ensure that the same type of incident does not occur again in the future.

In case of remaining one third of reported incidents the cause of the incident had already occurred before. Two main areas could be distinguished: nefarious activity and malfunction. The majority of nefarious activities was DDoS, SPAM and phishing attempts. These attacks were generally large in scale, targeting multiple systems or individuals at once. Most incidents with recurring root causes –unlike incidents attributed to new root causes—, did not cause service outages.

4 ANALYSIS OF AUTHORITY NOTIFICATION AND EXTERNAL SERVICE PROVIDER INVOLVEMENT

The incident reports sent to the CBH during the Pilot Project also included cases where further notification to an authority was necessary. In case of approximately five percent of the total number of reported incidents, another authority in addition the CBH was notified by the institutions concerned (Figure 23). In a quarter of these incidents, more than one other authority was notified.

Figure 23
Incident numbers as a function of authority notifications

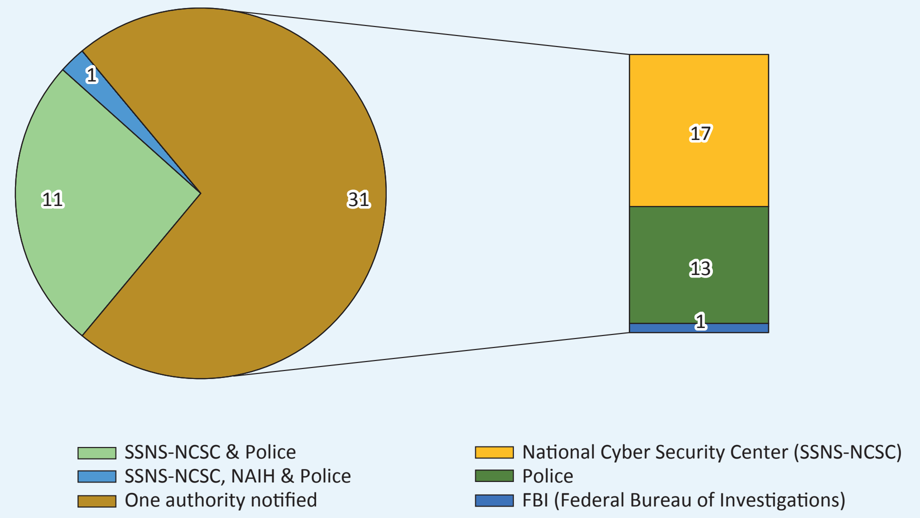


The ratio may change dynamically in the future depending on a number of factors, for example if the sensitivity of the institutions required to report incidents in the coming years will significantly differ from the sensitivity demonstrated during the Pilot Project, or if the scope of incidents that must be reported to the authorities changes, for instance as a result of the new regulations mentioned in the section on International regulatory initiatives.

When analysing this five percent of incident reports, if the incident report involved an authority other than the CBH, two cases could be distinguished. In almost three quarters of the incident reports, notification to an authority other than the CBH was sufficient. In slightly more than a quarter of cases, multiple authorities were notified at the same time. Among the data recorded, in the cases where more than one authority was notified, the statistical proportion of authorities notified was not measured in relation to the total number of incident reports. The total incident population was measured in relation to the number of incidents for which an authority was notified, not the number of actual notifications. In numerical terms, a total of 57 notifications were sent to the authorities for the 44 incident reports concerned. Notably, there were some reported incidents where the institution misjudged whether it notified an authority or a different stakeholder.

After aggregating the data on notifications to authorities, three domestic and one international authorities were identified under the Pilot Project, as the authorities to which incidents were reported (Figure 23): the SSNS-NCSC, the police, the NAIH, the Federal Bureau of Investigation (hereinafter: FBI).

Figure 24
Authority notification rate



In nearly 40 percent of cases, the SSNS-NCSC was informed, while in 30 percent of cases only a report to the police was submitted. The remaining 30 per cent were predominantly cases where the SSNS-NCSC and the police were notified at the same time. The SSNS-NCSC was notified by those institutions which, on account of being a critical infrastructure and/or essential services, have a reporting obligation.

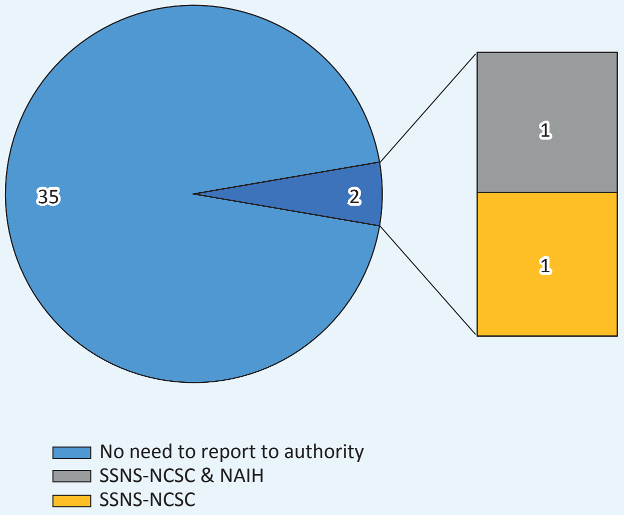
The CBH received information in all the cases examined above, so an authority would have been notified in all incidents and would have received reports even without the Pilot Project, due to the existing reporting obligations. Looking at the cases one by one, it can also be seen that the internal procedures of the institutions differ significantly in terms of which cases are reported to the police. The reporting obligations imposed on institutions may also differ significantly depending on the nature (e.g. bank or financial markets infrastructure) and criticality of the institution.

The notification of a foreign authority (FBI) was necessary due to a group-wide, large scale DDoS attack that affected not only the Hungarian institution but also institutions in other countries.

As already reported, for the overall incident population the leading root cause was failure/malfunction, followed by nefarious activity in second place. In contrast, for regulatory notifications, the vast majority of reported incidents fell into the cathegory of nefarious activity. Incidents involving the notification of an authority fall into the following types: nearly 40 percent of cases were phishing incidents; 25 percent were reported as bomb threats; in more than 15 percent of cases, there was a physical theft of some laptop; and in 12 percent of the cases, the institution was the victim of a DDoS attack. All 11 cases of the bomb threats were linked to a single institution, which is present in both on the Russian and the Ukrainian markets. The bomb threat is believed to be linked to the Russian-Ukrainian conflict. The bomb threats were sent by e-mail to a previously used e-mail address in broken Hungarian, using some Cyrillic letters.

For critical incidents, a similar distribution of regulatory notifications can be observed (Figure 25).

Figure 25
Number of critical incidents as a function of authority notifications



Banks and insurance companies are predominantly affected, with incidents resulting from failures, malfunctions and nefarious activities. A total of 37 critical incidents were reported to authorities during the Pilot Project, including 29 failures and malfunctions.

For critical incidents, similar to the proportion found in the analysis of the total incident population, approximately five per cent of the cases required notification to an authority other than the CBH.

Two domestic authorities have been identified in the relevant incident reports: SSNS-NCSC and NAIH.

In the case of critical incidents, two root causes were identified in the official notifications: a malicious network attack from the Internet or a DDoS attack.

Box 4
Case study of an incident at European level

A fundamental concept of the EU's international regulatory efforts, in the financial sector as well as in other sectors, is that operators contribute to the development of the European single market by providing cross-border services. The resilience of the global infrastructure that enables the digitalisation of cross-border services is of paramount importance in order to ensure the uninterrupted availability of communication channels. Regarding optical fibre cables, which form the backbone of communication infrastructures, it would be reasonable to assume that the communication and infrastructure networks essential for economic activities are immune to successful attacks by now.

On 27 April 2022, an unknown person or group deliberately cut several vital fiber-optic cables near Paris[30]. The string of vandalism was one of the largest attacks against Internet infrastructure in the history of France and highlights the vulnerability of critical interconnected communications networks.

[30] WIRED UK: The Unsolved Mystery Attack on Internet Cables in Paris (Available: https://www.wired.co.uk/article/france-paris-internet-cable-cuts-attack)

The attacks against the Internet network began in the early hours of 27 April, with the perpetrators cutting cables in three locations around the French capital in the course of around two hours. According to the authorities, all three incidents occurred at roughly the same time and were carried out in the same way. The cables were cut in a way that caused as much physical damage as possible, deliberately making the repair process more difficult. Two facts emerged about the series of incidents that distinguish them from previous incidents involving telecommunications towers and internet infrastructure. Firstly, the coordinated nature of the attacks, the simultaneous timing of their occurrence suggests an organised background and secondly, the extent of the damage caused, which may suggest that the attackers' aim was to deliberately cripple the French communication networks. Since in France optical-fiber cables that are part of the Internet backbone network usually follow existing physical infrastructure elements, so whoever carried out the attacks must have had precise knowledge of the cable routes.

That is why the French authorities have been following the incident with particular attention from the very first moment. The French Public Prosecutor's Office launched an investigation, supported by the Central Intelligence Authority (DGSI) of the Ministry of Defence and the Judicial Police, as following the incident the authorities maintained the possibility of a terrorist attack.

The incident caused disruptions in Internet access all across France, and mobile networks were also overloaded as a result of load balancing attempts. The damage proved to be much more extensive than initially reported, as we now know that the incident had a major impact across Europe and on many European institutions.

The incident also had an impact in Hungary: a financial service provider with European exposure experiencing a significant service outage days later across several of its process support systems. Earlier in the history of Hungarian payment services a similar incident to the one in Paris occurred in 2008, when unknown perpetrators damaged and stole 36 telecom trunk lines in two cable ducts near Határ street. As a result of the vandalism, fixed Internet services and 20,000 fixed telephone lines were unavailable, affecting hundreds of district offices and businesses. The interbank clearing system was paralysed for a day. Most telecommunication services in the country were also temporarily shut down.

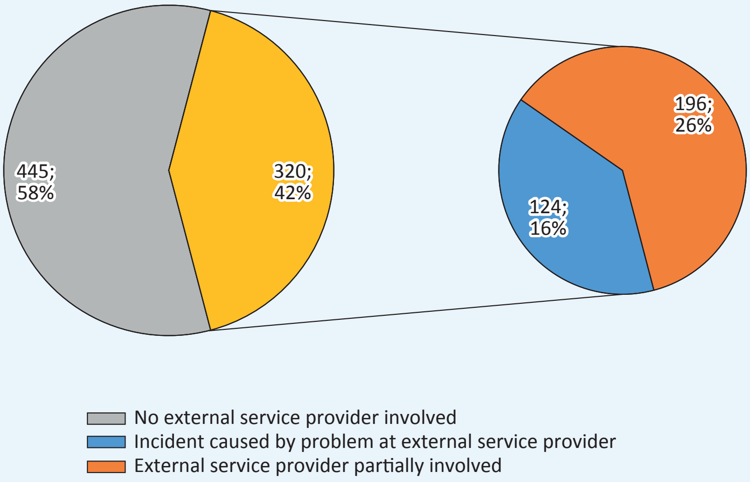
Although the Paris incident was quickly resolved by the operator and the impact of the outage on customers was negligible, the incident highlighted that the spill-over effects of a physical security incident can have cross-border implications.

After the closure of the Pilot Project, another high-profile incident involving the sabotage[31] of communication cables occurred in Europe: a section of the German railway network was paralysed by the attack. While examining these incidents, we have to ask ourselves whether we are seeing a new trend unfolding or if it is just a coincidence.

[31] POLITICO: 'Sabotage' causes major train disruption in northern Germany (Available: https://www.politico.eu/article/sabotage-causes-major-train-disruption-northern-germany/

When analysing the involvement of third parties in the reported incidents, 42% of the incidents involved an external service provider (Figure 26). Of the 320 incidents involving an external service provider, approximately 40%, or 124 cases, were caused by a failure at the external service provider, so in many cases the root cause analysis had to be performed by the external service provider where the failure occurred.

Figure 26
External service provider involvement rate



The largest number of incidents involving third parties were reported by institutions in relation to banking and financial infrastructure elements, often identifying operational problems not previously encountered, which should be taken into account during the risk analysis of outsourcing activities. Some of the incidents caused operational problems, with root causes in supply chain failures, which in many cases resulted in service outages. Another group was nefarious activity, where the root cause of most incidents was a targeted denial of service (DoS) attack. In these cases, the failures usually resulted in connectivity problems and slowdowns.

The analysis of the corrective actions shows that improvements and modifications have been introduced to avoid further incidents in these cases, in order to minimise the occurrence of future incidents due to the same cause.

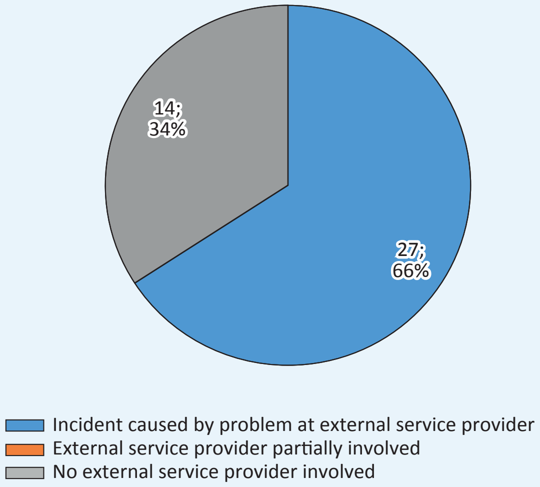
ENISA's report on supply chain attacks[32] also points out that supply chain attacks have been increasingly common for years, as supply chains can provide a larger and sometimes less resilient attack surface than the stringent network security of financial institutions. Once the supply chain has been successfully breached, attackers may have new opportunities to penetrate systems, in many cases from IT environments that are deemed trusted. Such a successful attack against an outsourced service provider has already occurred in the Hungarian financial sector, but the incident was not reported to the CBH in the context of the Pilot Project and the attacker did not proceed further towards the financial institutions connected to the service provider.

The use of external service providers therefore remains an option on the one hand and an increased security risk on the other, which is important to take into consideration in the planning phase of outsourcing services, as well as to monitor continuously during the service phase and to carefully resolve during the phase-out period.

[32] Available at: https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

When examining the relationship of critical incidents to external service providers, a significant difference is seen compared to the total set of incidents, as the third-party involvement rate is reversed, at over 66 percent. Looking at all incidents where an external service provider was involved (Figure 26), in 61 percent of cases the third party was only partially involved. In comparison, for critical incidents, 27 of the 41 reported critical incidents had a root cause in a third-party failure (Figure 27).

Figure 27
Number and proportion of critical incidents with external service provider involvement



The largest number of critical incidents caused by a failure at an external service provider affected banking systems due to specific, previously unseen operational problems. The incidents caused operational problems resulting in service outages. Incidents due to malfunctions involved system/service access, text messaging (SMS), data upload and data download errors, which took on average seven hours to resolve.

Box 5
Case studies of critical incidents involving external service providers

Based on the lessons learned from the Pilot, external service providers in the financial sector were a prime target for targeted attacks. The sector is increasingly characterised by third-party involvement, which increases the exposure of institutions, as not only their own digital assets but also those of third-party service providers become targets. As a good illustration of the process, the root cause of the largest of the critical incident alerts affecting 64,000 customers, was triggered by an operational malfunction at an external service provider. The failure resulted in tens of thousands of retail and business customers being unable to access certain services, with the affected institution effectively not being able to participate in the technical management of the incident.

In addition to external suppliers, card service providers can also be a prime target for more sophisticated attackers. For example, the only DDoS attack that was classified as a critical incident was against a 3D Secure Access Control Server (3DS) system vendor. The system responsible for cardholder security authentication became unavailable, causing serious operational problems for a domestic financial institution. Similar attacks have been seen frequently over the past few years. In general, and especially for DDoS attacks, it is important to note that in many cases, an attack on any specific target may be a distraction or an attempt to divert resources. Attacks against card service providers for instance are often followed by other types of card fraud, where attackers try to exploit the weaker fallback security mechanisms used in the event of 3DS unavailability in a multi-stage attack for financial gain.

The critical incidents presented also draw attention to third party risks, a topic that will receive increasing attention in the coming period. The lesson from the incidents is that the responsibility may not be outsourced, even if the incidents are due to problems at the suppliers.

Regards nefarious activities, the root cause of the incident was mostly the exploitation of a known flaw in an obsolete system component or a targeted denial of service attack, which was also reported to the appropriate authority.

Previous recurring incidents have either been caused by nefarious activity or disruptions to text messaging (SMS) services.

V Presentation of technical data

1 PRESENTATION OF THE HARDENIZE DATA COLLECTED DURING THE PILOT PROJECT

In cybersecurity, hardening is the process of reducing the vulnerability of the system in its different layers, making it resistant to possible attacks. This may be done by reconfiguring the system security settings or by integrating additional tools. The effectiveness of hardening can be measured by various methods, such as checking the appropriateness of the configuration settings and the existence of the protection mechanisms.

During the development of the threat landscape project, we assumed that although systems can have a wide range of vulnerabilities and may be attacked for a variety of reasons and on a variety of surfaces, a significant part of attacks are focused on targets available on the Internet, and therefore the Internet domains are among the most important attack surfaces.[33]

Therefore, during the Pilot Project we have supplemented the reporting period with Hardenize[34] review carried out by the SSNS-NCSC to identify possible correlations between incidents and domain settings and defence solutions for the participating institutions, and to draw attention to the adequacy of the domain settings or the risks arising from possible shortcomings in the present report.

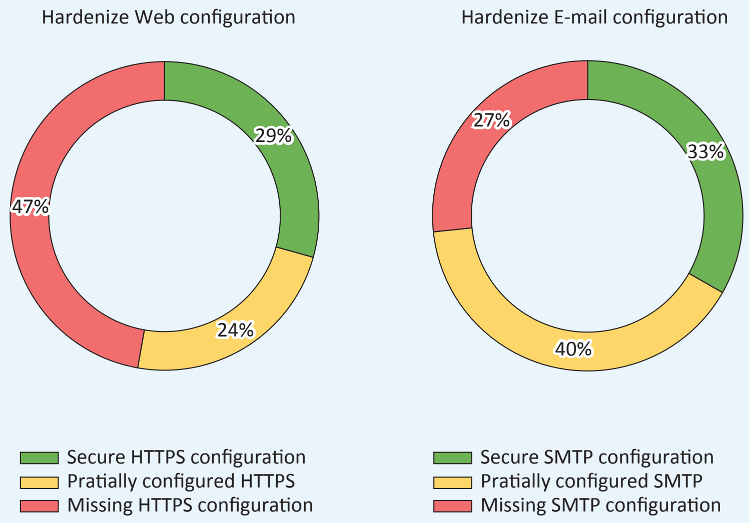
Hardenize is a web application that can scan domain settings and defence solutions. The application performs a series of scans based on the domain name you specify and provides a report on the domain configuration. Hardenize assesses the adequacy of DNS (Domain Name System), e-mail and web services separately, based on various application specific criteria. Thus, the Hardenize scan is a comprehensive security audit tool that evaluates domain, e-mail and web settings and configuration in a narrow audit timeframe. Based on the domain data provided by the institutions participating in the Pilot Project, the SSNS-NCSC carried out Hardenize scans on the systems of the participating institutions that were accessible from the Internet, which were intended to examine the configuration settings of the publicly available systems.

Based on the reports of the list of domains provided by the institutions participating in the Pilot Project, we have produced some charts which show the level of security settings of the institutions. The web and e-mail configuration figures were prepared to provide a general and a technical drilldown view, making it easy to see where institutions need to strengthen their security settings to make their services less vulnerable to cyber threats.

[33] “A domain name is a name that uniquely describes a specific part of the Internet, a domain. Domain names are assigned and interpreted hierarchically according to Domain Name System (DNS) rules.” Source: Wikipedia

[34] https://www.hardenize.com/

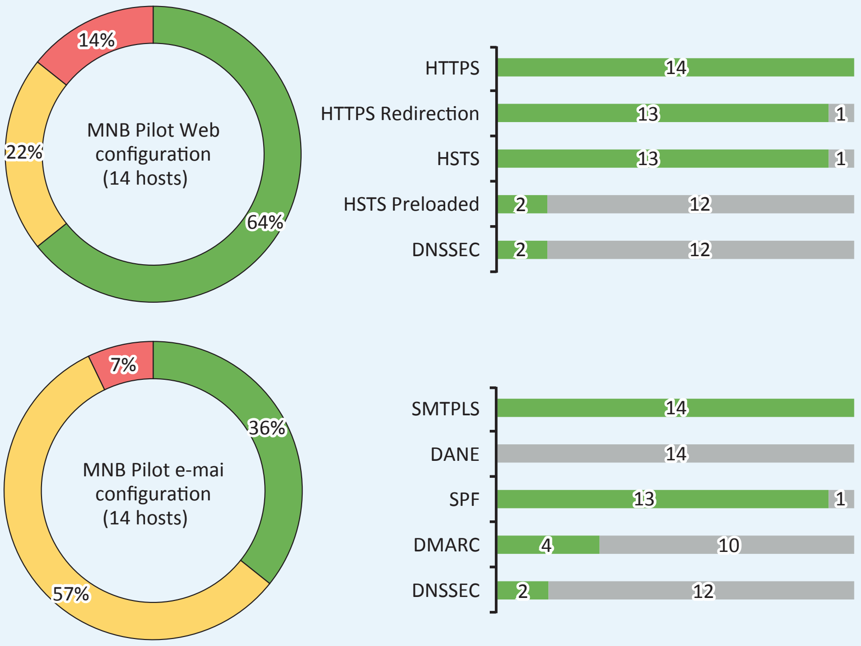
Figure 28
Summary of the SSNS-NCSC Hardenize report on infrastructure and e-mail settings in Hungary



Source: Hardenize, HU resilience dashboard

The SSNS-NCSC Hardenize report for Hungary, published by Hardenize[35], shows fewer data points than the analyses in our report. The total Hardenize report for Hungary consists of 351 data points, of which the number of data points particularly related to the CBH's Pilot Project is 14, whereas the number of data points made available to us under the Pilot Project exceeded one thousand. The discrepancy is due to the fact that the total list of domains submitted by the institutions included up to fifty domains per institution.

Figure 29
Pilot Project participant infrastructure and e-mail setup summaries of the SSNS-NCSC Hardenize report on Hungary



Source: Hardenize, HU resilience dashboard

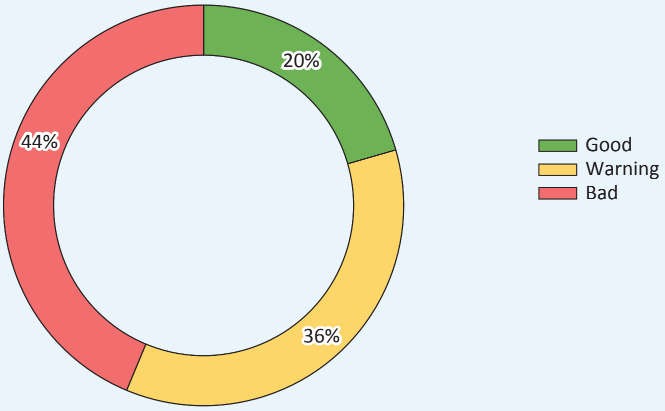
[35] https://www.hardenize.com/dashboards/hu-resilience/

The infrastructure and e-mail configuration summaries that can be viewed on the Hardenize dashboard have been prepared and are presented according to Hardenize's proprietary methodology. The figure showing the aggregation of the infrastructure configurations of 351 hosts in Hungary presented in the SSNS-NCSC Hardenize report (Figure 29), similarly to the breakdown of the hosts involved in the Pilot Project, is intended to show the summary and correctness of web, e-mail, and DNS configurations. The figures based on the SSNS-NCSC Hardenize data, produced as part of the CBH cyber threat landscape, show the presence or absence of settings and configurations in each case. The figures present a more comprehensive picture of how the institutions' devices are configured and thus their security posture as seen from the Internet.

2 INFRASTRUCTURE SETTINGS

Web configuration

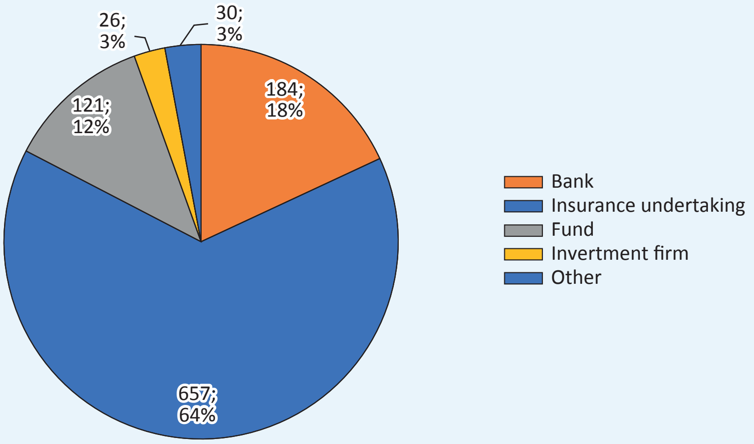
Figure 30
Complex web configuration for the domain data of the entire Pilot Project



The web configuration review provides a high-level overview of the web security settings of domains. Domain data was received from 37 of the 39 institutions participating in the Pilot Project. The web configuration security for all domains provided by the participants is presented in Figure 30. The web configuration overview analyses four features: the HTTPS, HSTS, HTTPS Redirection and HSTS Preloaded parameters (these technical concepts will be clarified later). Domains with all four parameters set were rated "Good". 20 percent of the domains received Good rating. This may be because institutions set all web configuration parameters only for their most important (critical) systems (and their associated domains). Presumably due to the time-consuming nature of the set-up, not all set-ups were implemented for less critical systems.

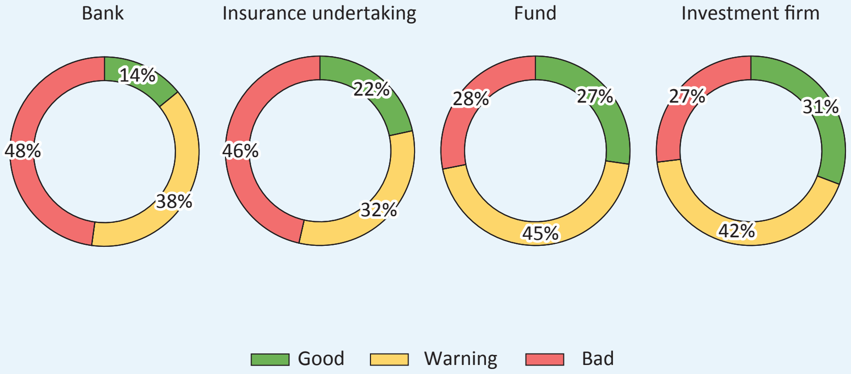
A "Warning" rating was given to domains whose HSTS and HSTS Preloaded parameters were not set. 36 percent of the domains received a Warning. The importance of these settings is that there should be no communication over HTTP at all, and all traffic should be forced to the encrypted data channel. "Bad" rating was given to the domains that did not have HTTPS or HTTPS Redirection configured in their parameters, which was the case for 44 percent of institutional domains. Setting up HTTPS and HTTPS Redirection is critical, as without them messages are sent over unencrypted communication channels. These settings are furthermore not appropriate for live systems because Government Decree No. 42/2015 (III. 12.) on protecting the information system of financial institutions, insurance undertakings, reinsurance undertakings, investment companies and commodity dealers (hereinafter: Government Decree 42/2015 (III.12)) requires institutions to ensure the confidentiality of data in transmission.

Figure 31
Number and proportion of domains for each type of institution



Of the types of institutions, insurance undertakings have the largest number of domains, accounting for more than 60 percent of the total number of institutional domains participating in the Pilot Project. While the number of domains linked to insurance undertakings was 657, the number of domains linked to banks, which had the second highest number of domains, was only 184.

Figure 32
Evaluation of the web configurations of the four types of institutions with the largest number of domains



The web settings for the four types of institutions with the highest number of domains are shown in Figure 32. The figure shows “Good”, “Warning” and “Bad” ratings based on the HTTPS, HSTS, HSTS Preloaded and HTTPS Redirection settings, in a way similar to Figure 30. The technical concepts of HTTPS, HTTPS Redirection, HSTS and HSTS Preloaded will be explained later.

The first figure is for banks, because these institutions are the most exposed to cyber-attacks. Almost 50 percent of their domains are not configured correctly, i.e., almost half of their domains do not have the HTTPS or HTTPS Redirection configured. Due to the unencrypted nature of the communication, a man-in-the-middle attack can be performed. A possible explanation is that the domain list includes elements that either serve the internal purposes of the institutions, or can only be accessed by specific means, or are unused and awaiting deletion. The ten insurance undertakings participating in the Pilot Project have almost three times as many domains as the participating banks, with almost the same non-compliance (“Bad” rating) rate. However, insurance undertakings have a significantly higher proportion of properly configured domains than banks: presumably more productive domains are in operation, where proper configuration is critical.

For the remaining two types of institutions (funds and investment firms), the measured values differ from those of banks and insurance undertakings. The explanation is probably that the number of domains for these types of institutions is on average much lower, so there are proportionally fewer domains that are waiting to be terminated, have been incorrectly configured or are intended for test purposes or internal use. For institution types with fewer domains, the "Warning" category was the largest. The proportion of compliant domains was higher and the proportion of non-compliant domains lower than for banks or insurance undertakings.

HTTPS, HTTPS Redirection

Websites must have some mechanism to ensure that visitors know they are in the right place. The simplest solution is HTTP connection over the TLS (Transport Layer Security), which is referred to as HTTPS. HTTPS also ensures the confidentiality, authenticity, and integrity of information. Systems that do not support HTTPS fail to provide these attributes during communication and are vulnerable to data modification and tampering. A working TLS (and HTTPS) service requires an asymmetric key pair, a certificate generated from the public key and the authentication of the certificate with a certificate chain traceable back to a qualified Certification Authority (CA) service provider. The availability of the HTTPS can only be determined for hosts with web content (accessible via HTTP), so for domains that are registered but do not contain an actual website, this is not possible. However, HTTPS availability alone is not enough: for its proper deployment, websites need to redirect all non-secure (plain text HTTP) traffic to the encrypted connection (HTTPS) on the web server side. This approach ensures that sensitive data cannot be exposed or modified in a man-in-the-middle attack, even if the attacker somehow redirects user traffic to the (unencrypted) HTTP connection. HTTPS Redirection can only be evaluated and interpreted for hosts where the service is available over HTTPS.

Figure 33
Web configuration parameters for the domain data of the entire Pilot Project

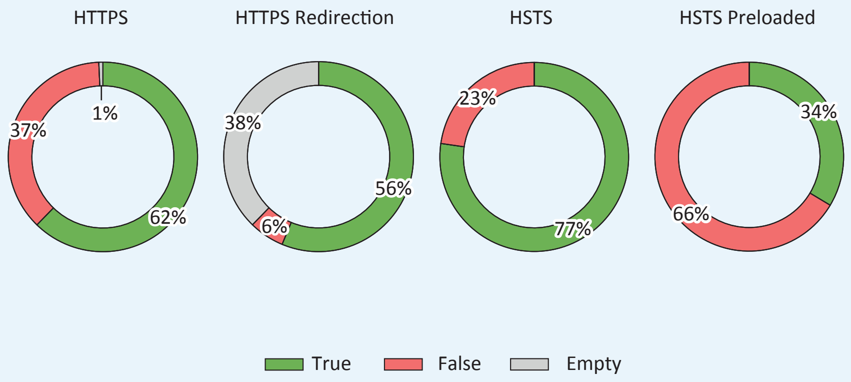


Figure 33 shows that 62 percent of the institutions' domains have HTTPS and 56 percent have HTTPS Redirection, suggesting that the domains of the institutions that operate in live environments are properly configured. HTTPS is not configured for 37 percent of the domains specified, while for HTTPS Redirection we see that 6 percent are not configured. Cases that cannot be examined are shown in grey in the figure, indicating blank values. This means that out of the 38 percent, the configuration cannot be examined due to the lack of HTTPS for 37 percent, and for 1 percent the value cannot be determined due to the unavailability of the domain under examination. The majority of these domains are presumably for internal use, which does not necessarily require strict configuration. The following two diagrams only apply to domains where HTTPS could be examined.

HTTP Strict Transport Security (HSTS); HSTS Preloaded

HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers on the client side to use HTTPS on the website to enforce secure communication. The HSTS solution, which is mandatory in all browsers, redirects traffic to HTTPS. If the browser receives an HSTS header in the HTTPS response message during the first access, it is required to use HTTPS for all further communication. The solution is dynamic, as it enforces HTTPS non-bypassability after the first response.

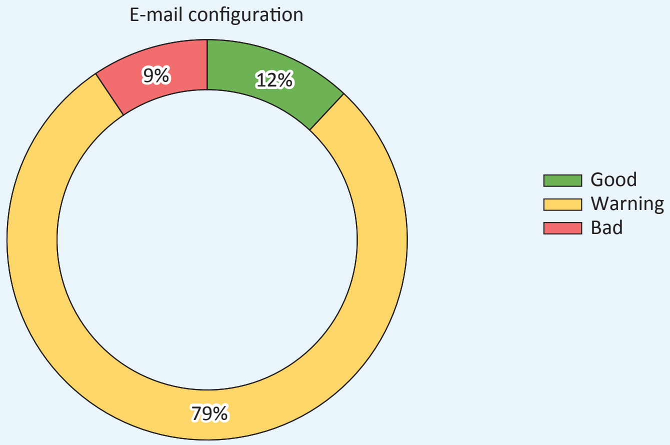
Without HSTS, active network attacks are easier to carry out: an attacker can force the client to send a request to the server via HTTP (without encryption), but this compromises the information sent by the client. Due to its function, HSTS can only be tested for hosts where the service is available via HTTPS. HSTS Preloaded is also a client-side protection mechanism, but here the browser enforces HTTPS based on static content. The gist of the solution is that, based on the list preloaded into the browser, even without HSTS headers, the browser will only attempt to connect to the list items using HTTPS. This means that strict security can be enforced from the first visit on. This approach provides the highest level of security for web communications available today. Both the HSTS and HSTS Preloaded settings can only be tested for hosts where service is available over HTTPS, so the figures do not take into account the 37 percent of domains when presenting the ratios; in other words, the HSTS and HSTS Preloaded figures present ratios for a smaller data set.

The figure shows that 77 percent of institution domains have HSTS configured, while the remaining 23 percent of domains could in principle redirect from HTTPS to HTTP. However, this is only a possibility in principle because the feasibility of circumvention depends heavily on the web application: whether it is really possible to redirect traffic to HTTP can only be explored in a specific experiment. The HSTS Preloaded compliance rate is 34 percent, which means that only 34 percent of domains with HTTPS are registered in the list that that makes HTTPS mandatory (on https://hstspreload.org/).

Adequately configured domains include the institutions' root domains, with which clients also communicate. Where HSTS or HSTS Preloaded is not configured, there may be domains that are used to display, share, or exchange less critical information, or that do not communicate with live data.

E-mail configuration

Figure 34
Aggregated e-mail configuration for the domain data of the entire Pilot Project



The examination of the e-mail configuration is intended to present the e-mail-related security settings of domains.

The evaluation of the e-mail configuration is based on three main properties: the SMTPTLS, SPF, and DMARC parameters, which will be explained in the following sections. Domains with all parameters set were rated “Good”. Domains with SPF or DMARC set as e-mail configuration parameters received the “Warning” rating. Domains where SMTPTLS was not set among the e-mail configuration parameters were rated “Bad”. Thus, the figure shows that 12 percent of institutions had “Good” settings, 79 percent received the “Warning” rating, and 9 percent of institutions had inadequate settings

("Bad"). It is likely that not all domains are used for e-mail communication. Sending e-mail without SPF and DMARC may be a challenge nowadays. Major e-mail providers, such as Gmail, Outlook, AOL, Yahoo, etc., do not accept mail from domains that do not have SPF set. Presumably, on the basis of risk proportionality, the root domains that institutions use for primary contact with customers are set up appropriately.

Figure 35
E-mail configuration settings for the four types of institutions with the largest number of domains

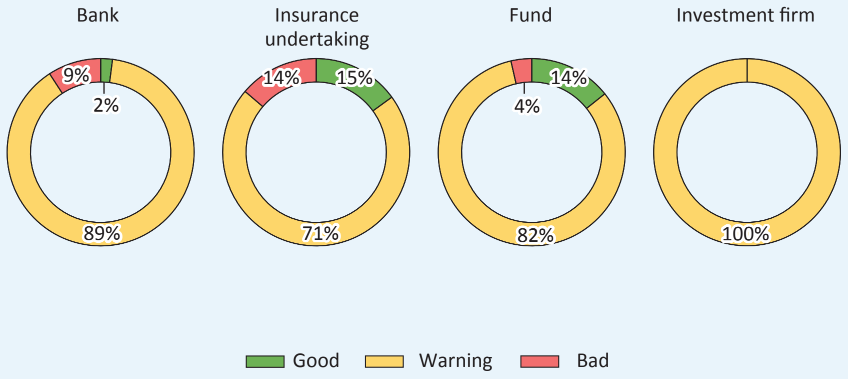
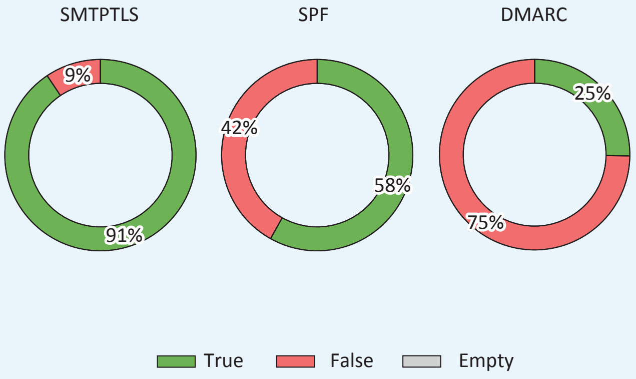


Figure 35 above illustrates the appropriateness the e-mail configuration settings of the four largest types of institutions. The e-mail configuration is evaluated on the basis of SMTPTLS, SPF and DMARC settings. The technical concepts of SMTPTLS, SPF and DMARC will be explained later.

E-mail configurations are almost identical across the types of institutions. The percentage of inadequately configured systems is visibly lower than for web configurations: 9 percent of bank SMTP servers are not properly configured, SMTPTLS is not set up, leaving them vulnerable to man-in-the-middle attacks. The same can be said of 14 percent of insurance undertakings and 4 percent of funds, while no investment companies had poorly configured SMTP servers. Since insurance companies and banks make up more than 60 percent of the total domain list, it is easier for them to have one or two poorly (or partially) configured e-mail servers. The appropriate value ("Good") includes e-mail servers linked to the institutions' default domains, where strict configuration is inevitable for customer interaction. Interestingly, there was no "Good" rating for investment companies, suggesting that the DMARC function is not used by them, so that message authentication and the possibility of feedback on abuse is not always available.

Figure 36
E-mail configuration parameters for the domain data of the entire Pilot Project



SMTPTLS

All host machines receiving e-mail need encryption to ensure the confidentiality and integrity of e-mail messages. One of the simplest solutions is to direct the SMTP stream to TLS, in other words to use SMTP over TLS. Another option is to build up TLS after an already established SMTP connection (STARTTLS). TLS requires a valid certificate for its operation, as described for HTTPS. A working TLS (and SMTPTLS) service requires an asymmetric key pair, a certificate generated from the public key. Certificate validation is not always done in a way that can be traced back to a qualified Certification Authority (CA) service provider, even though this would be expected for completeness. E-mail servers must support SMTPTLS on both the sending and receiving side and must use an appropriate TLS configuration and appropriate certificates. The existence of SMTPTLS can only be checked for domains with SMTP service (MX record) configured. Figure 35 shows that 91 percent of the institutions' domains have SMPTTLS set up and 9 percent do not, according to the August scan results.

SPF

The Sender Policy Framework (SPF) allows institutions to designate servers or other endpoints that are authorised to send e-mail messages on their behalf.

SPF settings are defined in the text field of DNS records. If the SPF is set correctly, spam sources (unauthorised senders) are easier to filter out. The figure shows that 58 percent of the institutions' domains have SPF set up and 42 percent do not, according to the August scan results. It is worth mentioning that the European Central Bank has required central banks to use the SPF for more than a decade.

DKIM

DomainKeys Identified Mail (DKIM) is a method whereby the SMTP server signs the messages it sends with its own private key.

The public key used for validation is located in the DNS text record of the institution, similarly to the information required for SPF. However, while the SPF only lists IP addresses and FQDN hostnames and thus restricts the set of sending hosts on the basis of IP address or FQDN, the public key provided by DKIM also allows for the validation of individual messages.

Hardenize does not specifically examine the functioning of DKIM, but only provides feedback on DMARC compliance.

DMARC

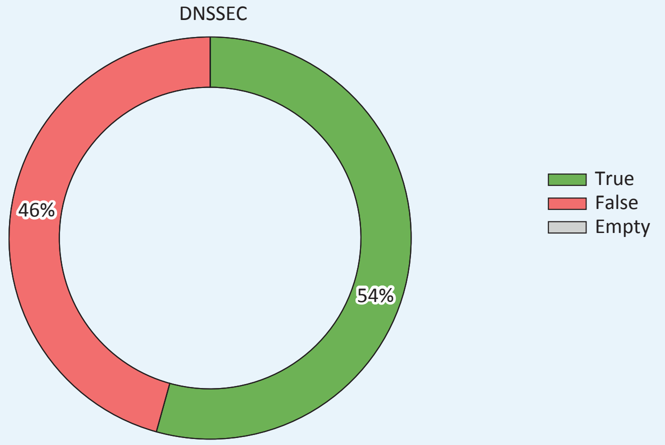
Domain-based Message Authentication, Reporting & Conformance (DMARC) provides institutions with additional options to define policy based rules for e-mail communication, such as how to handle unauthenticated e-mails (not identified using SPF and DKIM), providing feedback to the sending side. The implementation of DMARC has an added value after SPF and DKIM implementation, so it can only be tested for domains with working SPF and DKIM.

The figure shows that 25 percent of institutional domains have DMARC set up and 75 percent do not, according to the August scan results.

3 DNS CONFIGURATION

DNSSEC

Figure 37
DNSSEC configuration for the domain data of the entire Pilot Project



The Domain Name System SECurity extensions (DNSSEC) are an extension to the DNS protocol that provides cryptographic assurance of the authenticity and integrity of DNS response messages. DNSSEC provides protection against network attackers who can manipulate recursive (or caching) DNS servers, preventing victims from being redirected to false sites. The DNSSEC solution works by authenticating DNS responses based on public key cryptography. Authoritative DNS servers electronically sign the transmitted content in the text records, and caching DNS servers or hosts can verify the authenticity of the received information based on the public key stored in the text record of the domain. 54 percent of the institutions' domains have DNSSEC set, 46 percent do not. In the case of domains that are not properly configured, there may be reasons (use for special purposes or internal use by institutions) why the configuration may not be justified.

4 SUMMARY OF CONCLUSIONS FROM THE HARDENIZE DATA

The technical data collection and analysis developed by the SSNS-NCSC was incorporated into the analysis process of the project to compare the incident analysis and threat trends identified during the Pilot Project with the technical data collected by the SSNS-NCSC. Analysis based on individual institutional configuration data shows that there is no clear correlation between the security level of each institution's domain configurations and the incident data of the institutions. Most of the incidents during the Pilot Project were not due to attacks, but could be traced back to operational problems.

Based on the domain data provided by the institutions, the SSNS-NCSC ran a Hardenize scan at the beginning of each month of the Pilot Project. Although we have six months of data on the different domain configuration statuses, only the data from the beginning of August was used in the presentation of the technical data. On the one hand this is explained by the fact that the data for August 2022 represent the most recent technical situation, and on the other hand, we have not seen any significant configuration changes between the different months. Only a very few of the reviewed configuration states changed over the six months of the Pilot Project, indicating that domain related configuration parameters change over a longer time span for financial institutions in general.

Finally, it can be concluded that, although the settings described in Chapter V are not new and have long been an established practice, they do not seem to be a priority in all cases for the institutions under review.

VI Overview of the methodology

In summary, the aim of the Pilot Project was to produce the first threat landscape for the financial sector in Hungary using the data collected during the project, thus supporting decision makers and experts in the sector, and providing up-to-date threat information for all interested professionals. The report could be repeated annually, depending on future opportunities – eventually for the whole financial sector —, identifying current key threat trends and analysing changes in trends. In order to ensure that the report can be consistently repeated annually, a distinct methodological proposal has been developed in the framework of the threat landscape project, which clearly defines the preparatory activities, the execution of the data collection process, and the evaluation criteria.

In addition to the threat landscape methodology, we also defined the information and data that institutions must send to the CBH on the various incidents to ensure that the data received are suitable for the analysis and detection of future threat and incident trends. For the sake of uniform reporting and the subsequent processability of the data, the institutions are required to record the reports in a pre-defined structure, and an electronic incident reporting form has been developed in the framework of the project to support this process. The form provided the possibility to categorise incidents on multiple levels during the Pilot Project.

Of course, the incident data collection methodology developed under the project may be superseded or replaced by reporting obligations and rules deriving from EU legislation (DORA Regulation).

The incident reporting methodology and the methodology used for developing the threat landscape report were validated and tested during a six-month pilot period between February and July 2022.

The first issue we faced in developing the methodology was defining the concept of the incident itself. The current regulatory environment and different IT methodologies and standards have different definitions of this concept, so the broadest possible interpretation was used throughout the project. Accordingly, we collected data on operational incidents and malfunctions as well as cyberattacks. It is anticipated that the DORA Regulation will clarify the definitions, as one of the explicit aims of the regulation is to standardise the incident reporting processes, which will also require changes to the incident reports currently covered by PSD2. During the project, the following definitions were included in the incident reporting guide:

IT security incident: an unforeseen but already identified event that has occurred in the network or information system, regardless of being the result of any malicious activity or not. The incident has the characteristic of compromising the security of the network or information system or adversely affecting the security of the data processed, stored or transmitted therein, or the availability, confidentiality, continuity or authenticity of the financial services provided by the entity concerned.

Critical IT security incident (hereinafter: critical incident): an incident that has an adverse and potentially high impact on the institution’s network and information systems supporting critical functions.

The following incidents are critical in all cases:

- events that attract the attention of the press,
- unauthorised access to personal data of multiple customers involving bank secrets, payment secrets, insurance secrets, securities secrets, or fund secrets (e.g., data leakage, successful phishing),
- unauthorised activity in the IT system (e.g., external or internal fraud) resulting in data modification involving multiple customers,
- services considered critical based on the institution's Business Impact Analysis (BIA), that are expected to be down for more than 1 hour or below normal service levels, with a specific focus on:
    - electronic channels (online sales channels, payment cards, Internet banking and electronic payments),
    - account management in the case of credit institutions, investment companies and investment funds.

In line with the above definition, we did not collect any data on unsuccessful attacks – i.e., attacks that were averted and routinely dealt with – from the institutions participating in the Pilot Project. We considered but rejected the possibility of supplementing the incident data with threat intelligence data, as we already had sufficient data available during the project.

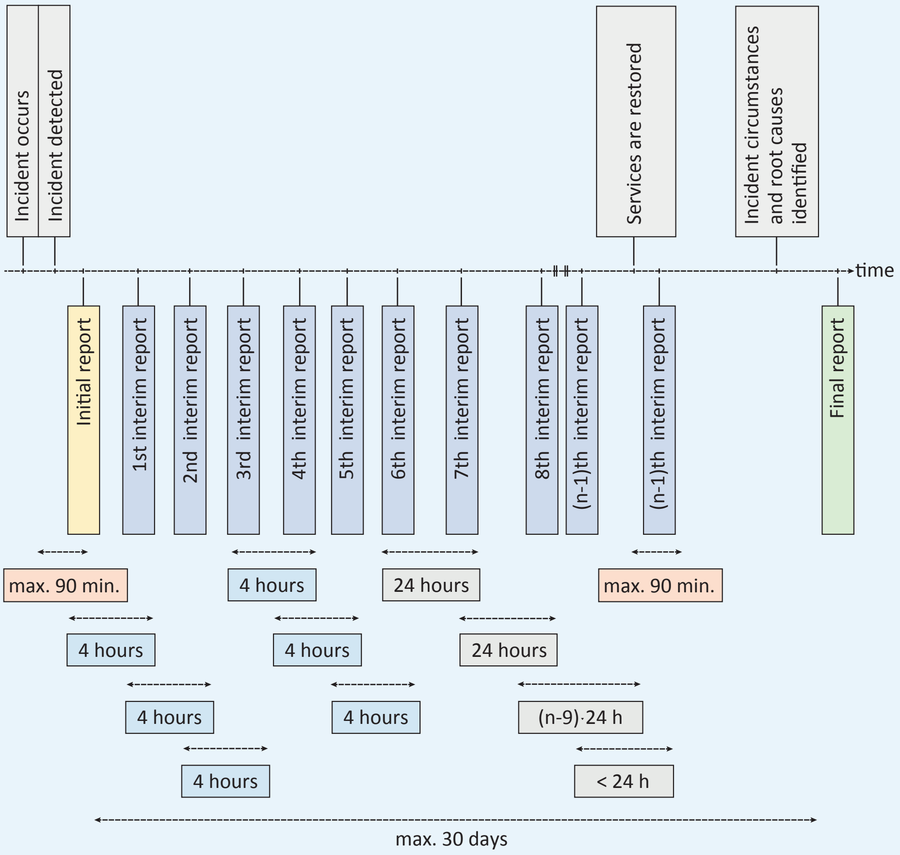
In the framework of the Pilot Project, the participating institutions undertook two types of incident reporting during the data collection period: monthly reports summarising all incidents for the respective month and immediate alerts on critical incidents in addition to the monthly reports.

Monthly reports had to be sent by institutions by the 10th day of the following month, even if there were no incidents in that month. In case of critical incidents, a more detailed reporting and post-incident response process, as described below, was to be followed by the reporting entities. Some institutions enquired about the possibility to automate monthly reporting, and as the Pilot Project has progressed, we have seen indications that some of the incoming monthly reports are automatically generated. The timeframes set for reporting incidents proved to be adequate for all institutions in case of the monthly summaries, with a significant number of institutions being able to send meaningful (not blank) monthly summaries days before the deadline.

The more detailed reports were referred to as alerts in the Pilot Project methodology, as the data received in the project were treated separately from the other regulatory reporting data received by the other CBH, and we wanted to emphasise this at the terminological level. Critical incidents were subject to three levels of alerts: the initial alert, the interim alert(s) and the final alert. There was one, and only one initial and one final alert for each incident. The number of interim alerts could range from 0 to 35, depending on the duration of the incident management.

The schedule for the three-level alerting requirements is presented in the following figure:

Figure 38
Schedule for the three-level alerting obligations



Critical incident alerts were to be sent according to the following schedule:

1. The initial alert had to be sent to the Supervision within 90 minutes from the time the incident was detected. Only one initial alert was required for each critical incident.

2. The institution had to send an interim alert (or alerts) if it was unable to send a final alert within 4 hours. The interim alert(s) (if necessary) had to be sent by the institution until the affected services were restored. Interim alerts were to be sent according to the following schedule:

   a. Every 4 hours for the first 24 hours,

   b. Daily after the first 24 hours (every 24 hours),

   c. The last interim alert must be sent within 90 minutes after the restoration of the affected services.

   d. If there are no more disrupted services and the last interim alert has already been sent, the supervised institution does not need to send any more interim alerts.

3. The final alert had to be provided to the Supervision within 30 days of the initial alert. The supervised institution could send the final alert when:

   a. the services affected have been fully restored and could be used to their full extent,

   b. they had investigated the circumstances of the incident by evaluating reliable sources (logs/records related to the incident), they were already in possession of the information necessary to understand the incident,

   c. the root cause(s) of the incident have been identified.

Only one final alert was required for each critical incident as well.

The following were not conditions for the final alert:

1. Closure of the procesdures of Business Continuity Plans (BCP) and/or Disaster Recovery Plans (DRP) put in place as a result of the incident. If there were still active BCP and/or DRP processes running, the institution could declare this in the final report.

2. Completeness of the incident response. If further actions were needed on the part of the supervised institution, these could be indicated in the final report.

Timeframes for reporting incidents may need to be reviewed in the future. For banks, an initial alert within 90 minutes is a feasible expectation, as they operate on a 24-hour basis to perform payment services related tasks. However, for institutions with no hours of service during nights and weekends, reporting incidents during these periods can be a problem even if the incident response/remediation itself is otherwise ensured.

Interim alerts were sent by a strikingly small number of institutions, typically less frequently than the specified intervals. However, during the Pilot Project, the CBH did not use the available supervisory tools on case of late reporting, so it is expected that compliance with deadlines would also receive more attention from the institutional side in the event of a mandatory incident reporting regulation similar to the Pilot Project being implemented.

Following the Pilot Project, the final phase of the data collection period was the data cleaning, in which all available incident reports were collected and standardised according to uniform criteria and reviewed to identify any discrepancies. In the first iteration of the cyber threat landscape project, for example, a strong emphasis had to be placed on checking the answers in each data field, based on the following:

- Reconciling the given and expected response format (e.g., a number is expected but the response is free text).

- Identification of logical inconsistencies (e.g., an incident must have occurred before or at the same time as its detection) to help ensure the accuracy of the figures.

- Standardisation of data points with the same information content (e.g., the difference between short and full company names).

During the six months of the Pilot Project, there was not a single month in which the automatic processing of all reports without manual data cleansing would be possible.

After the data collection and cleaning phase, the analysis activity was carried out. The analysis used data from critical incidents and monthly summaries to produce figures and comparisons based on pre-defined criteria. The review process involved both quantitative analyses (due to the large amount of incident data available) and qualitative analyses (which looked in more depth at particular issues identified as priorities). The different data points had to be treated and analysed separately by type and source, and correlations had to be established independently.

1 SUMMARY OF CONCLUSIONS FROM THE PILOT PROJECT

There was a certain improvement in the schedule and content of data reporting during the Pilot Project. In the first month (February), the reporting system did not in all cases have associated mature processes on the side of the institutions, and therefore the reports did not always follow the timeline expectations of the Supervision. The content of the reports and alerts also required clarifications or additional information in several cases. That said, analysis of the reported incident data shows that for banks reporting most of the incidents, this development process was completed quickly, with participating banks being able to complete the defined incident reporting process essentially without disruptions.

Depending on the type of institution, as the methodology became increasingly routine, the reporting system also became more and more aligned to expectations. On behalf of the Pilot Project participants, it became clear at the institutional level who is responsible for the availability of the alerts, what content the CBH expects and what deadlines need to be respected. The Pilot Project forms also facilitated the fulfilment of certain supervisory regulatory reporting obligations, e.g. the institutions could also comply with the reporting obligation set out in CBH Circular No 398-5/2015 (hereinafter: IFF alert). The possibility of automatically generating e-mails related to IFF alerts was also provided by the form; however, no institution made use of this possibility during the Pilot Project. Nevertheless, positive feedback was received from participating institutions and IT supervisors that the form facilitated the reporting of incidents in sufficient detail, resulting in fewer additional questions from supervisors. Institutions so far not subject to mandatory incident reporting had the opportunity to to gain experience in the reporting process.

As banks reported a significant proportion of incidents and there was no lag in the number of reported incidents in the initial period, it can be concluded that banks were able to implement the process within a tight timeframe and without major disruptions; hence, a similar process in the future would presumably not pose a major difficulty in this segment. At the same time it is not possible to say with certainty whether the participants reporting the fewest incidents – i.e., insurance brokers and financial undertakings – did indeed not have incidents, or whether incidents were not identified, or if the reporting process was not sufficiently elaborated. Only future, larger sample analyses and targeted data collections can answer this question.

The incident reporting form created during the preparatory phase of the project proved to be adequate, with institutions being clearly able to complete and send it according to the established rules after a shorter or a longer period of time. Feedback suggests that many institutions would welcome the possibility to automate all or as much of the filling in of the form as possible in-house in the future.

The sub-division of the categories that give the background database of the reporting form was critical because the incident reporting process is expected to be fast and efficient, and it is important in the reporting process that the experts involved can categorise incidents as easily as possible. Based on the analysis of the data, the number of incidents categorised as “other” is negligible, so the design of the categories can be considered appropriate overall, but based on institutional feedback, fine-tuning may still be needed.

The notification form was in Excel format, without the use of macros for ease of use, and had to be sent to the CBH as an e-mail attachment. During the project, we considered and rejected the use of the ERA system for CBH data reporting, as neither the availability and lead time of the system nor the range of people having access to it on the institutional side (alerts typically coming from IT security departments, while the ERA system is usually accessed by the reporting service) were in favour of this approach.

In relation to the usability of the reporting form, based on the experience of the Pilot Project, further development of the input validating controls of the data entry fields (institution identifier, date selector, etc.) and further support and assistance for the description of corrective actions and critical alert annexes may be necessary in the future.

Experience gained on the applicability of the methodology confirms that the developed incident reporting process is methodologically sound and can be adequately applied in practice; the developed form helped institutions to provide all the necessary information, thus reducing the number of further clarification questions. Less than 4 percent of incidents were reported in the “other” category, which suggests that the form created for reporting incidents could be adequately interpreted and used in practice by the institutions, while further analysis and classification of this unclassified type of incidents may provide future opportunities for fine-tuning the categories and subcategories. Other fine-tuning options identified include the restructuring of fraud incident reporting, the clarification of data recording on the number of affected customers and the revision of the reporting timeframe for smaller institutions.

It is interesting to note that no correlation was found between the Hardenize data collected by the SSNS-NCSC, which provide information on the correct configuration of the institution's external domains, and the data submitted during the incident reporting, i.e. there was no discernible correlation between the security level achieved by the institutions' externally visible site configurations and the number and type of incidents reported by the given institution.

In view of the future expectations of the DORA Regulation on incident reporting, the feedback from the Pilot Project has provided useful practical experience to the participating institutions in preparing for future expectations, at organisational, decisionmaker, and expert level.

Edward Teller

(15 January 1908 – 9 September 2003)

Hungarian-American nuclear physicist, who made a number of discoveries and pioneering procedural inventions. He participated in the production of the first atomic bomb (1945), then led the development team of the hydrogen bomb, so became known colloquially as “the father of the hydrogen bomb”.

CYBER THREAT LANDSCAPE REPORT OF THE HUNGARIAN FINANCIAL SECTOR 2022

December 2022

Design: Prospektus Kft.

6 Tartu u., Veszprém H-8200

mnb.hu

H-1013 BUDAPEST, KRISZTINA KÖRÚT 55.