ECONOMY AND FINANCE • VOL. 10. ISS. 2 • JUNE 2023 • DOI: 10.33908/EF.2023.2.5

CYBER SECURITY AND ARTIFICIAL INTELLIGENCE

Péter Bagó[1]

ABSTRACT
Cyber security is one of the key challenges in the age of information technology, which is particularly important in the financial sector, where security is key both for customers and institutions. Data protection, fighting fraud and preventing cyber attacks are areas in which artificial intelligence and automated systems can provide significant assistance. The use of AI and machine learning for cybersecurity allows systems to be recovered quickly and effectively after a cyber attack. Using AI algorithms, experts can immediately assess damage and respond to cyber incidents with AI. In the paper the support of cyber protection with artificial intelligence is presented in the finance sector. There are major overlaps with infrastructural protection, individual security levels and proper data protection.

JEL codes: G00, O33, Q55

Keywords: artificial intelligence, cyber defence, finance sector, fintech

1 CYBERSECURITY IN FINANCE

One should make a difference between cybersecurity and its application jointly with artificial intelligence. However, one should give and overview of the security rules of key importance in 2023, which should be observed by all financial service providers.

- Use strong passwords. Every user should use strong passwords for their accounts, which comprise upper and lowercase letters, numbers and special characters and should be of at least eight-character long.
- Two-step authentication Two-step authentication is important for cybersecurity. It means authentication must be verified by using two distinct factors, for instance, a password and an individual code or fingerprint.

1 Bagó, Péter assistant professor, head of department, Corvinus University of Budapest, Institute of Enterprise and Innovation, Department of Innovation and Business Incubation E-mail: peter.bago@uni-corvinus.hu.

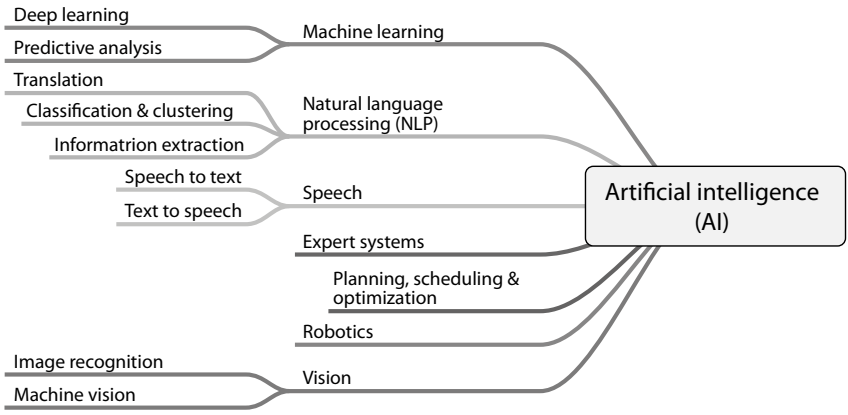
- Software updates All software updates must be installed so that your computer and data should be safe.
- Firewall and virus protection Firewalls and virus protection should be installed on computers to prevent intrusion by malware.
- Backup systems Regular security backup of data is important to ensure data are preserved in a potential data loss or damage.
- User training Employees must be trained and informed about cybersecurity risks and proper security practice for organisational security.
- Permanent monitoring Permanent monitoring of cybersecurity is important for timely detection of any threats and proper response.

To see how artificial intelligence can help the finance sector, the list is much longer but it also touches upon basic issues of infrastructure.

- Detection and response AI systems can collect and analyse large amounts of data for system security. In addition, they can identify threats traditional security systems would easily overlook and will send an alarm to the relevant personnel.
- Reporting AI can draft reports helping cybersecurity teams better understand the vulnerability of systems or reveal the areas that need particular attention.
- Automated response Automated responses can be generated with AI that can manage security threats immediately. For instance, if a security incident occurs, an AI system can automatically change passwords, disable accounts, or withdraw access rights.
- Ongoing learning and updates AI algorithms learn from previous experience and are updated continually with the latest cybersecurity-related information. This allows them to be always up to date and to respond to the newest challenges properly.
- Network security AI can supervise, identify, and analyse the total network traffic to identify potential threats, which could be easily overlooked otherwise. In addition, AI systems can monitor networks and control security levels continually.
- Comprehensive analysis AI can compare enormous amounts of data and analyse them within the system. It can detect anomalies in the system, which cannot be identified or can only be identified with difficulty using traditional security systems.
- Detect phishing AI can detect phishing attacks, it can identify phoney e-mails, websites and applications to help enterprises in secure data management.

- Cloud-based security solutions Using AI and cloud-based technologies, enterprises can improve their security solutions, since cloud-based systems can manage big data more efficiently and can respond immediately in a potential security incident.
- Intelligent network protection Using AI in network protection allows users to detect and prevent cyber attacks. Intelligent network protection can automatically identify and stop cyber attacks and allows continual monitoring of the network and quick response to security incidents.
- Higher level authentication Using AI, enterprises can strengthen authentication through identification and authentication solutions. Face and voice recognition, the application of biometric data and other innovative solutions will make user identification and authentication easier, more efficient and increase security.
- Faster and more efficient response AI allows faster and more efficient response to security incidents. Automated incident and security incident management systems can make an immediate report of the incident and allow fast intervention and troubleshooting reducing harmful effects in that way.

Figure 1
Evolution of artificial intelligence



Source: Ray, 2022

Cybersecurity is extremely important in the finance sector because of the sensitivity and confidentiality of financial data. Analysts have found over the past few years that using artificial intelligence is gaining popularity and many financial institutions enhance their cybersecurity through using AI. The opportunities of-

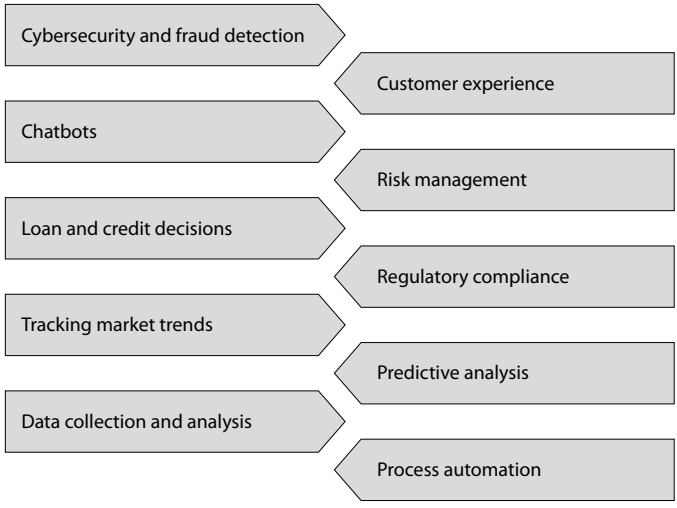
fered by AI may transform the landscape of cybersecurity in the finance sector. AI can be used to analyse enormous amounts of data, which will detect anomalies and patterns indicating cyber threats. Algorithms of machine learning help recognise patterns of behaviour indicating fraud, for instance, fishing attacks, ransomware attacks or identity fraud. AI can be applied to boost the speed and improve the accuracy of detecting threats and responding. Traditional cybersecurity systems rely on rule-based algorithms that are pre-programmed to detect actual threats. However, such systems can be easily bypassed by attackers using new developing technologies. AI-based cybersecurity systems can adapt to and learn from new threats, which makes the detection and mitigation of cyberthreats more effective. What is more, AI-based security systems can provide financial institutions with information about threats in real time allowing fast response. AI can be used to automate security tasks, which means freeing cybersecurity experts to perform more complex tasks that require human knowledge. The use of AI also causes worries from the aspect of financial institutions. One of the biggest worries is the reliability of AI connected with issues of responsibility. AI systems run on data fed into them earlier, and if those data are corrupt or incorrect, AI cannot operate well. The use of AI in cybersecurity includes the application of proper measures of data protection. Financial institutions must ensure the protection of the data managed by AI and user rights and access to data must be strictly controlled. AI-based cybersecurity systems can identify threats and can troubleshoot immediately and effectively mitigating risks and losses for financial institutions. Using AI to identify threats faster and more accurately, cybersecurity experts can save time and energy, which allows them to focus on other tasks. To sum up, AI offers major advantages in the field of cybersecurity in the finance sector. Financial institutions can identify risks with the help of AI and eliminate them quickly and efficiently mitigating losses and improving customer experience in financial institutions. The application of AI, however, necessitates strict measures of data protection and liability insurance to guarantee the security of financial institutions and their customers.

Algorithms can process and learn from data via machine learning, which allows automation and increases effectiveness. Artificial intelligence allows the intelligent use of the data generated by machine learning in decision making processes and can reach the level of human intelligence in finance. To sum up, both technologies have an important part to play in finance and, used jointly, can render data analysis and processing more effective and profitable in the field of financial services (Ray, 2022; *Pintér*, 2008).

Next, *Figure 2* presents five main categories of AI applications in the banking sector.

- The *first category* includes chatbots and virtual assistants that provide bank customers with personalised services from the management of shopping to money transfers.
- The *second category* introduces anti-fraud AI technologies that can help identify and mitigate the risk of rip-offs and fraud.
- One can find automated decision-making systems in the *third category* that can help banks to manage big data more efficiently and to prepare forecasts for business decisions.
- The *fourth category* is robot authentication. Its purpose is to save human labour and to improve the effectiveness of processes.
- The *fifth* and last *category* is that of AI-based detection technologies, for instance, face and fingerprint identification that can improve authentication processes and the safety of banking transactions.

Figure 2
AI technologies applied in banking



Source: Appinventive, 2023

Customer service for banks is one of the key application areas of AI. Banks use chatbots and voice assistants to provide 24/7 customer support and assistance. Those virtual assistants operate on AI and natural language processing (NLP) technology, which allows them to understand customers' questions and give relevant answers. This will not only improve customer satisfaction but also reduce the

workload of customer service staff. Banks use AI-based algorithms to detect and mitigate diverse types of risks, for instance, credit risk, market risk or operational risk. AI algorithms can identify patterns and anomalies indicating potential risk by analysing enormous amounts of data. It helps banks make informed decisions and reduce losses. Further, AI is also used to detect fraud in the banking sector. AI-based fraud detection systems can analyse enormous amounts of transactional data in real time, so they can detect suspicious activities. This can help banks detect fraud early on and prevent losses. AI is also used for securities market forecasts. AI algorithms can provide forecasts on securities prices and other market indicators based on the market data analysed. This can help investors make better informed decisions regarding the management of their portfolios.

1.1 Cybersecurity trends

Cybersecurity faces diverse challenges one of them being the protection of personal data and data security. AI works by analysing enormous amounts of data including personal data. Therefore, banks and financial institutions must ensure data protection and data security in AI applications. AI is becoming a key player in the process of digital transformation. Its advantages such as efficiency and improved risk management help banks implement new digital technologies and improve customer experience. AI provides banks with major advantage including efficiency and improved risk management as well as customer experience. On the other hand, the challenges posed by AI and its impact on human labour must also be managed if you wish to implement AI successfully in the banking sector (Appinventiv, 2023).

Further research supports that cyber attacks are increasing, particularly those targeting companies and government bodies. Automated and refined cyber attacks such as AI-based attacks are expected to increase in 2023. A study by Deloitte emphasises how important threat management, incident management, data protection and cybersecurity education of the staff are for enterprises to establish and implement productive cybersecurity strategies. In addition, the study goes into details about the changes of legislation and regulations as well as business and technology trends that may have an impact on the environment of cybersecurity in 2023 (Deloitte, 2023). McAfee also believe cyber attacks are going to continue particularly in manufacturing, education, and healthcare. The spread of recent technologies such as IoT (Internet of Things) tools and 5G networks will present new security challenges. The threats mentioned include AI and machine learning-based attacks, manipulation on social media networks and further growth of ransomware attacks. McAfee discuss the importance of initiative-taking cybersecurity measures implemented by organisations based on forecasts including

stronger identification, education, and the improvement of incident management skills to ensure successful defence. They also emphasise the importance of cooperation and the exchange of information between organisations to ensure effective prevention and provide prompt response (McAfee, 2023).

Accenture (2023) believe banks, in general, provide better defence against external attacks but their level of preparedness to manage internal threats is lower. According to their study (Accenture, 2023), the protection of data and defence against unauthorised access continue to be the primary challenges for banks.

The whole finance sector is affected. Allianz publish an "Allianz Risk Barometer" report every year, in which "business interruption" is the most dangerous incident. Denial of service attacks are, in principle, in that category too, so this is just an approach of current attacks from another perspective.

On the other hand, the Allianz report indicates attacks do not only focus on banks but also on the whole finance sector (Allianz, 2023). According to Cyberedge (2023), data protection and security regulations are going to be stricter in 2023 particularly in the European Union where the basic regulation on data protection (GDPR) will continue to affect the business sector. The importance of data protection will continue to increase, and enterprises will have to implement stricter defence measures to counter data loss, phishing, and other types of cyber attacks.

Cyberedge underline that smart tools and the internet of things (IoT) may present significant security challenge in 2023. As smart homes, and industrial and healthcare IoT tools gain momentum, attackers will also use them more often to conduct targeted cyber-attacks. Home office is expected to remain a popular form of work applied widely in 2023, but its security risks continue to be there, so organisations may face increased costs to improve the security of tools used in home office (Cyberedge, 2023).

Studies indicate people, or more exactly, employees, rather than the systems are in the focus of the attacks. Think of attacks compromising emails or cloud subscriptions (Proofpoint, 2023). A study by ESET follows the same train of thought. According to them, cybersecurity trends in 2023 can create a blurred borderline in our brave new world; it can generate complex problems for data security and the protection of privacy while work and social life tend to be connected more (ESET, 2023). According to TÜV SÜD, cost effective cybersecurity solutions are of key importance as well as the start of regulation via the standardisation of digital confidence, while training tailored to target groups and critical infrastructure (KRITIS) are in focus (TÜV, 2023). According to *Paula Januszkiewicz*, cybersecurity expert with Microsoft, the most significant changes affecting cybersecurity in 2023 will be abound preparedness to counter threats. Organisations must be continually ready to face an attack, an effort of intrusion, and must possess the

tools used to keep them under control. Strict control of privileged access, and user identification will be other key topics of the year (Microsoft. 2023).

2 MONEY LAUNDERING AND ARTIFICIAL INTELLIGENCE

Money laundering has a devastating effect on global finance. The International Monetary Fund (IMF) estimate the money laundered in the world at approximately USD 2 to 5 trillion annually. It means money laundering measures higher than any other financial fraud including tax dodging or securities manipulation. Thus, if artificial intelligence can save a fraction of the above value, governments, organisations, companies and individuals can achieve crime prevention to such an extent that proves it is worth special attention. The connection between cyber-defence and money laundering is that money launderers often apply cyber attacks, computer fraud and other methods of cybercrime to hide laundered money and to prevent their identification. They, for instance, often use fake websites or computer programmes to acquire banking data, customer identifiers or transactions. Then, they can use those data to open fake accounts, transfer money or other methods of money laundering. Cyber-defence, therefore, is key in the fight against money laundering. Banks and other financial institutions must apply strict security measures to protect personal and financial data. They must also prepare for cybercrime and the related money laundering. Countries having ambitious standards of cyber-defence are at an advantage in detecting and preventing money laundering and other financial crimes. That is why education on, and development of cyber-defence are important to mitigate the risk of cybercrime and money laundering.

According to a study by McKinsey (*Biswas* et al., 2020), AI allows banks to make their business processes more efficient and effective, to improve their product and service portfolios and to boost customer satisfaction. The use of AI is advantageous to banks for many reasons, for instance, improving their customer service, increasing the efficiency of risk management, supervising transactions, and preventing fraud. The analysis underlines further development of AI can help banks make prompt decisions in the field of supervising transactions and risk management. Further, AI allows banks to offer their customers tailor-made products and services. The analysis also states banks must promote the spread of using AI in their organisation and ensure the necessary resources, technological skills and expert knowledge are available. In addition, banks must face further challenges, such as protection of personal data and the legislative environment. According to the analysis, the use of AI requires a comprehensive strategic approach by the banks, which allows that AI systems are integrated into the business processes,

that applications are widely used and that the development and operational costs of AI are optimised. The use of AI systems and technologies will have a major effect on banks and their customers. Banks that can use AI properly will have a long-term competitive advantage and will be more successful on the market. The article concludes AI solutions play an important part in the future of financial service providers, since they can make banking processes more effective and customer friendly. Financial institutions using AI can evaluate risks more accurately and effectively, they can improve through-time and customer service. However, the article also points out the implementation of AI does present major challenges, for instance, the issues of data protection and security as well as training and investment into innovative technologies. According to the article, financial service providers must prepare for both the challenges and opportunities offered by AI solutions to be successful in future.

2.1 What is money laundering?

Money laundering is a criminal act during which money of illegal origin is transformed into money seemingly coming from a legitimate source. The process of hiding the traces of illegitimate money is important so that its source and path cannot be traced back. The process of money laundering means screening the source of profit made on illegal activities. This crime is a major threat to the economy and the society since money laundering can contribute to financing terrorism or other criminal acts. So, the relevant authorities and financial institutions should pay attention and prevent money laundering by applying suitable regulations and measures (Wolters, 2018).

A three-phase model displays the process of money laundering, which demonstrates how to achieve clear traceability of the origins of money, i.e., the way to legalise money. The model originates in the US. Process steps are the following:

- Placement/depositing
- Layering,
- Integration (*Gál*, 2007).

In the first step, the money to be laundered, which is typically cash, is deposited in the financial system in some form. Banks are typical targets. These days the global financial sector has been prepared for this step. The appearance of substantial amounts of cash is an indicator and sign of danger. The most important thing to do then is to find the origin of the money in a way that can verify in a credible way the origin of the amount to be deposited in the bank. In some cases, you can see a sales agreement, severance pay or family inheritance.

The second step of the process is layering. It means complex transactions are performed involving more than one account or more than one customer. The transactions typically affect accounts managed by different banks, they may be in different currencies and in different countries. It is all the better if they lead to countries you can only obtain banking information from with difficulty. The process is important because if you want to retrace those transfers, you will meet obstacles and sometimes it is next to impossible to find the source. You can ask customers for information on one or another transaction, but you may need international collaboration to decompile the whole chain. On the other hand, if you only look at a small section of the transfers, you can only see a customer performing a transfer to another customer, which can be of an average size. If you want information about the background of the transfer, they will be happy to answer or to show invoices or contracts. At that point, the prevention of money laundering is difficult.

The third step following deposit and layering is integration. It means the amounts having run through different accounts are withdrawn or invested. It is, in fact, the step where it is posted as clean income, or the customer uses the money for a major investment. Its source can be said to be clean as there is nothing to prove the opposite. For example, when an accountant books money added as extra income over a month or two. Sometimes, the process is closed with cash withdrawn and taxes paid, which promote the illusion of legality. These days customers often withdraw the amount they need in small portions subject to the maximum capacity of cash machines. They will do what they can to avoid a visit to the bank branch, because they can meet there a person dangerous to them: the bank officer who, as the first line of defence to prevent money laundering, will be curious to get information about the amount. For the same reason, automatic paying-in and deposit machines are highly popular. Banks, naturally, must prepare for this, and must monitor them subject to filtering in compliance with their procedure.

Warning signs are easy to be seen in the above process. The best opportunity to block the process is at the first step, when cash is deposited. The end of the process in most cases is a cash withdrawal or high-value investment - another cash transaction. Investigating the origin of the transactions and their purpose should be part of the prevention of money laundering. To sum up, one can say that exceptionally large cash movements are the best indicator of money laundering.

2.2 Monitoring or filtering?

It is obvious from the above that monitoring as many customers and checking as many transactions as you can is necessary.

"Section 33:

In the application of this subsection 1, automatic filter system: an IT system suitable for sorting out the customer and the transaction from the point of view of money laundering and terrorist financing based on prior parameterization and not requiring human intervention".[2]

The provision cited above proves that service providers are obliged to apply a filtering system to support their activities preventing money laundering and generating signals with no human intervention. Here, difference must be made between monitoring and filtering.

A monitoring system is suitable for subsequent, post-monitoring activity. In that case, it will check completed transactions subsequently based on pre-set rules or scenarios. In practice it means that customer transactions are continually loaded into the monitoring system, which will filter them and generate signals or warning according to the pre-set rules. Such a system is not artificial intelligence by itself that would unambiguously tell you what money laundering is and what is not. However, the more accurate your settings and rule definitions are, the more accurate the filtering results will be and the more probable it will be that such an alarm is real. The only drawback of it is that a set of rules of such depth cannot operate in real time, when you only have a few seconds to perform a transfer. As shown in the above example, the problem arises because a transaction can have travelled a number of accounts or countries by the time an investigation is conducted. MNB has decided 30 or 20 workdays are available to investigate an alarm.

The operation of filtering is different as its task is to filter traffic in real time. With respect to international traffic, it is also expected to filter for sanctions. Such transfers are released in several cycles every day. Should the system find any simi-

2 26/2020-as (VIII.25.) MNB rendelet a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól [MNB Decree on the implementation of the Act on the Prevention and Suppression of Money Laundering and the Financing of Terrorism for service providers supervised by MNB and on the development of a filtering system according to the Act on the Implementation of of Financial and Property Restrictive Measures ordered by the European Union and the UN Security Council and about the detailed rules of the minimum requirements for its operation, 26/2020 (VIII.25.)]. (https://net.jogtar.hu/jogszabaly?docid=a2000026.mnb).

larity with a sanctioned entity, an alarm is generated, and the transaction will be continued or rejected subject to analysis. In this way both incoming and outgoing transfers can be filtered.

The filtering system typically looks for character match in sanctions list, while monitoring examines pre-defined parameters. A filtering system will not only look for suspicious transactions but also suspicious customers. A monitoring system will detect suspicious transactions based on a pre-set rule. The operation and the task of the two systems can be easily compared in a table:

Table 1
Categories of filtering systems

	Legal provision	
	Law LII of 2017	**Law LIII of 2017**
Task	Filter and block customers and transactions subject to sanctions	Detect peculiarity indicating money laundering
Data source	Sanctions lists	Archived historical data
Methodology	Comparison (character match)	Detect peculiarities by pre-defined parameters
Measure	Stop suspicious customers and transactions, take measures	Filter and check suspicious transactions, take measures
Time scale	Real time, built into process	Subsequent, not real time

Source: based on Lukács (2022)

Hungarian and international regulations are much broader than what is presented in this paper and discussing them is not part of our topic. With respect to the main topic, you can see some rules will have to be established for the monitoring system so that the traffic of cryptocurrencies become visible.

2.3 Authority report

In compliance with Law LIII of 2017 on the prevention and suppression of money laundering and terrorism financing, service providers shall:

"**Section 30** (1) * The manager, employee and supporting family member of the service provider

a) for money laundering,

b) to finance terrorism, or

c) for the derivation of a thing from a punishable act

in the event of any indicative data, fact, or circumstance (hereafter referred to as: data, fact, or circumstance on which the report is based) arises, the person specified in Section 31, Paragraph (1) must immediately make a written report (hereafter referred to as the report).

(2) The notification specified in paragraph (1) must contain the data recorded

a) by the service provider according to 7-14/A

b) a detailed description of the data, facts, and circumstances on which the notification is based and

c) documents supporting the data, facts, and circumstances on which the notification is based if they are available.

(3) The manager, employee and supporting family member of the service provider shall report the emergence of data, facts and circumstances indicating money laundering, financing of terrorism or the derivation of a thing from a punishable act in the case of executed or to be executed transactions and transactions initiated by the customer but not executed. It is also obligated to investigate in the case specified in paragraph (8) of Section 13."

The above provisions define primarily what an authority report exactly is. If a service provider thinks they detect some suspicious circumstance in the case of the above filtering systems, they shall make a written report in compliance with c). The above quote does not identify for whom the report is meant. All notifications shall be addressed to the National Tax and Customs Administration, Hungarian Financial Intelligence Unit (NAV PEI). The law requires that a complete investigative file must be sent including all information available to the service provider immediately as they detect suspicious activity, i.e., without delay. It is a question what exactly NAV PEI does with those notifications since service providers have no feedback in most cases. NAV PEI sometimes send a letter informing the service provider with reference to the identifier or the notification that the authority "has successfully used" their report, whatever that means. NAV PEI does have connections with international anti-money laundering authorities, so they can not only investigate in this country but also internationally. It is, naturally, also true from the other side, i.e., NAV PEI receive requests by international authorities they must answer or participate in investigations in progress.

Natural persons, self-employed entrepreneurs or corporate customers can also comply with the obligation to report a claim. The expected minimum data content is the following – more information can be sent but not less. It depends if all of them are available, but efforts must be made to have them:

- the transaction,
- the suspicious circumstance described in detail,

- related partners,
- public company information,
- indication by partner bank if any
- message withdrawing the transaction if any
- document certifying source of transaction.

Authority notifications are of key importance. This is to advise the authority to investigate a customer engaged in an activity found suspicious. The more sophisticated filters and workflows are established by a service provider, the more difficult money laundering will be with them. The more sophisticated risk sensitivity a service provider has, the more in-depth analyses they can perform in their own filtering system (in an optimal case) or with the help of supplementary reports and information. Then they must forward the information obtained to NAV PEI without delay, that will either agree with the suspicion and launch proceedings or say thank you for the warning and close the investigation. Service providers can only report suspicion, but they are not authorised to decide if the act was illegal (NAV, 2022).

3 THREATS IN THE EUROPEAN UNION

The financial sector must face the following threats in the EU including Hungary, which is published by the European Union Agency for Cybersecurity (ENISA) in its annual reports:

1. Ransomware
2. Malware
3. Social engineering threats
4. Threats against data
5. Threats against availability: Denial of service
6. Threats against availability: Internet threats
7. Disinformation - misinformation
8. Supply-chain attacks

Reading the 2022 list, you can notice that the old technique of social engineering threats have "catapulted" to place three; they had not been there on the ENISA list in 2021. More accurately, you can say crypto-jacking swapped places with social engineering threats. It means two things. One is that the exchange rate of crypto-currencies fell to a fraction about a year ago, so interest in them has also declined. Covid might be the other reason, i.e., people's approach has changed, so social

engineering has gained momentum. According to antivirus manufacturer ESET, spam and phishing are the two leading methods of social engineering (ESET, 2022). Social engineering includes many more techniques, some of which have hardly anything to do with IT, such as baiting when a criminal offers a reward in return for information (Terranova, 2022). It should be noted that Kevin Mitnick, one of the most famous hackers in the world, found his way into computer systems using social engineering, persuasion. (Mitnick, 2022).

Attacks against financial institutions and services use increasingly sophisticated methods and a range of solutions. In Hungary, the National Cyber Defence Institute (NBSZ-NKI) monitor and manage attacks, but unfortunately they do not share detailed information with the public. They will only say in their weekly newsletters what the given level of threats is, for instance, the threat level of ransomware was medium in week 50 of 2022 (NBSZ, 2022). MNB, on the other hand, do publish more accurate data obtained from NBSZ-NKI, which can be read in numerical form. Twenty-one threats were followed in the period from 1 February to 31 July 2022. However, no details are available, for instance, you will not learn how those attacks ended, whether they were successful, which organisation was attacked, for instance, a bank, a financial institution or a fintech company (MNB, 2022). All that is an indication that such attacks are present in Hungary too. The statistics show the authority learn about 4 to 5 such attacks every month. The above report included information from all the authorities taking part in the defence, i.e., MNB was aware about 765 incidents in the five months mentioned, which supposes activities of a worrying size.

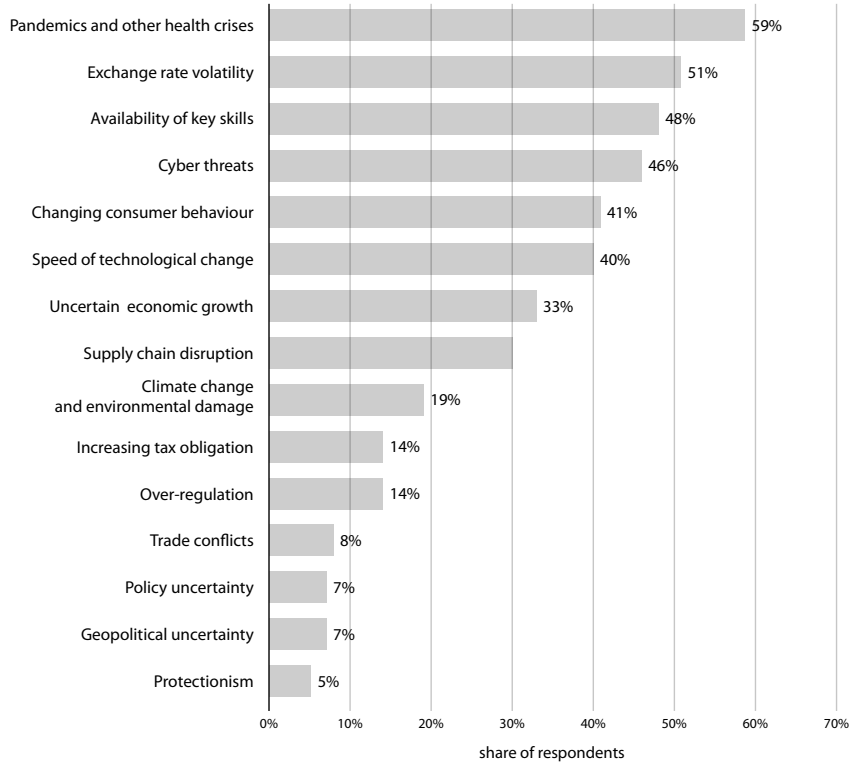
In addition to the ENISA reports mentioned above, the EU also is also engaged in the following areas:

- Measures responding to cybersecurity challenges
- Cyber resilience
- Fight against cybercrime
- Increased cyber diplomacy
- Cybersecurity collaboration
- Funding and research
- Cybersecurity of critical infrastructure (ET, 2023)

3.1 Companies and cybersecurity

It is worth looking into how companies think about the topic. The following is a figure presenting threats built into the core activities of companies. As you can see, about half of the companies are aware of online threats:

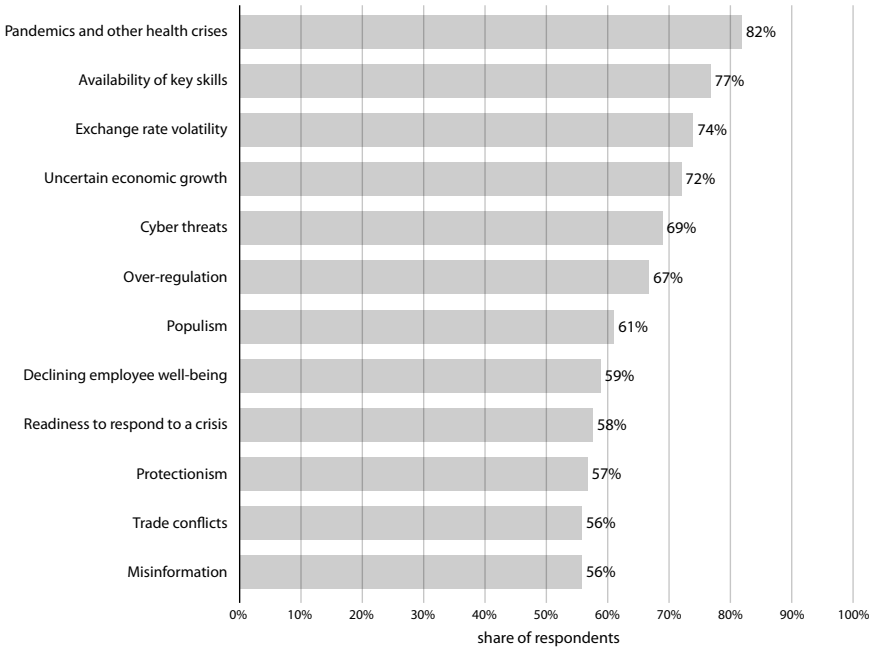
Figure 3
Company threats in Hungary in 2021



Source: Statista, 2022a

The next figure is more emphatic about the importance of managing threats; almost two-third of company executives believe such threats may affect company growth:

Figure 4
Risk of company growth acknowledged by company executives



Source: Statista, 2022b

Customer cloud services expand all the time. The advantages they offer are extremely important for financial service providers. Customer clouds, however, are not simple distribution channels but basic building blocks of customer relations. The appearance of such services and technologies is a challenge for financial service providers since customer clouds keep penetrating new areas in financial services.

McKinsey & Company advisors propose the introduction of AI banks to exploit the opportunities of customer clouds and to make customer relations more effective. AI banks offer the advantage of easier access to financial services for customers, improved digital experience and the elimination of lengthy and clumsy administration at bank branches customers often experience. AI banks, however, are not only instruments to improve customer experience and easier access to financial services. They can also help financial institutions automate business processes, which may result in cost reduction eventually. AI banks can automate customer service queries, they can answer them faster and more accurately, and can

analyse them, which allows better understanding of customer needs by customer service and marketing staff. The use of AI banks is not only important because of customer clouds or the automation of customer service processes. AI banks allow financial institutions to make tailor-made offers by analysing customer behaviour, which respond to customer needs and preferences. As mentioned above, AI banks must ensure proper data protection and the protection of personal data. Still, the advantages of AI are bigger than its potential risks. AI allows banks to offer their customers tailor-made customer service, to improve their channels and customer retainment. The use of AI leads to understanding and optimising customers' digital journeys. AI applications will have a major impact on the finance sector and the banks that refuse to apply them will be at a disadvantage compared to their competitors. The opportunities of AI are inexhaustible. Banks must be prepared to use AI in their business. AI banks will be the ones that can apply AI and the latest technologies servicing customer needs.

Shortcomings in compliance with the rules are a risk, which may result in grave issues, such as fines or loss of company reputation (*Deutsch*–Pintér, 2018). However, attractive opportunities arise for the financial and banking sector if those risks are professionally managed. Data protection and supervision of compliance are increasingly necessary in the banking sector. Regulations on data protection get stricter step by step in banking, which is a new challenge for participants. Observing the rules, however, is not only mandatory but it also offers an opportunity for the sector to improve competitiveness. The article cited also mentions that, in addition to observing the rules, it is also important that the processes of data protection and compliance risk are implemented and maintained effectively. This means those involved must pay attention to effectively manage compliance control and data protection issues. Finally, the article underlines the new opportunities offered to finance and banking for a more effective management of data protection and compliance risks. Data analysis and automation allow stakeholders to manage data protection regulations and compliance risks more effectively. Automated tools and AI can help risk management and improve effectiveness in the sector. Such tools can analyse data and identify anomalies, which allows bank to recognise risk earlier and take the necessary steps to prevent them. In addition, automated processes reduce the possibility of human error, which is an additional advantage for the financial sector.

In finance, the challenges and risks of compliance can be managed with modern technologies including AI and automation. But banks must continue to remain watchful in a changing legal environment and must update and improve their compliance programmes to meet requirements and minimise risks (*Quereshi*, 2019).

Data and the consequences drawn from them are important in the financial sector from the aspect of business growth and success. The traditional methods of data analysis are often limited and do not provide sufficient information. The use of AI and ML can revolutionise the processes of data analysis assisting financial organisations in improving business performance and raising customer satisfaction. AI and ML can collect and interpret vast amounts of data. The automation of data analysis can reduce the risk of human error and improve efficiency. Such technologies allow data to be analysed faster and more accurately, which can help financial enterprises make decision making more effective. The use of AI and ML, in addition, allows that forecasts and trends are analysed more accurately, which helps financial enterprises establish their business strategies. Such technologies allow to prepare personalised offers, which can boost customer satisfaction and loyalty. The use of AI and ML, however, presents challenges too. Financial enterprises must guarantee data protection and data security as well as the ethical application of the technologies.

Compliance with data protection rules and legal provisions is key particularly in the case of financial services. On the other hand, using AI and ML can provide a solution for more efficient data management and improved business processes. Financial enterprises must find the correct balance between technological advantages and risks to achieve the best result for their customers and to improve their competitive edge (*Qureshi,* 2019).

The opportunities of using AI and ML are clear and offer the sector competitive advantage to apply a new approach by implementing and using the new technologies. AI and ML applications provide better efficiency, increased customer satisfaction and higher security for banking and financial services by improving business processes. On the other hand, the successful implementation and use of AI and ML applications are not simple; the enterprises must understand their advantages and limitations and must prepare for their implementation and application. If, however, the enterprises apply those technologies successfully, they can enjoy major advantage on the market and will comply with the strict requirements set by regulators and customers alike (*Narayanan*, 2019).

4 RELATIONSHIP OF OPEN BANKING AND ARTIFICIAL INTELLIGENCE

Open Banking and AI are closely related, since both technologies allow better management of financial services and products offering their customers personalised services and products. Open Banking means that banks share users' banking data with third party applications approved by the customers. By means of such applications, customers can manage their accounts and other financial products on a single interface making finance management simpler. AI can help banks and applications in that regard providing more efficient data management, analysis and use so that the banks can offer their customers personalised services. AI can be useful in many areas of Open Banking, for instance, the optimisation of customer services, transaction analysis and prevention of financial offences. AI can assist banks in their fight against money laundering and fraud by detecting anomalies in transactions and account management.

One should keep in mind that GDPR and PSD2 are both directives related to financial services. The objective of GDPR is the protection of personal data while PSD2 is aimed at improving the security and efficiency of financial transactions. However, those directives can be contradictory. PSD2 - Payment Services Directive 2 - is an EU Directive regulating financial services, which allows customers to share their financial data with third party applications. Its objective was to boost competition on the market of financial services and to promote innovation in the industry (Pintér, 2022).

The part AI plays in PSD2 is a more efficient analysis and management of data. AI can analyse substantial amounts of data and identify customers' needs and habits. This allows banks and applications to offer their customers personalised services and to have a better understanding of the money market. The use of AI in PSD2 can also help in the fight against financial fraud and money laundering. AI can identify customers in connection with whom the probability of fraud or money laundering is high, so it can warn banks to take the necessary measures. Using AI, banks and applications can identify customers whose transactions differ from standard financial behaviour and can warn banks to check those transactions. AI can identify customers' queries and problems and provide immediate answer with the help of chatbots and other automated solutions. This allows banks and applications to manage customer-related enquires and problems more effectively and faster. To sum up, the use of AI in PSD2 allows banks and applications to manage customers' financial data more effectively and to have better understanding of their customers' needs and habits.

4.1 Threat or opportunity?

The use of AI in Open Banking is both a threat and an opportunity for financial service providers depending upon its utilisation. AI in Open Banking allows banks and fintech companies to gain better understanding of customers' financial needs and habits. On the other hand, AI in Open Banking can be a threat if customers' financial data are not managed properly. A fault in an AI device or a programming error can result in the violation of data protection and can increase the risk of access by cyber-criminals. Unauthorised access to customer data must be prevented to properly protect customers' data for maintaining trust and observing legal rules. So, using AI is an opportunity for providing more efficient and personalised financial services and products in Open Banking, but it requires special attention from the aspects of data protection and security. Banks and fintech enterprises must apply proper measures of data protection and security to guarantee that their customers' financial data can be managed safely.

The connection between GDPR (general data protection regulation) and artificial intelligence is an important topic from the aspect of data protection and the management of personal data. The objective of GDPR is to provide protection when the personal data of EU citizens are managed, while AI is a technology that allows the analysis and use of data.

The use of AI presents challenges of data protection from the aspect of GDPR. Data must be processed for AI and customers' agreement and data protection are key during data collection and storage. GDPR rules include the obligation of storing and protecting data securely and the right of access to personal data. Personal data must be managed in compliance with data protection regulations. The use of AI offers many advantages from the aspect of data protection. AI can protect personal data and can analyse data more accurately, which improves security and data protection. AI provides customers with more personalised services and products, which promotes customers' trust and loyalty. To sum up, the connection of GDPR and AI means that financial service providers must ensure the compliance of data management processes with the requirements of the data protection regulations.

5 SUMMARY

The use of artificial intelligence can provide major advantage in the field of financial services. Here are some examples:

- Reduced costs: financial institutions can reduce costs and improve efficiency by means of AI-based automated processes.
- Better customer service: AI offers personalised customer service and can boost customer satisfaction.
- Risk management: AI-based analytics allow better risk assessment and timely intervention to avoid problems.
- Intruder detection: financial institutions can recognise security threats and can reduce the number of fraud cases:
- Better data analysis: AI-based analytics can help improve data analysis through which financial institutions can have better understanding of customer and market trends.

The ongoing development of AI may result in further innovation and developments in future. The use of artificial intelligence can help in several areas of the finance sector, including, among others, the detection of fraud and abuse, risk management, making investment decisions, customer relations and more efficient internal operations. AI-based tools and algorithms allow financial institutions to collect, analyse and evaluate substantial amounts of data in order to make more effective decisions.

For instance, AI-based systems can detect and identify suspicious transactions that may be connected to money laundering or other illegal activities. Such systems help financial institutions prevent money laundering and terrorism financing. AI and machine learning are useful in risk management processes because algorithms help financial institutions identify risky transactions and high-risk customers. Because of this, banks can have more effective risk management, they can minimise losses and optimise their investments. AI can be of use in investment decisions. Algorithms can analyse a large amount of data fast, for instance, stock exchange data, companies' financial reports, macro-economic indicators, etc. Such systems allow investment decision makers to obtain timely and effective information about the markets so that they can increase investment yield. The use of AI and machine learning allows the financial sector to improve customer relations and customer service. Algorithms and AI allow financial institutions to offer their customers personalised services and solutions improving customer experience in that way.

REFERENCES

Accenture (2023): Accenture: Cybersecurity for Financial Services – Balancing External Threats and Internal Challenges.

Allianz (2023): Allianz Risk Barometer. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.

Appinventiv (2023): AI in Banking – How Artificial Intelligence is Used in Banks. https://appinventiv.com/blog/ai-in-banking/.

Biswas, S. –Carson, B. –Chung, V. –Singh, S. –Thom, R. (2020): AI-bank of the future: Can banks meet the AI challenge? McKinsey, https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge.

CyberEdge (2023): Cyberthreat Defense Report. https://cyber-edge.com/cdr/.

Deloitte (2023): Global Future of Cyber Survey, Building long-term value by putting cyber at the heart of the business. https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html.

Deutsch, N. – Pintér, É. (2018): The Link between Corporate Social Responsibility and Financial Performance in the Hungarian Banking Sector in the Years Following the Global Crisis. *Financial and Economic Review*, 17(2), 124–145, http://epa.oszk.hu/02700/02758/00016/pdf/EPA02758_financial_economic_review_2018_2_124-145.pdf.

ESET (2022): Hogyan veszélyezteti ez a támadási forma vállalkozását? [How will this attack endanger your enterprise?]. https://www.eset.com/hu/it-biztonsagi-temak-cegeknek/social-engineering/.

ESET (2023): Cybersecurity Trends 2023: Securing our hybrid lives. https://www.eset.com/int/business/resource-center/reports/eset-cybersecurity-trends-2023/.

ENISA (2022): ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

European Council (2023): Cybersecurity: how the EU tackles cyber threats? https://www.consilium.europa.eu/en/policies/cybersecurity/.

Gál, I. L. (2007): A pénzmosás hatályos büntetőjogi szabályozása Magyarországon [Effective criminal legislation on money laundering in Hungary]. https://www.mnb.hu/letoltes/pszafhu-rtfkonf-gali.pdf

Lukács, Zs. (2022): Budapest Institute of Banking (presentation).

Mitnick, K. (2022): The History of Social Engineering. https://www.mitnicksecurity.com/the-history-of-social-engineering.

Microsoft (2023): Top 10 questions on Cybersecurity in 2023. https://news.microsoft.com/en-cee/2023/02/01/top-10-questions-on-cybersecurity-in-2023/.

McAfee (2023): McAfee 2023 Threat Predictions: Evolution and Exploitation. https://www.mcafee.com/blogs/security-news/mcafee-2023-threat-predictions-evolution-and-exploitation/?gclid=EAIaIQobChMIwNDZ90n8_gIVgqzVCh28NwJbEAAYASAAEgK9kvD_BwE.

MNB (2022): A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022 [Cyber-threat report]. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf.

Narayanan, K. (2019): Harnessing the power of AI & ML for Analytics in Banking and Financial Services. OneGlobe, https://www.oneglobesystems.com/blog/harnessing-the-power-of-ai-ml-for-analytics-in-banking-and-financial-services.

NAV (2022): NAV PEI Office. https://pei.nav.gov.hu/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda.

NBSZ (2022): Nemzetközi IT-biztonsági sajtószemle [International IT security press review]. NKI, https://nki.gov.hu/wp-content/uploads/2022/12/Sajtoszemle_50.-het.pdf.

Pintér, É. (2008): A pénzügyi szolgáltatások reintegrációja – a bankbiztosítási tevékenységet befolyásoló tendenciák [Reintegration of financial services – trends affecting bankassurance]. Doctoral thesis, Pécsi Tudományegyetem Közgazdaságtudományi Kar, Gazdálkodástani Doktori Iskola, https://pea.lib.pte.hu/handle/pea/15208.

Pintér, É. (2022): Az innováció természetrajza. [Nature of innovation]. In Stukovszky, Tamás – Illyés, Péter (eds.) (2022): *A kis- és középvállalkozások innovációja: Elmélet és gyakorlat*. [Innovation in small and medium-sized enterprises: theory and practice]. Budapest: Akadémiai Kiadó, 81–96.

Proofpoint (2023): Cyber Security Focused on "People".

Qureshi, M. W. (2019): Understanding Compliance Risk in Finance and Banking. *ISACA Journal*, 3, 1–7, https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-4/understanding-compliance-risk-in-finance-and-banking_joa_eng_0719.pdf.

Ray, T. (2017/2022): Scopes of Machine Learning and Artificial Intelligence in Banking & Financial Services |ML & AI – The Future of Fintechs. https://www.stoodnt.com/blog/scopes-of-machine-learning-and-artificial-intelligence-in-banking-financial-services-ml-ai-the-future-of-fintechs/.

Statista (2022a): Threats explicitly factored into companies' strategic risk management activities in Hungary 2021. https://www.statista.com/statistics/1239649/hungary-threats-factored-into-companies-strategic-risk-management/.

Statista (2022b): CEOs' opinion on potential economic, policy, social, environmental and business threats to companies' growth prospect in Hungary 2021. https://www.statista.com/statistics/1234133/hungary-potential-threats-to-companies-growth/.

Terranova (2022): 9 Examples of Social Engineering Attacks. https://terranovasecurity.com/examples-of-social-engineering-attacks/.

TÜV (2023): IT Security Act & KRITIS. https://it-tuv.com/en/leistungen/security-and-value-of-information/it-security-act-kritis/.

Wolters (2018): *Wolters Kluwer Adó-kódex*, XXVII(6), 2.