Cyber Security Challenges through the Lens of Financial Industry

Iustina Alina Boitan
Associate Professor within Bucharest University of Economic Studies

Abstract

The paper aims at drawing attention on cyber security risks the financial industry is exposed to, which recently started to raise increased concern among European and international authorities, in terms of proper prevention, identification, assessment and management. It is an issue of utmost importance the more so that the financial landscape is continuously changing, to keep pace with the technological innovations applied to banking activity, digitization, large-scale use of internet banking/mobile banking. Cyber security risks are included in the broader framework of IT fraud; neglecting their careful monitoring would trigger serious financial and reputational implications for the financial industry. The paper synthesizes the guidelines and reports recently published by the International Monetary Fund, World Bank, Bank of International Settlements, European Central Bank, European Commission, big-four audit companies as well as research centres, to illustrate which is their response to the digital environment trend and cyber security challenge. Then, it reviews the main typologies of threats included in the cyber security risk, graphically depicts the perceived exposure to cyber risks in comparison with other categories of risks, delineates between key risks and emerging risks, and discusses the risk management responsibilities to be assigned to bank's board, operational management, risk/internal control/compliance oversight function and internal audit function (known also as the three lines of defence).

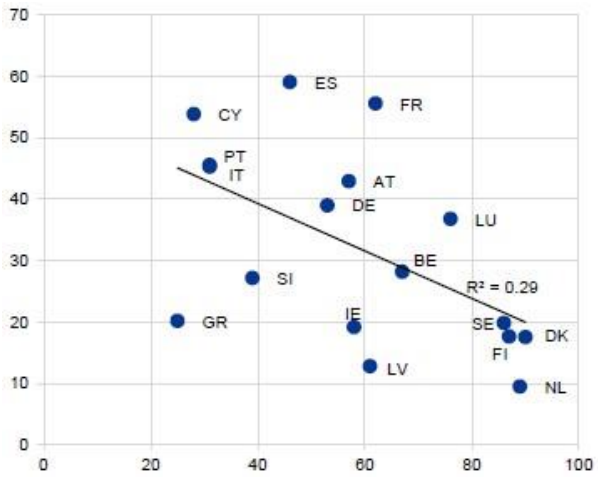
Keywords: IT fraud, digitization, cyber risk, banking, risk management

1. Introduction

Digitalisation of banking activity exerts an impact on the features depicted by financial products, on their cost, but also it significantly changes the territorial spread of the bank branch network and its exposure to risk, by raising cyber security concerns. Andersson et al. (2018) analyse the potential impact of digitalisation on banks' costs and profitability, which seems to be multifaceted and nuanced. Increased investments in digital technologies are able to improve bank revenues and efficiency, stimulating profitability. But they entail also additional running costs represented by the cyber security threat. The pace of digital transformation across European countries and the substitution of traditional bank branch networks by digital channels are highly heterogeneous. As figure 1 show, banking systems in Northern Europe countries

record the smallest territorial branch networks due to large scale use of internet for banking purposes.

Figure 1. The share of population using internet banking vs. the number of branches per 100,000 inhabitants (2017 year-end data)



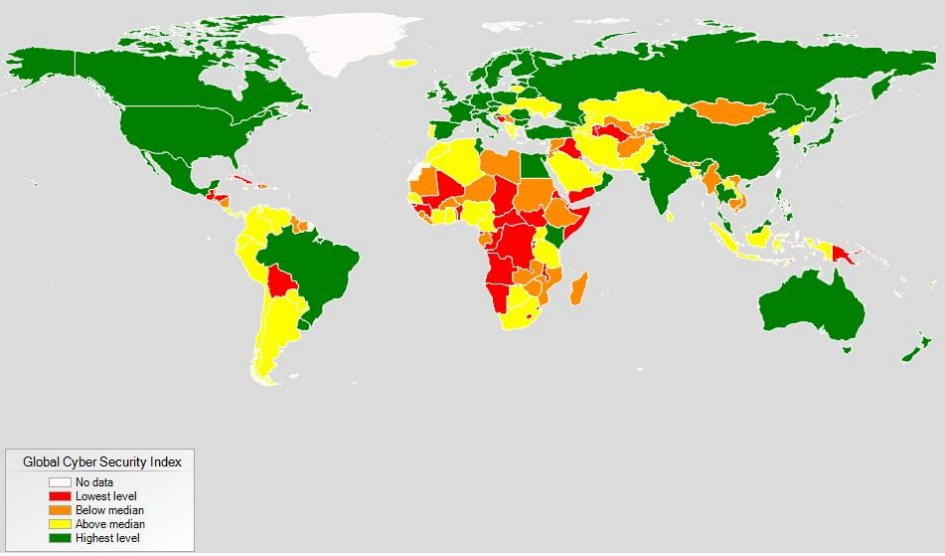
Legend: x-axis: percentage of individuals using the internet for banking; y-axis: number of bank branches per 100,000 inhabitants

Source: Anderssen et al. 2018, p. 131

A comprehensive definition of cyber-risk includes it in the category of operational risks "to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" (Cebula and Young, 2010).

The Chartered Institute of Internal Auditors (2018) draws attention that organisations of all types, both in the public and private sectors, are becoming more vulnerable to the risks related to technology dependence. The Institute of Internal Auditors (2016) claims that "cyber security must be considered holistically and systemically, as the effects of failure can range from an inability to conduct basic operational processes, to loss of intellectual property, to potentially significant reputational damage. It is not solely a technology risk; it is a business risk". Globally, the financial sector is highly exposed to cyber risk, irrespective it is a low-income or developed economy. To better monitor its trend, the International Telecommunication Unit of the United Nations has launched a Global Cyber Security Index (see figure 2). It can be noticed that cyber security monitoring is the highest in Europe, America and Asia.

Figure 2. The Global Cyber Security Index (2017)



Source: Bouveret, 2018

Although the situation looks optimistic, in practice there is a consensus among cyber experts that an IT system can hardly be completely cyber-secured, due to the manifold external and internal threats. Cyber-risk, as any other type of fraud risks, can be mitigated but not completely eliminated (CEPS, 2018).

Data breaches recorded as cyber-incidents may be represented by: steal of customer data or of money from customers' accounts, unauthorised access to customer information and databases by using an internal login, phishing, business disruption.

Frauds committed by relying on one of the three channels: internet baking, mobile banking or phone banking are included in the category of remote banking fraud losses and share the same basic feature: a fraudster gains access to an individual's bank account and makes an unauthorised transfer of money from that account. Banks and card companies have stopped the occurrence of unauthorised fraud in total amount of £1.66 billion in 2018 (UK Finance, 2019).

The Institute of International Finance (2017) classifies cyber-attacks in four main categories (see figure 3) and emphasizes that any attack on financial system's critical components or services could have either direct or indirect impacts that could threaten the stability of the financial system, or the financial security of its participants.

Figure 3. Typology of cyber-attacks

Other data collected by the Systemic Risk Barometer survey revealed that respondents asked to identify the top 5 systemic risks to the broader economy, looking ahead into 2018 and beyond, have mentioned cyber risk on the first position, followed by geopolitical risk, impact of new regulations, and Great Britain exit from the EU (Bouveret, 2018).

The audit company KPMG (2018) has performed a ranking of the top risk categories institutions are exposed in the near future, the first place being held by digitalisation, Industry 4.0 and Internet of Things. The following positions are occupied by cloud computing, the EU-General Data Protection Regulation and the cyber security. Digitalisation is considered an emerging risk, while cyber security is a key one.

The survey performed by the European Confederation of Institutes of Internal Auditing (2019) among the heads of the internal audit department in 9 European countries uncovered the list of the hot topics monitored by them in the last years, as well as future prospects. The conclusion is striking: cyber security and data protection represent a top concern (figure 4).

Figure 4. Monitoring areas considered by internal audit departments

2018	2019	2020
1. GDPR and the data protection challenge	1. Cybersecurity: IT governance & third parties	1. Cybersecurity & data privacy: rising expectations of internal audit
2. Cybersecurity: a path to maturity	2. Data protection & strategies in a post-GDPR world	2. The increasing regulatory burden
3. Regulatory complexity and uncertainty	3. Digitalisation, automation & AI: technology adoption risks	3. Digitalisation & business model disruption
4. Pace of innovation	4. Sustainability: the environment & social ethics	4. Looking beyond third parties
5. Political uncertainty: Brexit and other unknowns	5. Anti-bribery & anti-corruption compliance	5. Business resilience, brand value & reputation
6. Vendor risk and third party assurance	6. Communication risk: protecting brand & reputation	6. Financial risks: from low returns to rising debt
7. The culture conundrum	7. Workplace culture: discrimination & staff inequality	7. Geopolitical instability & the macroeconomy
8. Workforces: planning for the future	8. A new era of trade: protectionism & sanctions	8. Human capital: the organisation of the future
9. Evolving the internal audit function	9. Risk governance & controls: adapting to change	9. Governance, ethics & culture: the exemplary organisation
	10. Auditing the right risks: taking a genuinely risk-based approach	10. Climate change: risk vs opportunity

Source: European Confederation of Institutes of Internal Auditing (2019)

2. Review of regulatory frameworks related to the cyber security challenge

In Europe cyber security is jointly targeted by the EC and other European authorities, as well as by central banks and practitioners. In 2013 the European Commission has adopted a Cybersecurity Strategy for the European Union while in 2016 it has been adopted the Network and Information Security Directive meant to enforce European cyber security law, by adding new information security and incident notification requirements for operators of essential services and digital service providers. Also, in 2016 it has been adopted the General Data Protection Regulation which constitutes too a major shift in European data protection law.

Another international organisation that significantly contributes to achieving a state of global financial integrity is the International Monetary Fund. Its Strategy on Anti-Money Laundering and Combating the Financing of Terrorism first launched in 2014 has been recently revised and updated (IMF 2019), so as to outline Fund's on-going engagement in all areas that could negatively affect financial integrity, such as Fintech, illicit financial flows, and relevant aspects of cyber security.

The Chartered Institute of Internal Auditors (2018) warns that "forthcoming regulations will increase the burden on organisations to ensure they have effective cyber security strategies and culture in place, in addition to robust controls and policies to prevent and remediate attacks".

Regulatory frameworks have to be complemented with appropriate tools meant to quantify cyber risk exposure. In this respect, a singular approach belongs to International Monetary Fund (Bouveret, 2018) which developed a quantitative framework for assessing cyber risk in the financial sector. Bank of England has designed a framework called CBEST to deliver controlled, intelligence-led cyber security tests for systemic financial institutions in UK, meant to look for potential network entry points from the target organisation's website, to identify vulnerabilities that can be exploited by fraudsters, and then simulating a cyber-attack by using the tactics, techniques and procedures of threat actors known to have an interest in the target organisation.

3. Cyber security risk management

The Chartered Institute of Internal Auditors (2018) highlights that a "strong cyber awareness culture is one of the best defences against cyber-attacks" and states that the internal audit function plays a crucial role in ensuring that this culture is understood and effectively implemented by staff at all levels.

A proper cyber risk management framework is the result of defining several layers of risk defence, represented by bank's board and executive management function and the so called three lines of defence, namely: operational management, risk/internal control/compliance departments and internal audit (Chartered Institute of Internal Auditors, 2018).

UK Finance (2019) emphasizes that financial industry has to strengthen its commitment towards tackling fraud and scams by implementing various measures, such as:

- advanced security systems to protect customers, including real-time transaction analysis, sophisticated ways of authenticating customers, behavioural biometrics on devices and technology;
- design of a Banking Protocol to serve as rapid warning and response scheme through which bank branch staff can alert police in case of fraud suspicions;
- developing new technology meant to track suspicious payments and identify money mule accounts.

A complementary initiative belongs to the Centre for European Policy Studies - CEPS (2018) that has organised a Task Force meeting gathering experts from the financial industry, tech industry, national supervisors and European institutions. The policy recommendations raised in order to boost financial industry's cyber-resilience against current and future threats are:

- ✓ need for increased convergence in the definition of cyber-incidents;
- ✓ improvement of the existing framework for cyber-incidents reporting;
- ✓ adopting a decision on whether the data held by the centralised hub should be shared with supervisors, and customers;
- ✓ development of consistent, reliable and exploitable statistics on cyber-trends;
- ✓ implementation of best practices for cyber-hygiene by regulators and supervisors;

- ✓ strengthening of the European Cybersecurity Certification Scheme;
- ✓ reinforcement of cross-border cooperation and legal convergence, both within the EU and globally;
- ✓ design of best practices for the resolution of cyber-attacks cases;
- ✓ assessment by policy-makers of the feasibility and necessity of creating an emergency fund in case of large cyber-attacks.

4. Conclusion

An open question which poses great concerns for regulators and financial industry is whether they manage appropriately the financial crime risks, among which cyber risks are increasingly present. Proactive conduct and collaboration between all directly involved actors in the financial industry is of utmost importance, in order to uncover new, emerging risks and the measures and regulations to be adopted to mitigate them.

The Institute of International Finance (2017) recognizes the efforts already done by the private sector and the authorities to address the increasing threats arising from cyber-attacks, but claims that more analyses need to be performed so as to target the emerging threats to financial stability.

References

Andersson, M., Kok C., Mirza, H., Móré, C. and Mosthaf, J. (2018). How can euro area banks reach sustainable profitability in the future? ECB Financial Stability Review, November 2018.

Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, IMF WP/18/143.

CBEST: http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

Cebula, J.J. and Young, L.R. (2010). "A taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Centre for European Policy Studies-CEPS (2018). Cybersecurity in Finance Getting the policy mix right! Report of a CEPS-ECRI Task Force, June 2018

Chartered Institute of Internal Auditors (2018). Cyber security, December 2018

European Confederation of Institutes of Internal Auditing (2019). Risk in focus 2020: hot topics for internal auditors.

Institute of Internal Auditors (2016). Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser, Issue 4/2016.

Institute of International Finance (2017). Cyber Security & Financial Stability: How cyberattacks could materially impact the global financial system, September 2017

International Monetary Fund (2019). Review of the Fund's strategy on anti-money laundering and combating the financing of terrorism, IMF Policy Paper, February 2019.

KPMG (2018). 20 key risks to consider by internal audit before 2020

UK Finance (2019). Fraud the Facts 2019.The definitive overview of payment industry fraud