FINANCIAL SERVICES, ePAYMENTS AND INSURANCE SECTOR REPORT

Cyber security for the finance and insurance sector

WG3 I Sectoral Demand

MARCH 2018

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg3_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

This document will be continuously updated based on developments within the sector and ECSO members' input.

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

The digital world is changing at the speed of light and in such a way that no one could expect until few years ago. Almost everything is interconnected, and the advent of new technologies has spread a series of benefits but also threats. Cyber security is, more than ever, of paramount importance to protect the whole EU Digital Single Market and, as acknowledged also by the NIS Directive, the financial industry is one of the main critical sector. Cyber criminals are more and more active and sophisticated, especially in this lucrative sector. Indeed, cyber-attacks on critical financial infrastructures could create serious damage to people and economy with relevant costs and potentially generating a systemic impact. The importance of cyber security in the financial sector should be addressed starting with research and development, keeping in mind the need to implement and leverage tools helpful to mitigate and tackle cyber threats, improving cyber resilience. Cyber security enhancements can only be effectively attained if the appropriate education and training programmes are undertaken involving all the stakeholders, that means to create awareness from Board members to employees, from university students to overall citizens and customers. It is worth mentioning that cyber insurance is coming to light helping businesses and people to protect themselves from risks related to the negative impacts of cyber threats and incidents, and this entails the need to quantify and measure new risk categories related to cyber security. Companies involved in cyber insurance have to tackle cyber security issues both as a threat for themselves, just like any other company, but also as a new business opportunity.

The purpose of this document is to give a general overview about cyber security in the financial and insurance sector, starting from the Digital Single Market landscape and its transformation, going through the analysis of all the actors involved in this scenario, to the issues and new challenges arising from the EU evolving cyber security scenario and regulatory framework.

The need for readiness and awareness in cyber security issues is a clear objective, paving the way towards a public and private cooperation to reach the common goal of an enhanced cyber resilience across Europe. Keeping this in mind, a joint effort between the stakeholders shall lead to leveraging the new instruments and looking into possible operational paths to achieve an improved cyber resilient Digital Single Market.

2 Landscape

In the digital era everything and everyone is interconnected. Stopping the digital evolution is not an option, since this would hinder a country's economic and social growth. Digitalisation and globalisation have created an extremely interconnected world, whatever the industry it belongs to, each institution, shall cope with the opportunities and the threats arising from a global perspective.

Operating in an open economy, with high level of interdependencies, introduces a high systemic risk that covers the entire EU financial system. To mitigate the systemic risk exposure of the Digital Single Market, enhancing cyber security is a key success factor. The implementation of a Single Financial Market represents a prerequisite to foster European competitiveness and to stay up with the European citizens' evolving expectations around their customer experience.

Cyber security and digital privacy feature high on the list of the political priorities of the European Commission: trust and security are at the core of the Digital Single Market Strategy, while the fight against cybercrime is one of the three pillars of the European Agenda on Security. The European Commission has launched the Horizon 2020 Programme to foster secure European society in a context of dramatic transformation, growing global interdependencies and threats, and to strengthen the European culture of freedom and justice, addressing also the broad cyber security issues. In addition, Science Europe, the association of the European Research Funding Organisation (RFO) and Research Performing Organisation (RPO) is working on the Framework Programme 9 (FP9), that will represent the next R&I programme of the European Commission, after the expiration of the Horizon 2020 programme.

Business, governments and individuals are rapidly taking advantage of faster and cheaper digital technologies to deliver an unprecedented array of social and economic benefits. However, without tools and partnerships aimed at solving or mitigating cyber challenges, leaders in business, government, and across society cannot pursue the benefits of digitalisation with confidence.

Looking at the EU citizens, the digital economy represents an ongoing opportunity, leveraging the omni-channel interactions within the financial system. European citizens' daily life entails digital banking and payments as a final step in most purchasing activities; this is true when the payments are done in proximity (credit/debit card POS, NFC) and even more when they occur remotely (e-payments and m-payments). The proliferation of digital devices represents the omni-channel challenge requiring efficient authentication and authorisation means and data security features. It is to be noticed that Strong Customer Authentication is among the key items addressed with the new Payment Services Directive, PSD2. To individuals, cyber risk could entail potential financial loss and data breaches, but even worse the most critical asset at stake is their trust. Losing customers' trust would endanger the foundation of the entire financial system.

Small and medium size businesses are a driving force in today's global economy as they account for a major portion of the gross domestic product (GDP) in many countries. Technology companies have taken note; more major service and software providers are tailoring their offerings to smaller organisations. As the frequency and sophistication of cybercrime attacks intensifies, it has become clear that small and medium size business vulnerability is shared by larger enterprises which depend on these businesses as part of their supply chain or vendor ecosystem. Government and industry security requirements have begun to impact smaller businesses; they must prove they are

taking steps to secure data, transactions, and infrastructure, otherwise they will undergo the risk of losing partners and clients.

Clear, cost-effective access to complete cyber security solutions is essential—not only to individual companies, but to the health of the overall economy and the security of everyone's data. Small and medium size businesses tend not to have the budget, resources or skills to tackle the increasingly complex security challenge on their own, and are increasingly turning to Managed Service Providers (MSPs) to protect their data, network, employees, and customers from cybercrime. In this respect, the evolution of cloud services, towards cyber safer technologies, with features linked to cryptography and data protection, could be beneficial to the growth of the Digital Single Market.

The financial industry represents the backbone of the economy altogether, providing services to the consumers, the corporates (irrespective of their sizes), and the public administrations. In this respect, the European Central Bank (ECB) has identified that the significant banks must undergo their direct oversight through the Single Supervisory Mechanism and the ECB has also pinpointed cyber security as a major item among the topics that have a systemic relevance.

As a matter of fact, while the large banks are involved with several Financial Markets Infrastructures (FMIs) spread around the world, they do mostly leverage the same communication channels, and more and more tend to operate and handle financial transactions in real-time (or near real-time). Within a financial industry that is highly interconnected and relies heavily on widespread ICT, cyber risk is to be considered as a systemic risk that could affect the whole economy. That is why the BIS/IOSCO Guidance on cyber resilience for Financial Market Infrastructures states that each FMI should immediately take necessary steps in concert with relevant stakeholders to improve their cyber resilience. FMI's should also develop concrete plans to improve their cyber resilience, leveraging three main cooperation streams: Info-sharing, Crisis Communication & Management, and Crisis Simulation exercises. In this respect, financial institutions have to cope with multiple regulatory requirements stemming our from EU Directives and Regulations such as PSD2, NIS and GDPR, but next to that they will have to look at national regulatory requirements and operational requirements related to the FMIs, first of all the financial market infrastructures managed by the ECB, such as Target2.

Cyber risk management is therefore a top priority for the financial industry. The number and frequency of more sophisticated cyber attacks to the banking sector are ever growing and the need to develop a comprehensive cyber security framework, to protect the integrated financial market and to combat cyber fraud, is clear.

To enhance cyber security, a mandatory step is to take a more holistic approach beyond the individual institution creating a cooperative approach to cyber defence. This entails a huge collaborative effort that addresses the entire supply chain and involves all stakeholders that are also playing an active role in the daily interactions, e.g. customers, suppliers, correspondents, FMIs. It is therefore important to foster the collaboration among peers at sectorial level, but even further across industries, as is also highlighted with the adoption of the NIS Directive concept of "Operator of Essential Services" that belong to several industries.

Sharing threats and vulnerability information, conducting coordinated cyber emergency exercises and simulations, managing rapid response to cyber incidents and developing crisis management communication and procedures are the main topics on which the collaboration needs to be enhanced. These issues are clearly underlined also by the European Commission in his Cyber Security Blueprint (*Commission Recommendation 2017/1584 of 13 September 2017*), containing a

set of recommendations included in the wider Cyber Security Package, regarding the coordinated response to large-scale cross-border cybersecurity incidents and crisis

The protection and involvement of all EU citizens in the fight against cybercrime is a necessary target to face the continuous evolution of cyber threats and IT risk. The continuous investment in the Finance & Insurance sector on cyber risks is justified by, inter alia, the following basic considerations:

- The high impact on all European citizens;
- The systemic risk associated;
- The ability to support the competitiveness and the growth of the entire European economy;
- The huge amount of sensible personal data managed through the Finance and Insurance sector.

The proliferation of big data itself has introduced new possibilities in terms of analytics and security solutions to protect data and prevent future cyber attacks. However, just as big data has opened up new possibilities for cyber security teams, it has also given cyber criminals the opportunity to access huge quantities of sensitive and personal information through the use of advanced rogue technologies. Personal data therefore becomes an asset to be protected against cyber attacks.

Technology is transforming the financial sector. As the world's largest user of IT products and services, finance stands to benefit from new generations of processing, storage, mobile and authentication technologies as well as social networks, artificial intelligence or distributed systems. New business models are emerging and innovation in the financial sector is assuming a growing importance. In this respect, we shall highlight that the FinTech involvement is twofold: as new participants in the “traditional” payments value chain (e.g. PISP under PSD2), and as actors pushing for new technologies and new business models (e.g. DLT). Competition and collaboration between financial institutions and FinTechs will surely bring innovative business models to the benefit of the wider community.

The evolution of technology and its impact in creating new business models is also reflected in the regulatory evolution that acknowledges and addresses new business roles and patterns. It is worth mentioning that the Payment Service Directive 2, (PSD2) opens the playing field far beyond what was foreseen under the first Payment Service Directive (PSD), and it creates clear roles accessible to FinTechs. On the other hand, in order to achieve a level playing field, the FinTechs will have to undergo the same regulatory burden with respect to oversight and compliance with the regulatory requirements. The underling concept shall be “same risks same rules”.

3 User Engagement

The finance and insurance sector encompasses a wide variety of stakeholders. Financial and insurance services are offered to all citizens, to private corporates and to public administrations as well. We can therefore distinguish between several actors in the financial industry: from citizens to government and public administrations, large multinational corporates, SMEs and start-ups, university and research centres, consumers and employees. It is of utmost importance to understand the cyber security needs from each group, but also to involve and educate them since they should also become an integral part of cyber security programmes.

The actors identified in the finance and insurance sector and the possible strategy to involve each category to define cyber security requirements and programmes are:

- **European Citizens and Consumers**: The general population must be engaged as active security providers, not only as simply beneficiaries of security policy, because their behaviours can create threats. The European Citizens could be a target for Governments' mass communication programs. In their role of consumers, they should be educated through a customer education marketing and communication policy that can transfer the value of a safer and more secure financial service provider and can also strengthen their awareness to protect the very last mile of the security value chain. It is also possible to envisage to undertake joint activities with consumer association such as BEUC - The European Consumer Organisation and their federated national associations.

- **Private corporates**: Private corporates do represent a major customer set in the financial industry and this applies to both banking and insurance companies. At the same time, private corporates often act as suppliers to the industry. Here again, a possible way to raise awareness is to leverage the interactions through associations, the cross industries cyber security conferences and international organisations such as ECSO itself. When the corporates act as suppliers, they should be involved in third party supply chain cyber security assessment programmes.

- **Financial and Insurance Companies**: Cyber security is an increasingly critical threat to global financial institutions and the broader financial system. Large financial institutions are prime targets for activists, organised crime, and cyber terrorists. The interconnectedness of financial institutions leaves them vulnerable to disruption, threatening the stability of the international financial system. To increase the cyber resilience across the financial system, national and international associations, such as EBF and Insurance Europe, are good channels to define widespread cyber security programmes. Other useful means are conferences and sectorial working groups.

- **Financial and Insurance Companies employees**: While the boards and senior management of financial institutions are increasingly aware of the issue, a much broader and deeper understanding of the nature of the threat and the potential responses is needed among banking and insurance employees. This objective can be attained with the roll-out of specific educational programmes and information sharing initiatives.

- **Government and public administration**: Governments shall represent a driving force in raising the awareness and in setting best practices to improve the system's overall cyber resilience. Under the NIS Directive governments have to identify critical business, critical

infrastructures and enforce or mandate them to comply on certain security frameworks. Improved collaboration and information sharing between the public and private sectors are also required. Together, private and public stakeholders must deploy cyber security frameworks to mitigate the risks.

- **Universities and Research centres**: Universities play a key role in fostering innovation in the cyber fight, improving the knowledge around the whole cyber security landscape. In some universities there are specific courses and trainings, also through public-private partnerships. It is fundamental to teach people about the risks and cyber threats in a world more and more dependent on technology. Research centres will also take up an important position in the cyber security arena, with the development of new technologies and innovative researches related to cyber security (e.g. risk measurement methodologies and quantum computing).

- **FinTech:** FinTech companies are an additional player within the financial industry. These large non-banking companies can count upon a large customer base with huge digital interactions and user-friendliness. Their business model is about simplifying finance and providing services by making them cheaper, faster and seamless for the customers. A way for the banks/financial institutions to offer these next generation services and to ride the FinTech disruptive force expediently is by partnering with FinTech and helping the bank customers use the services seamlessly and then integrating them. Here again, leveraging the opportunities to foster the sharing of information, of expectations and vision can prove to be beneficial to everyone**.**

4 Sector Specificities

The resilience of the financial system needs to be enhanced. Each and every single financial institution should take all possible measures to identify, mitigate and protect itself from cyber risk. Nonetheless, in a highly integrated financial world all the components need to be protected along with all interconnections. Taking into account the NIST Framework functions (Identify, Protect and Detect), to reach an appropriate and consistent level of risk mitigation it is important to foster information sharing. Information sharing that for some security features could even be extended to sharing common infrastructures for several financial institutions. Furthermore, the information sharing could be extended beyond the specific industry and become a cross-industry asset.

For example, setting up an EU financial ISAC, or information hub, could create an added value for the whole financial industry, and this could be managed by a neutral EU public stakeholder (e.g. ECB/EBA/ ENISA) to improve prevention, response and lesson learned, enhancing the resilience of the overall financial system. By doing so, each institution would be responsible for its incident management but could contribute to creating and using a common set of re-usable knowledge. In order to be able to leverage such knowledge, it is of the utmost importance that the information flow is bi-directional. The financial institutions could report incidents but should also receive anonymised feeds from the Hub, to increase the capabilities in identification, protection and detection of each and every institution and the overall financial system.

Looking at the Respond and Recover NIST Framework functions and at the NIS Directive we can appreciate the effort towards the definition of common procedures to foster cooperation in cyber crisis management, setting up a collaboration among national, EU (e.g. ENISA) and international organisations. It is worth mentioning that EU regulation, with the NIS Directive, does not introduce common procedures for cyber crisis management, nonetheless the definition of such procedures might be done leveraging the progress that will be achieved in a first stage with info sharing & incident reporting procedures. The EU framework for incident reporting which emanates from the latest regulatory evolution foresees the involvement of multiple authorities at national and European level, applying different procedures and templates, creating possible overlaps and redundancy in reported information. It is likely that a single incident might require the fulfilment of multiple reporting requirements, causing a heavy burden on stakeholders. The need for harmonisation and coordination among the different stakeholders is clear, as is the urgent need for standardisation of templates and procedures. These could lead to the implementation of harmonised tools, adopting a common taxonomy and undertaking frequent testing exercises, the readiness to cope with large scale cyber incidents and the response process should become clearer and smoother.

So far, the ECB, the national authorities and even ENISA have already undertaken some crisis management testing, however, strengthening the EU cyber resilience industry should require more cyber crisis simulation and war gaming with wider cooperation. These kinds of exercises must be implemented with the largest number of participants across the European Union, involving private and public companies, critical infrastructures, operators, EU and national organisations. These simulations would foster situational awareness and structured cooperation during cyber crises, while an increased familiarity with these collaboration procedures could allow for a faster and more coordinated response to cyber crisis.

On September 13 the European Commission released a proposal for a Regulation on the future of ENISA the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") called the “Cybersecurity Act”. It is proposed that the current role of ENISA should be strengthened in several areas, e.g. the NIS Directive implementation, the review of the EU Cybersecurity Strategy. Two of the new key areas identified, where the Agency would play an important role, are cyber security crisis management and cyber security certification and standardisation of ICT products and services. In addition, it is proposed for the Agency to have a permanent mandate which would allow for a more strategic and longer-term planning, thus enabling for a better preparedness to tackle the future challenges.

Another area for cooperation among different interconnected players is to address the cyber issues along the supply chain management that represents another important topic to critical infrastructure organisations and to financial institutions. The development of secure financial products and services must be based upon secure components, processes and procedures (secure by design). The supply chain is often the weakest link for cyber security and in an integrated and interconnected eco-system this is an unbearable risk. Qualifying and evaluating every single entity along the supply chain is of utmost importance to adopt a cyber secure supply chain policy and to enhance the overall resilience. In this respect, the evolution of best practices consists in requesting providers to undertake a self-assessment (e.g. through penetration testing), or to comply with the customer’s cyber requirements, or to adopt certification schemas.

Looking at the other side of the end to end (E2E) value chain, the focus shifts towards the customers. In this perspective, privacy, data protection and data integrity, represent major challenges in the digital banking era and need to be protected.

- Insurance and finance operations often involve cross-border transactions. Combining the cross-border and the multichannel interaction modes requires a high level of data management and data protection against cyber threats, adopting a privacy preserving approach to cross border data transfer.

- Under the PSD2 Directive (2366/2015), non-regulated third-party providers (TPPs) can partially cover the value chain of payment systems. The PSD2, with XS2A accounts provision, also introduces the obligation to provide them with access to information and therefore to sensible data, increasing the cyber risk on privacy, data protection and communication protocols.

- Among the financial industry players, we should not forget that insurance companies have traditionally priced risks based on risk factors, and these risk factors are defined on the basis of a huge amount of sensible data collection, therefore the challenge is to combine privacy preserving approach and risk evaluation. The shift towards more risk sensitive prices, driven by increased data availability, means that insurers will collect and analyse a larger amount of data, mainly personal and sensitive ones, on the other side this huge amount of data is an appealing asset for cyber-criminals.

The collection and management of data in a digital framework highlights several needs, among other customers’ awareness, user friendliness, privacy and cyber security assurance. Indeed, EU regulation also reflects the sensitivity of data protection and digital identity with GDPR and e-IDAS, both do also foresee an incident reporting to the respective national authorities.

A major need in the coming years will be to create an environment in which financial innovation can thrive to meet the evolving expectation of customers, without entailing a loss in security and

data protection. Innovation introduces new challenges for the financial sector which must ensure that consumers are protected. FinTechs involvement introduces new opportunities and challenges, e.g. fostering access to financial services for consumers and businesses, bringing down operational costs and increasing efficiency for the industry; making the single market more competitive by lowering barriers to entry; balancing greater data sharing and transparency with privacy needs[1]. New financial technologies can also help individuals and SME's to access alternative funding sources for supporting their cash flow and risk capital needs. However, recently the EU consumer organisations have received a growing number of complaints from consumers who have been targeted by fraud or scams when using social media websites, as well as having been subject to certain terms of services that do not respect EU consumer law. On this basis, EU consumer authorities sent a letter to Facebook, Twitter and Google asking them to address the two areas of concern. Following this letter, the EU Consumer Authorities and the European Commission met with these companies to hear and discuss their proposed solutions. These companies will have to define detailed measures to comply with the EU regulatory framework. This is to demonstrate that FinTechs are in the position to leverage a large customer base and to facilitate their users' digital experience by introducing functionalities along the financial value chain (e.g. Amazon Cash), while they could at the same time, however, introduce additional vulnerabilities. For the growth of the EU financial market it is desirable that FinTechs and financial institutions identify areas where their joint efforts can deliver value-added services in partnership. Furthermore, the Commission will establish an EU FinTech Lab, with the aim of raising the level of regulatory and supervisory capacity and knowledge about new technologies, through demonstrations and expert discussion in a non-commercial, neutral financial technology Laboratory. The Lab will bring together multiple vendors with regulators and supervisors to enable discussion of regulatory and supervisory concerns.

Another development arising from technological innovation is ICT cloud architectures. Cloud is surely a double-edged sword; traditionally, banks were reluctant to adopt cloud, but it has since been recognised that the cloud can ease disaster recovery and business continuity management. On the other hand, it requires specific actions to mitigate a wider and beyond control attack surface. The concept of distributed architecture has moved forward also beyond the ICT infrastructure to move into business models. Among the distributed business models, the most known are Distributed Ledger Technologies (DLT) (e.g. Blockchain), and these business developments do also need a wider approach by considering cyber risk evaluation. One of the issues is linked to the use of cryptography deployed to sign messages and transmit data. Cryptography is a powerful enabler to DLT's that is however challenged on its turn by the quantum technology. Quantum computing could solve many existing cryptographic algorithms, showing that the cyber fight is a never-ending story whereby the quest for research and innovation cannot stop.

Whilst insurance companies, like any other financial institution, need to manage cyber security risks, they can also leverage a new revenue stream coming from innovative products and services to provide trusted means of transferring cyber security risk (cyber insurance) across industries. However, to further develop the cyber insurance sector, it is necessary to quantify and evaluate the cyber risk, which entails the need for a definition of a common measuring system. The creation of a clear set of cyber security definitions and measurements should be done in accordance with other international standards, to simplify information exchange and to encourage due diligence

[1] European Commission "Consumer Financial Services Action Plan: Better products and more choice for European consumers"; March 2017

processes. The introduction of cyber security definitions, statistics and measuring systems to quantify, mitigate and manage cyber risk can also be considered one of the necessary targets to create a common EU cyber risk benchmark that can be used to compare enterprises' resilience to cyber risk across Europe, making cyber risk exposure comparable. This could also enable the introduction of a related European framework for standardisation, labelling and certification.

The implementation of educational and training programmes is the last, but not the least, necessary success factor in tackling cyber security issues. Cyber risk should be considered as a top priority risk, included in the field of enterprise risk management, and top management should be involved in the definition of a cyber security plan to manage the risk in accordance with their company strategic goals. Top management and executives' involvement, with an accurate understanding of the cyber risk consequences, can ease the adoption of new technologies and features that can reduce cyber risk by accepting to undertake the associated additional investments. Furthermore, for any financial institutions' employee, a minimum common degree of understanding of cyber risk could be considered as a must.

It is expected that there will be an impressive lack of skilled IT personnel specialised in cyber security, so to avoid this shortage and to develop specific competences, education programmes should be set up with the universities. Already today, a shortage of experts has been observed and the growth of the market will be inhibited unless sufficient numbers of experts are trained in cyber security. Customers should also receive some communication and training around cyber security to reduce the risk of becoming a victim of cyber fraud, to develop awareness around the value of cyber security and to become an active part of cyber risk mitigation.

Ensuring a safe digital banking environment is the basic requirement for the smooth growth of the European economy. Cyber security can hinder or foster the development of the Digital Single Market, paving the way to its growth and bringing down barriers to unlock online opportunities.

5 Market Study

The EU Single Market allows people, services, goods, and capital to move freely in an economy producing around 15 trillion euro annually. It offers new opportunities to European businesses, enhancing competition and leading to more choice, better services, as well as lower prices for over 500 million consumers[2].

The introduction of the internet has dramatically changed the way people communicate, but also their lifestyle. With significant impacts on all sectors, the "digital revolution" has created a brand new eco-system. EUROSTAT reports that 82% of the European population have used the internet in the last 3 months and the 55% have purchased something in internet in the last 3 months. Today, the network has more than a billion websites, a figure that is steadily growing, and there are more than 3.5 billion Internet users worldwide[3].

According to KPMG "Global CEO Outlook Survey 2016", about 42% of the CEO respondents from the banking world believe that banking will be completely transformed over the next three years and 65% are concerned that the business model can be revolutionised by new entrants. The cyber insurance market is in its embryonal stage because the modelling of cyber risk has proved to be difficult due to a lack of available data. Meanwhile, the finance sector is opening up to new entrants because of this digital transformation coupled with the regulatory evolution: some non-banking operators entered in the competitive arena, challenging the banks in offering some services. Google, Amazon, PayPal and many other digital operators are starting to offer payment services and other traditional banking services. The competition between traditional banks and new competitors is open and the result will depend on the ability of banks to let their business models evolve to meet the customers' expectations.

The financial sector involves B2B and B2C services: banks, investment funds, stock exchanges, real estate, and all kinds of insurers. Banks and insurance companies represent large markets, with a direct impact on EU citizens' daily life. The financial services industry supports the prosperous evolution of the whole economy across all industrial sectors. At the same time, the finance and insurance sector has been historically appealing to hackers. Banks alone experience three times as many security attacks and incidents as any other sector. According to Ponemon Institute and Accenture "2017 Cost of Cyber Crime Study & the Risk of Business Innovation", while the cost of cyber-crime impacts all industries, companies in financial services have experienced the highest annualised cost[4]. The following considerations apply:

- Most attacks are directed at stealing money;
- Banks and insurance companies maintain an enormous database of customer data, including credit card information, email addresses, financial statements;
- Banks increasingly rely on internet and mobile technology to deliver services valued by the customer, by doing so they increasingly rely on infrastructures and technologies beyond their direct control;

[2] Ibid
[3] KPMG advisory "Digital banking 2017"; March 2017
[4] Ponemon Institute and Accenture "2017 Cost of Cyber Crime Study & the Risk of Business Innovation"; October 2017

- Banks and insurance companies face a complex security environment since they have to defend themselves and their customers from cyber attacks, comply with evolving regulations, compete on the market with fast changing business requirements, and face the time to market pressure and expansion into new markets.

Given the scale of the risk, the number of attacks, the number of years of experience in defending the assets and the mission critical ICT systems, this sector is at the forefront of securing information systems, networks and internet, mobile and multi-channel access in general.

The main areas of interest for further evolution of the digital financial market, which can dramatically increase the available market for cyber security services and solutions to support enhancements of cyber resilience are:

- Mobile security (area with largest forecasted growth, as security measures in this area are lagging behind), looking also at lightweight cryptography supporting innovative multichannel technologies;
- Innovative systems to detect and respond to attacks;
- Security awareness, education and training programmes;
- Incident reporting and crisis management procedures' harmonisation and review;
- Regulatory Sandboxes, test-bed environments to simulation & training exercises;
- Third party security assessment, supply chain certification processes;
- Cloud computing and cloud based business continuity processes;
- Threat intelligence with integration of activities at national and international level, since the Finance and Insurance industry is highly globalised;
- Pre-emptive activities to manage and study malware families most commonly used and prepare detection and reaction systems in advance or able to respond to variants;
- Advanced and innovative identification and authentication techniques to foster strong authentication and increase user-friendliness for customers.

Retail financial services are an integral part of people's daily lives. These services include bank accounts, credit/debit cards, consumer and mortgage credit, insurance and long-term savings products. Innovative on-line services are transforming the way people use financial services. They also represent a major opportunity for bringing to all Europeans the benefits of a more deeply integrated Digital Single Market for financial services. Nowadays, the markets for these services remain fragmented; only 7% of consumers have purchased a financial service from another EU Member State, however, when the operations and the regulation will make it smoother and supported by clearer rules, this percentage is expected to grow dramatically.

Having said that, it is pretty difficult to have a precise indication of the market size. It is a general understanding that there is a lack of market knowledge: standardised market definitions, statistical information, market monitoring and trend analysis. Notwithstanding the challenge to put in place standard definitions and measurements, to have an idea of the dimension of the phenomenon, it is worth reporting some findings of relevant research:

- According to "Cyber Security Market Report - Q2 2017" published by cyber security Venture[5], globally the cyber security market by 2017 will be exceed $1 Trillion from 2017 to 2021.
- According to PwC "Insurance 2020 & beyond: reaping the dividends of cyber resilience"[6] paper, cyber crime costs the global economy more than $400 billion a year.
- European banks are major investors in IT infrastructure and services, pouring billions of euros into innovation, research and maintenance every year. Research among banks conducted by Celent in 2015 shows that European banks in 2018 expect to invest 62 billion in IT[7].

The insurance sector looks at the cyber market from two different points of view: on the one hand, insurance companies are subjected to expenditures and potential losses arising from cyber security threats (e.g. data breaches, stealing of sensitive data) similarly to other financial institutions. On the other hand, cyber risk represents for the insurance sector a revenue stream and a potentially huge opportunity.

This unique situation must tackle the same difficulties in sizing and quantifying the "cyber risk". In addition, statistical data on the financial impact of cyber attacks are limited, making more complex the evaluation and pricing of cyber risk, in order to define adequate cyber insurance contracts. As a reference for the potential opportunity, we can consider that according to the PwC "Insurance 2020 & beyond: reaping the dividends of cyber resilience"[8] paper:

- Annual gross written premiums are set to increase from around $2.5 billion today to grow to $5 billion in annual premiums by 2018;
- The cyber insurance market could reach $7.5 billion by the end of the decade (2020).

The potential size of the generated cyber solutions in the Finance and Insurance sector represents a huge opportunity to boost European economy, by overcoming the customer fear and enhancing their trust in digital means. As stated by the EC[9], the Digital Single Market could contribute Euro 415 billion per year to the European economy, with as many as 3.8 million new jobs, boosting growth, competition, investment and innovation.

Eurostat reports that in Europe there are 315.000.000 users that use internet every day, and the EBF highlights that 15% of European consumers bought online from other EU countries in 2014. These figures outline that there is a great opportunity for growth in Europe. Each single user accesses several marketplaces, applications and payment methods. Each single access needs cyber protection, with respect to both identity, data and privacy, and last but not least payments and account information. European citizens are particularly sensitive to cyber security. The more people feel comfortable in leveraging the supply of digital marketplaces, the higher the trust on security features, and the steadier the growth of the Digital Single Market will be.

[5] Cybersecurity Venture "Cybersecurity Market Report – Q2 2017": http://cybersecurityventures.com/cybersecurity-market-report/
[6] PwC "Insurance 2020 & beyond: reaping the dividends of cyber resilience": http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html
[7] EBF "The EBF blueprint for digital banking and policy change": http://www.ebfdigitalbanking.eu/EBFDB_2.html
[8] PwC "Insurance 2020 & beyond: reaping the dividends of cyber resilience": http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html
[9] EC priority Digital Single Market "Bringing down barriers to unlock online opportunities": https://ec.europa.eu/priorities/digital-single-market_en

The use of mobile devices for both online banking and the purchase of goods and services (both online and in person) has increased dramatically over the last couple of years. With this increase in usage, there has been a corresponding increase in the threats affecting payments. Innovations in mobile payment options facilitate adoption of the technology by consumers and businesses, but also increase the interest of fraudsters to steal money, payment card information or history of operations.

In 2015, a Mobile Payments Security Study conducted by ISACA mentioned that "the global mobile payment market, will be worth an estimated US $2.8 trillion by 2020, according to Future Market Insights. As the use of mobile payment picks up speed, the associated risks grow as well." More than 900 ISACA cyber security member experts participated in the study reaching the following conclusions:

- Only 23% believe that mobile payments are secure in keeping personal information safe
- Nearly half (47%) say mobile payments are not secure and 30% are unsure
- 87% expect to see an increase in mobile payment data breaches over the next 12 months, yet 42% of respondents have used this payment method in 2015

On the supply side, the introduction of new technologies, smartphones, tablets, and new security solutions make it easier and safer to leverage the opportunities of digital infrastructure combined with the trust offered by the banking industry. Digital banking is much more than home banking, it's about making the entire customer experience convenient, whether this is for e-commerce, or trading activities, if it is leveraged in proximity use cases or remotely.

On the demand side, another very important consideration is the demographic evolution. At present, and even more in the future, the demand side will be led by generations of people that have higher education, are acquainted with the use of the internet and English, have more and more digital devices, and less borders. Millennials (Generation Y) and Digital Natives (Generation Z) are the born European citizens, their mind-set is different, the new generations have a fast and open approach to whatever is offered on the market. In the future, the digital banking services must be able to cope with the rapid evolution of the Digital Single Market. Studying, travelling, buying, working, trading is going to be done, at least at European level, by leveraging a borderless digital environment that is part of daily life. Ensuring a safe cross-border digital banking environment is therefore the basic requirement for the smooth growth of European economy.

A new paradigm shift could take place with the introduction of quantum computing. While addressing the roll-out of consolidated innovation technologies (i.e. mobile payments), the struggle moves forward at the forefront of innovation frontiers. The quantum era will usher in a new phase in the eternal race between defenders and attackers of our sensitive data. Cryptography will be the battlefield on which this war of the future will be fought, the contenders of which are already preparing for a confrontation that could take place in the coming years. Quantum computing could be able to break most of the current encryption algorithms, especially those based on public keys, on the other hand, it could also create new unbreakable codes. Quantum cryptography will make things very difficult for cyber criminals, while current encryption systems are secure because intruders who attempt to access information can only do so by solving complex problems.

Another interesting characteristic of the security market is linked to cloud computing. Historically, financial institutions have been reluctant to bring any part of their data to outsourcing, and when these kinds of decisions were taken a due diligence on the providers datacentre was the first step of any due diligence assessment. In recent years, financial institutions have also widely adopted

solutions offered in SaaS mode and have adopted cloud based architectures for some services. As cloud environments grow, data privacy issues and cyber threats are expanding and even becoming international. These issues are raising many legal questions for firms making data centre and cloud operation decisions. In a not atypical scenario, a cloud involves a diversified file system with data in multiple physical locations sitting in public and private clouds. This is something which could lead to cross border investigations in the event of data breaches, the potential reach for such investigations should be viewed in the context of the impending data regulations that will come out of the EU. Some of these risks are linked to weak cloud security measures of the services, such as storing data without controls such as encryption, or lack of multi-factor authentication to access the service. According to a recent Gartner[10] study the highest growth will come from cloud system infrastructure services (infrastructure as a service [IaaS]), which is projected to grow 36.8 percent in 2017 to reach $34.6 billion. Cloud application services (software as a service [SaaS]) is expected to grow 20.1 percent to reach $46.3 billion. The recent evolution of the financial sector mind-set is that cloud computing, given the distributed architecture, could in turn be a success factor in tackling Disaster Recovery and Business Continuity, thus it could also be considered a risk mitigation factor.

[10] "Forecast: Public Cloud Services, Worldwide, 2014-2020, 4Q16 Update." – Gartner 2017

References

Cybersecurity Venture “Cybersecurity Market Report – Q3 2016”: http://cybersecurityventures.com/cybersecurity-market-report/

EBF “The EBF blueprint for digital banking and policy change”: http://www.ebfdigitalbanking.eu/EBFDB_2.html

European Commission “Consumer Financial Services Action Plan: Better products and more choice for European consumers”; March 2017

European Commission priority Digital Single Market “Bringing down barriers to unlock online opportunities”: https://ec.europa.eu/priorities/digital-single-market_en

Gartner "Forecast: Public Cloud Services, Worldwide, 2014-2020, 4Q16 Update.", 2017

KPMG advisory “Digital banking 2017“; March 2017

Ponemon Institute “2016 Cost of Cyber Crime Study & the Risk of Business Innovation”; October 2016

PwC “Insurance 2020 & beyond: reaping the dividends of cyber resilience”: http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html

PwC “Insurance 2020 & beyond: reaping the dividends of cyber resilience”: http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html