SUERF
THE EUROPEAN MONEY AND FINANCE FORUM

**SUERF Policy Note**
**Issue No 206, November 2020**

# Cyber risk in the financial sector

By Iñaki Aldasoro, Jon Frost, Leonardo Gambacorta, Thomas Leach and David Whyte*

*JEL codes: D5, D62, D82, G2, H41.*

*Keywords: Cyber risks, financial institutions, value-at-risk.*

*Cyber attacks on financial institutions and financial market infrastructures have become more frequent and sophisticated, prompting ever-larger investments and efforts. This note explores causes, considers the specific vulnerabilities of the financial sector, examines costs and financial stability implications and outlines possible policy responses. International cooperation is key, as authorities face similar issues and cyber resilience is, fundamentally, a global public good.*

* Iñaki Aldasoro, Jon Frost, Leonardo Gambacorta and David Whyte are with the Bank for International Settlements (BIS); Thomas Leach is with the University of Pavia.

The views expressed in the note belong to the authors and are not necessarily the views of the BIS. The authors would like to thank Claudio Borio, Stijn Claessens and Hyun Song Shin (BIS) and Paolo Giudici (University of Pavia) for comments and suggestions. Thomas Leach acknowledges support from the European Union's Horizon 2020 training and innovation programme "FIN-TECH", under the grant agreement No. 825215 (Topic ICT-35-2018, Type of actions: CSA).

## 1. Introduction

The financial sector has long been spearheading cyber security enhancements, with many regulatory and industry-wide initiatives. However, cyber attacks on financial institutions and financial market infrastructures (FMIs) have become more frequent and sophisticated, prompting ever-larger investments and efforts. In parallel, financial institutions, regulators, national governments and international groups have been working to improve overall operational resilience and ensure financial stability. The threat landscape has evolved further since the outbreak of the Covid-19 pandemic, not least due to the higher prevalence of work-from-home (WFH) arrangements and the associated demands on IT systems.

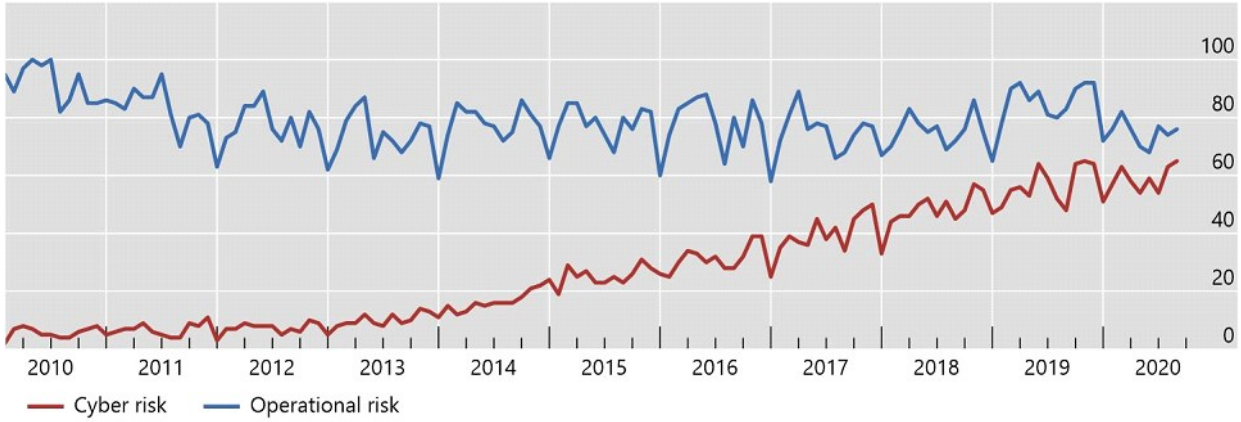
This note offers a taxonomy of cyber incidents. It explores causes, considers the specific vulnerabilities of the financial sector, examines costs and financial stability implications and outlines possible policy responses. International cooperation is key, as authorities face similar issues and cyber resilience is, fundamentally, a global public good (Carstens, 2019; Cœuré, 2019).

## 2. Cyber risk: taxonomy and specificity

Cyber risk is receiving growing attention. Graph 1 reports the number of online searches for "cyber risk" over the last decade and compares it with that for "operational risk". Despite the fact that cyber risk is only a subset of a firm's operational risk, worldwide search interest for the two terms is today almost on a par. Despite growing public concerns about cyber risk, there is still no commonly agreed definition.[1] Broadly speaking, cyber risk is understood to be the risk of financial loss, disruption or reputational damage resulting from the failure of IT systems. Cyber attacks are one type of cyber risk.

Interest in cyber risk is on par with operational risk[1]

Search interest, index — Graph 1




[1] Number of worldwide searches for "cyber risk" and "operational risk" relative to the highest point (=100). Data accessed on 20 Aug 2020.

Source: Google Trends.

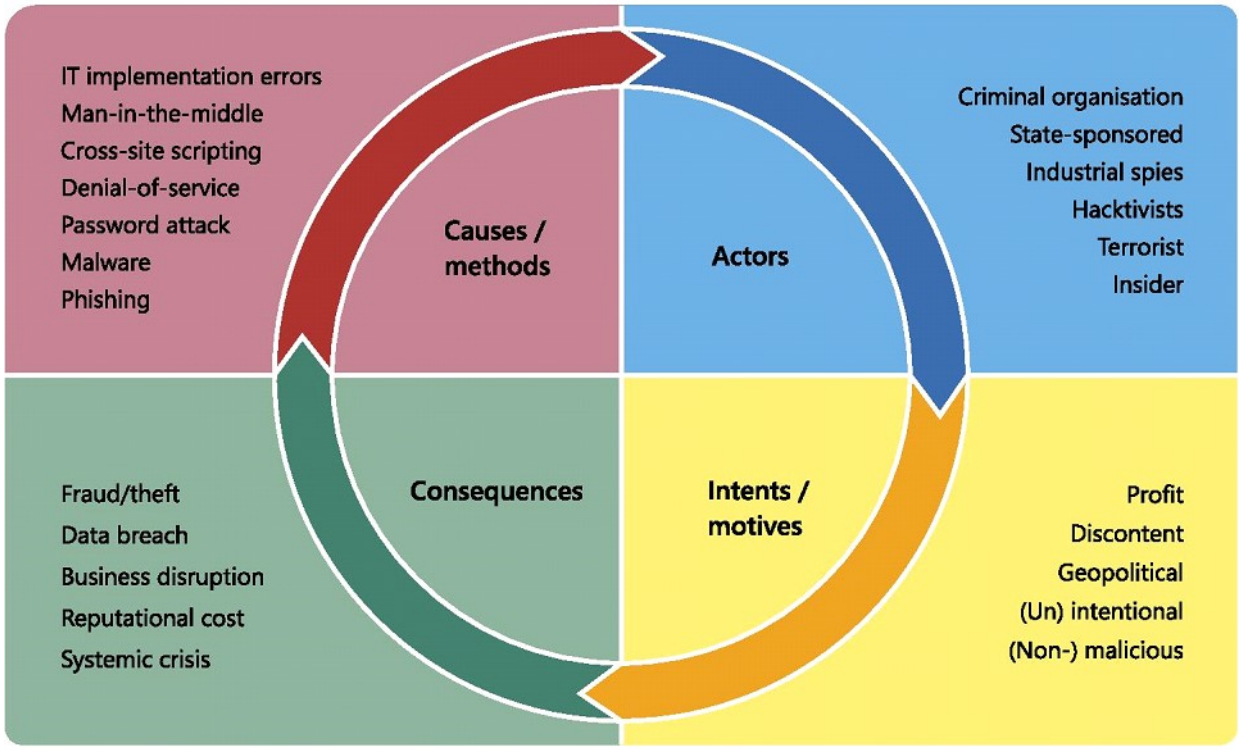
[1] According to the Financial Stability Board (FSB) Cyber Lexicon, cyber risk refers to "*the combination of the probability of cyber incidents occurring and their impact*". A "cyber incident", in turn, is *"any observable occurrence in an information system… that: (i) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not"*. Besides the FSB Cyber Lexicon, there are a number of glossaries or lexicons of cyber security terms, including the US Department of Defense Dictionary of Military and Associated Terms, and the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms.

Cyber incidents have a number of dimensions. Graph 2 provides a taxonomy, based on four categories: cause, actor, intent and consequence (Curti et al. 2019).

The **causes** can be very different, including both unintended incidents and intentional attacks. Examples of the former include accidental data disclosure as well as errors in implementation, configuration and processing in IT systems. The best known causes (methods) of cyber attacks are malware, cross-site scripting, phishing, password cracking, zero-day exploits, and denial-of-service and man-in-the-middle attacks.

The **actors** vary. They include outright criminal and terrorist organisations, industrial spies, "hacktivists" (such as the Anonymous group), or state and state-sponsored players. The damage they can cause depends on their sophistication and resources. For example, in 2016, hackers associated with North Korea carried out a notable attack by breaching the systems of Bangladesh Bank and using the SWIFT network to send fraudulent money transfer orders.[2] The attack highlighted rising cyber risks for payment systems and associated infrastructures.[3]

A simple taxonomy of cyber risks — Graph 2




The examples for each category are not meant to be exhaustive.

Source: BIS elaboration.

[2] See Bangladesh Bank and Federal Reserve Bank of New York, "Joint Statement", 1 February 2019.

[3] In response to ever more sophisticated attacks, SWIFT launched its Customer Security Programme (CSP) in 2016 (see SWIFT, 2019).

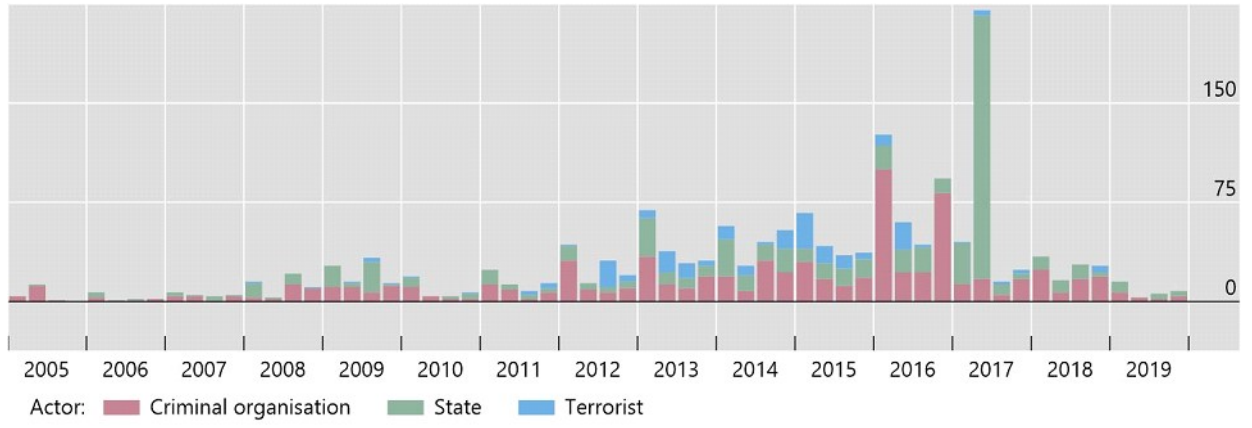
Graph 3 shows the number of cyber incidents by types of external actor over the period 2005–19. Criminal organisations have been the most common threat actors. In 2016 and 2017, more incidents came from state actors, including the Bank Bangladesh attack. More recently, state actors are suspected to have initiated the WannaCry attacks[4] and numerous hacks of crypto-asset trading platforms.

As regards **intent**, around 40% of cyber incidents are intentional and malicious, rather than accidental, ie they are "cyber attacks" (Aldasoro et al., 2020b). The ultimate purpose can be profit (eg ransomware, industrial spying), geopolitical (state-sponsored attacks on critical infrastructures) or general discontent (hacktivism).

The **consequences** of cyber incidents can be monetary and/or reputational. They can involve a loss of the *confidentiality, integrity* or *availability* of assets and services. Business disruptions and IT system failures can damage integrity and availability. Data breaches compromise confidentiality, with financial and reputational losses. Fraud and theft include the loss of funds or any information (eg intellectual property) that may or may not be personally identifiable. In some circumstances, cyber attacks could have systemic implications and cause serious economic dislocations.

Frequency of cyber incidents by external actors

Number of incidents — Graph 3




Source: I Aldasoro, L Gambacorta, P Giudici and T Leach, "The drivers of cyber risk", *BIS Working Papers*, no 865, May 2020.

The risks and consequences of cyber attacks differ from generic IT risks for at least three reasons. First, cyber attacks are malicious. Second, they are highly scalable, ie they can spread rapidly through copycat attacks or perhaps occur simultaneously due to common sources of vulnerability across IT systems and institutions. Third, they are constantly evolving, with threat actors responding to countermeasures.

The rapid evolution of the cyber attack landscape is challenging authorities' ability to assess the threats adequately. In the past, sophisticated targeted intrusions were the exclusive domain of nation states, as they alone possessed the necessary motivation, resources and technical talent to penetrate well defended networks. However, this is no longer the case. Sophisticated exploit tools and software frameworks are widely available on

[4] The WannaCry attack, conducted in May 2017, involved the use of ransomware that encrypted data (including sensitive medical data) and demanded ransom payments in Bitcoin on targeted computers. For information on this attack and others attributed to North Korean groups, see US Treasury (2019).

the internet at no or little cost, lowering entry barriers. Crimeware as a service (CaaS) is a viable business model whereby criminal actors for hire utilise state-of-the-art attack tools and techniques against specified targets. Perhaps most worrisome are firms that conduct research to identify zero-day exploits,[5] which are then offered for sale.

The operational disruptions of the Covid-19 pandemic may have opened up new possibilities for attacks. Evidence to date suggests that the causes, actors and intent of such attacks have been broadly similar to those pre-pandemic (CERT-EU, 2020). Yet there has been a sharp rise in Covid-related phishing, for instance e-mails or attachments that purport to hold information related to Covid-19 and in fact carry malware. Given the widespread use of WFH arrangements, threat actors are able to leverage operational uncertainty and the use of personal devices. For instance, the use of remote access technologies such as the Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) has increased by 41% and 33%, respectively, since the onset of the Covid-19 outbreak (ZDNet, 2020). Unless well managed, this may allow new opportunities for threat actors to penetrate IT systems and carry out cyber attacks (Crisanto and Prenio, 2020). WFH may also challenge business continuity plans and the response to an operational or cyber incident (CPMI, 2020).

## 3. Quantifying the costs and risks in the financial sector

The financial sector is particularly vulnerable. Zakrzewski et al. (2019) finds that financial services firms are 300 times more likely to be targeted than others. This may reflect that successful criminal attacks on financial firms could be particularly rewarding. Accounts, customer information, associated transactions as well as backup systems are all digitised (Brenner, 2017). And the consequences may have larger systemic implications, owing to the high degree of interconnectivity, nationally and internationally.

Unsurprisingly, the financial sector, where telework is more common, has seen a growing incidence of cyber attacks since the end of February 2020. According to a survey conducted by Financial Services Information Sharing and Analysis Center (FS-ISAC, 2020) among financial institutions, there has been a substantial increase in phishing, suspicious scanning and malicious activity against webpages for WFH staff to access the network. Payment firms, insurance companies and credit unions have seen the strongest increase (Aldasoro, Frost, Gambacorta and Whyte, 2020).

The costs of cyber incidents more generally are difficult to quantify. One limitation is the paucity of data. This is due, in particular, to the lack of a common standard for recording them and, importantly, to the victims' reluctance to report due to reputational concerns. For example, in the United Kingdom, only 49 cyber attacks were reported to financial authorities in 2017 (Butler, 2017).

Using a unique database of more than 100,000 cyber incidents across sectors, Aldasoro et al. (2020b) documents the main drivers and costs of cyber incidents (for more details see Box A).[6] For the firms affected, the average cost per incident across all industries over the 2002–19 period was $2.6 million. While the average frequency

[5] A zero-day exploit is an attack against a software or hardware vulnerability that has been discovered but not publicly disclosed. Their discovery can result in a situation where both vendors and customers are exposed to a cyber attack for which detection signatures and remedial patches are not available.

[6] The data set is from Advisen, a for-profit organisation that collects the data from reliable and publicly verifiable sources such as websites, newsfeeds, specialised legal information services, multiple online data breach clearing houses and federal and state governments in the United States. The data are not based on self-reporting, reducing concerns related to underreporting of cyber incidents. For alternative estimates of cyber risks using Advisen data, see also Romanosky (2016) and Chande and Yanchus (2019).

was around six times higher for the financial sector, the cost was lower, at around $1.7 million, probably due to regulation and supervision. Fraud accounts for 49% of events, data breaches for 46% and business disruption for the remaining 5% (61%, 37% and 2% in the financial sector, respectively). Cyber attacks have, on average, lower costs, because most incidents simply reflect general discontent. However, some actors seek a profit or to inflict the largest possible losses and damage. Incidents related to crypto-exchanges, which are largely unregulated, produce higher losses.

## Trends and drivers of cyber costs: is the financial sector different? Box A

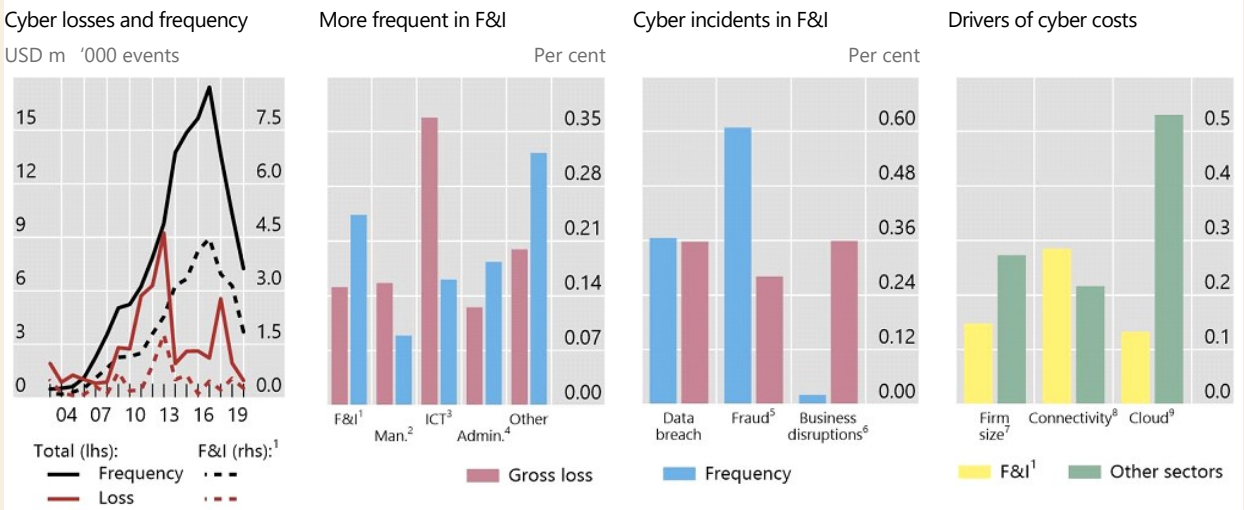
Despite growing attention, little is known about cyber incidents, their drivers, costs and mitigating factors. A recent study by Aldasoro et al. (2020b) investigates the drivers of cyber costs across sectors using a unique data set from Advisen of over 100,000 cyber incidents.

The frequency of cyber incidents rose strongly in the decade to 2016, but has since receded somewhat (Graph A1, left-hand panel). This reduction could reflect increased investment in cyber security, but also delays in discovery or reporting.

Cyber incidents are more frequent in the financial sector. A quarter of all cyber incidents affected the finance and insurance sector (F&I) (second panel). While the numbers are higher, the corresponding gross losses are not necessarily larger. Fraud, notably in the form of privacy violations and phishing/skimming scams, is most frequent but least costly (third panel). Data breaches are both relatively frequent and costly, while business disruptions are quite infrequent but can have high costs.

The study has several other findings. The cost of cyber incidents is generally larger for bigger firms, but this effect is smaller for the financial sector (the first two columns in the fourth panel indicate the relationship between cyber cost and firm size). Cyber incidents can be interconnected, ie a single incident can hit several organisations at the same time. The higher this connectivity, the higher the cost, especially for financial firms (third and fourth columns in the fourth panel). Cloud technology can reduce IT costs, improve resilience and enable firms to scale better. However, the use of cloud services is associated with lower costs only for minor cyber incidents. When cyber incidents are large, there is no visible effect. Moreover, this effect is significantly smaller for the financial sector (last two columns in fourth panel). As cloud use increases and cloud providers become systemically important, cloud dependence is likely to increase tail risks.

Cyber events and losses across sectors Graph A1




[1] Finance and insurance. [2] Manufacturing and retail trade. [3] Information and Communications, and Professional, Scientific and Technical Services. [4] Administration and Support. [5] Phishing/skimming and privacy violations. [6] IT implementation errors, security incidents and other. [7] Elasticity of cyber costs with respect to the log of firm revenues. [8] Marginal effect. Connectivity refers to the number of cyber incidents connected to any given cyber event. [9] Cloud refers to reliance on cloud services at the industry level. For presentational purposes, coefficients have been multiplied by minus one and represent marginal gains.

Sources: Aldasoro et al. (2020b); Advisen.

These estimates consider the average actual (ex post) costs of cyber incidents, but do not take into account the (ex ante) risk of tail events. Value-at-risk models consider unexpected losses that materialise in particularly adverse scenarios. Using ORX data, Aldasoro et al. (2020a) suggests that, while cyber losses are on average a very small fraction of banks' total operational risk losses, the distribution could be quite skewed and cyber risk could account for up to a third of total operational value-at-risk (for more details see Box B).[7] These estimates do not consider contagion effects. According to some estimates by Bouveret (2018) based on data collected from media and newspaper articles over the 2009–17 period, the value-at-risk for the whole banking sector, taking into account contagion effects, could amount to 14–19% of banks' aggregate net income.[8] Moreover, bottom-up stress testing by the Monetary Authority of Singapore suggests that, without specific mitigating measures, severe direct and indirect cyber attacks could reduce aggregate banks' total capital adequacy ratios by up to 0.4 percentage points.[9]

## 4. Cyber risk and financial stability

A business disruption to a large financial institution and/or FMI can have a significant systemic impact, beyond the financial system (Kopp et al., 2017). Risk concentration, interconnections and the lack of substitutes in the case of FMIs contribute to spillover effects. Models that take spillover effects across sectors into account suggest that the losses could be sizeable. Dreyer et al. (2018) suggests that the cost of cyber crime for all economic sectors could be substantial, at more than 1% of global GDP.[10] The quantification of the systemic impact depends on a number of assumptions and can be assessed from at least three different angles.

A first angle focuses on **potential scenarios** (Boer and Vazquez, 2017; MAS, 2018; ESRB, 2020). These can include a cyber attack affecting the availability of a major payments system or FMI, or a breach that compromises confidentiality of key financial or personal data. For instance, Kopp and Kaffenberger (2019) consider a scenario in which a central counterparty (CCP) is the subject of a cyber attack. Intentional data manipulation could be especially damaging, as it may erode confidence, triggering feedback loops, and require a prolonged recovery period. In cases where the intent is to cause damage, eg as part of a terrorist attack or as a form of cyber warfare, costs may be much higher than in the case of theft.

[7] ORX is a consortium founded by banks with the aim of sharing operational loss risk data in an anonymised fashion in order to benchmark operational risk models. The sample includes a group of 74 large banks from North and Latin America, Asia-Pacific, Europe and Africa.

[8] Contagion is introduced in the model by assuming that each cyber attack has a probability of affecting one or several firms (Bouveret, 2018).

[9] Damages could be larger in the case of data damage-related attacks, eg corruption of data from a data service provider (see MAS, 2019).

[10] The study defines a methodology that identifies the value-at-risk from cyber incidents by country and industry sector and computes the systemic costs of cyber risk between industry sectors from 60 countries (for more info see Dreyer et al. 2018).

## Operational and cyber risks in the banking sector **Box B**

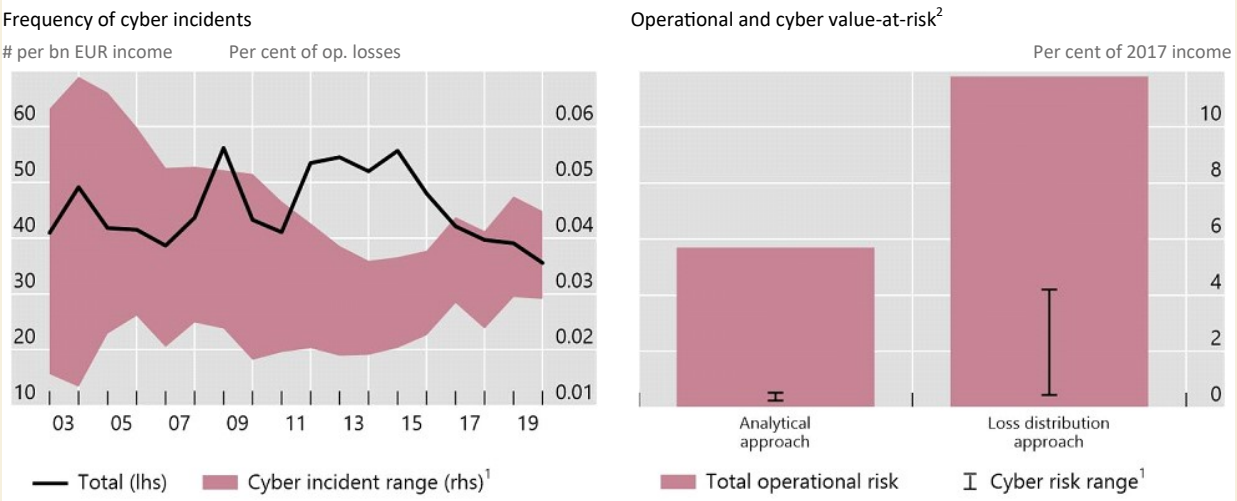
Cyber- and IT-related risks are a subset of operational risk. A recent research by Aldasoro et al. (2020a) investigates operational and cyber risks using a unique cross-country data set from ORX of over 700,000 operational loss events at 74 large banks across the globe. The study leverages a granular classification of operational risk events to construct a range for the frequency and cost of cyber risk.

Cyber losses represent a small share of banks' overall operational losses (less than 0.2%). The frequency of cyber incidents is small in relation to all operational risk events (Graph B1, left-hand panel) but it has increased in recent years.

One way to assess potential losses from cyber incidents is by estimating value-at-risk (VaR) measures. The VaR indicates the level of risk to which a firm, a portfolio or a single position may be exposed over a given time period. Estimates suggest that in the sample considered the operational VaR ranges from around 6% to 12% of income, depending on the method used (right-hand panel). The cyber VaR, in turn, can range from 0.2% to 4.2% of income. This amounts to around a third of operational VaR. Cyber VaR could indeed be relatively high because – although cyber risk incidents are relatively far less frequent and, on average, less costly – they could in extreme cases be particularly damaging.

The seriousness of operational and cyber risks depends on the supervisory environment. A higher quality of supervision – as measured by a financial and supervisory quality index – goes hand in hand with smaller and less frequent losses.

Cyber risk in the financial sector small but growing relative to operational risk **Graph B1**




[1] Min-max range as a percentage of total operational risk. The range is obtained from the level 2 classification of operational risk events under the Basel Framework, www.bis.org/basel_framework/chapter/OPE/30.htm?inforce=20191215. The minimum includes the categories ET0103 (Intentional damage to systems by internal staff), ET0202 (Wilful damage, eg hacking, software/hardware, theft of data) and ET0601 (Technology & infrastructure failures). The maximum estimate adds ET0101 (Internal fraud – Unauthorised activity), ET0102 (Internal theft & fraud) and ET0201 (External theft & fraud). [2] Losses are extrapolated from the tail (99.9th percentile of the distribution) based on the parameters of an assumed probability distribution over one year. The analytical approach is based on the internal measurement of losses and allows the VaR to be derived analytically. The loss distribution approach takes better account of the fat-tailed nature of operational loss data, and is estimated with Bayesian techniques.

Sources: Aldasoro et al. (2020a); ORX.

A second angle focuses on **transmission channels**. These include spillovers through the payments system. For example, Eisenbach et al. (2019) find that, if any of the five most active US banks were impaired for a full day, this could affect 38% of the banking network and cost more than USD 210 billion (2.5 times daily GDP) in foregone

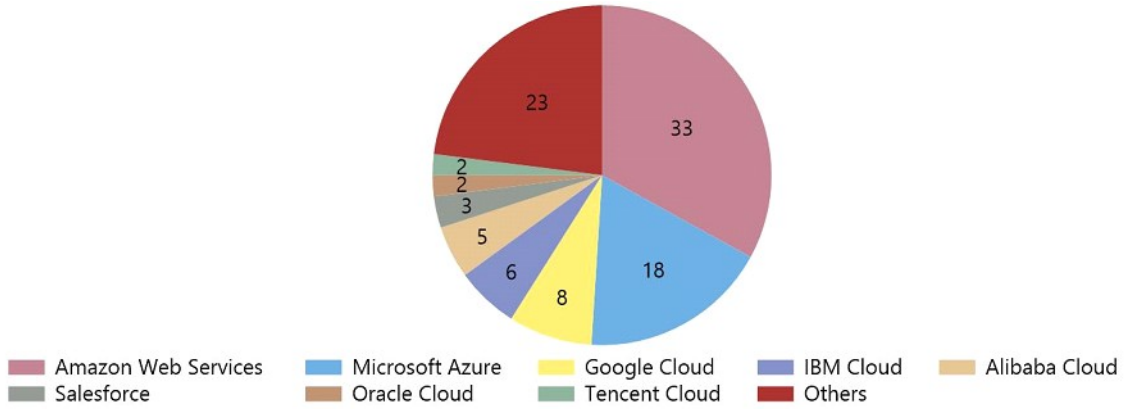
payment activity.[11] Another study by Duffie and Younger (2019) traces how there could be serious and contagious wholesale bank runs if the US payment and settlement system went offline during the day.[12] Using Australian data, Clarke and Hancock (2019) found that disruptions at one large bank could result in up to AUD 38 billion of unsettled payments (7.5 times daily GDP) – though the systemic impact could be substantially offset by liquidity-saving measures in the real-time gross settlement (RTGS) system.[13]

The third angle focuses on **growing third-party dependencies**. Reliance on cloud computing is increasing rapidly. Evidence suggests that firms using the cloud have so far seen lower cyber losses (Box A). However, the market for cloud services is highly concentrated (Graph 4), and there are warnings about increased homogeneity in the financial sector and the greater risk of single points of failure (Danielsson and Macrae, 2019; FSB, 2019, BCBS, 2018).[14] A recent survey indicates that 82% of companies increased cloud usage as a result of the coronavirus pandemic and 91% are planning a more strategic use of cloud in the near future (Snow, 2020). Through shared software, hardware and vendors, incidents could, in principle, spread more quickly, leading to higher losses for financial institutions and stress in the financial system (Welburn and Strong, 2019). In the first four months of 2020, cyber threats targeting cloud services increased by six times in the financial industry (McAfee, 2020).

The market for cloud services is highly concentrated[1]

In per cent

Graph 4




[1] The graph reports the share of each firm in the Cloud Infrastructure-as-a-Service (IaaS) market, across all industries, as of Q4 2019.

Source: Synergy Research Group.

[11] Impacts would be even more disruptive on days with higher payments activity and in counties with more concentrated banking markets (see Eisenbach et al., 2019).

[12] This study analyses a sample of 12 systemically important US financial institutions. It suggests that these firms have sufficient stocks of high-quality liquid assets to cover wholesale funding runoffs in a relatively extreme cyber event, but that the disruption could damage the real economy (see Duffie and Younger, 2019).

[13] The AUD 38 billion refers to the daily average of unsettled payments in the Reserve Bank Information and Transfer System (RITS) replica model under the assumption of no reaction, and including unsettled payments resulting from a 30% reduction in liquidity in the systems with bilateral offset. If the reaction time were limited to two hours, the unsettled payments could be reduced to AUD 15 billion (see Clarke and Hancock, 2019).

[14] For a discussion of cloud service providers as critical infrastructures and potential policy responses, see Carr et al. (2019).

## 5. How can systemic vulnerabilities be mitigated?

Policymakers and businesses are actively working together to mitigate cyber risks and their systemic implications. These efforts fall into four areas.

First, many private and public sector organisations are strengthening their **operational resilience**. In many cases, this involves aligning security activities with business objectives and prioritising cyber security investments. It also involves instilling an "assume-breach" mentality at both the operational and governance levels. Organisations can also learn from each other. For instance, the BIS has recently created a Cyber Resilience Coordination Centre (CRCC). Its objective is to provide a structured and trusted approach to knowledge-sharing and collaboration among central banks.[15] While global information-sharing and regulatory cooperation on cyber risk may be constrained due to the topic's political sensitivity, the central banking community may be more able to foster open dialogue. The need for coordination and common policy responses is particularly high during the current pandemic due to the shared nature of vulnerabilities in a WFH environment.

Second, financial supervisors and overseers are leveraging national or international **standards or guidance** to promote cyber resilience (CPMI-IOSCO, 2016; US NIST, 2018; ISO/IEC, 2018). In many cases, authorities are using existing regulatory and supervisory tools to set expectations for cyber risk management, testing and incident response.[16] Many authorities are adopting a principles-based approach, and are emphasising response and recovery rather than prevention (FSB, 2020; BCBS, 2020). Some are engaging in testing or simulations of actual cyber incidents, in cooperation with the financial sector.[17] Globally, the CPMI and IOSCO have issued guidance on cyber resilience for FMIs, and have since been engaging with the industry to promote practices set out in the guidance. The CPMI has also developed a global strategy on reducing risks of wholesale payments fraud related to endpoint security (CPMI, 2018; 2019). In addition to global initiatives, there are also several regional groups and cooperation forums.[18]

Third, several **private sector-led initiatives** are under way.[19] These can support cooperation and coordination in incident prevention, response and recovery, and information-sharing. To help mitigate cyber risks from third-

[15] The CRCC has developed three lines of activity. First, it has set up a "cyber range". The range replicates actual attacks and couples them with "live" testing of incident response capabilities in a realistic but simulated and controlled test environment. Second, the CRCC's Annual Cyber Security Seminars seek to strengthen and coordinate best practice in the central bank community. Third, the BIS is working with the Carnegie Mellon Software Engineering Institute (CERT/SEI) on a customised operational resilience assessment framework to help central banks self-assess their cyber security posture.

[16] For a description of the range of practices in different jurisdictions, see BCBS (2018), FSB (2017) and IAIS (2016).

[17] For the United States, see Mester (2019). The United Kingdom has the CBEST framework and the ECB has a threat intelligence-based ethical red-teaming (TIBER) framework.

[18] For example, in the European Union, the European Systemic Risk Board (ESRB) and ECB have worked on financial stability risks that could stem from cyber incidents. In Asia, the Association of Southeast Asian Nations (ASEAN) has a Cyber Capacity Development Project in cooperation with Japan, and in 2019 launched a Singapore-ASEAN Cybersecurity Centre of Excellence. In Latin America, the FSI, CEMLA and ASBA have convened discussions of central banks and regulators on cyber risk.

[19] This includes initiatives such as computer emergency response teams (CERTs) at the national level, and the Forum of Incident Response and Security Teams (FIRST) at the global level. Finally, the FS-ISAC is an international effort with the aim of reducing cyber risk in the financial sector. It does this by providing a platform to share actionable threat intelligence whilst providing resiliency resources and fostering a trusted collaborative peer-to-peer network of experts.

party dependencies in cloud services, financial institutions are cooperating on frameworks for data portability and interoperability across cloud providers (FSB, 2019; G7, 2018).

Fourth, **cyber insurance** markets are developing (Biener et al., 2015). Cyber insurance could help firms to cover losses and encourage improvements in cyber resilience. That said, such coverage may be insufficient to avoid large tail risks, and may even work to spread the losses from systemic shocks.

## 6. Conclusions

The digital revolution has increased the interconnectivity and complexity of the economy and financial system. The use of technology and the internet have improved financial sector productivity, but also make it more vulnerable to the spread of viruses and malware. Moreover, the greater use of cloud services exposes the system to further to common risks, thus increasing the potential for systemic cyber attacks.

Despite the large and growing exposure to cyber risks, cyber costs are difficult to define and quantify. This note offers a taxonomy of cyber incidents. It explores causes, considers the specific vulnerabilities of the financial sector, examines costs and financial stability implications and outlines possible policy responses.

Policymakers and businesses are actively working together to mitigate cyber risks and their systemic implications. Cooperation efforts fall into four areas. First, many private and public sector organisations are strengthening their operational resilience. In many cases, this involves aligning security activities with business objectives and prioritising cyber security investments. Second, financial supervisors and overseers are leveraging national or international standards or guidance to promote cyber resilience. Third, private sector-led initiatives are under way to support cooperation and coordination in incident prevention, response and recovery, and information-sharing. Fourth, cyber insurance markets are developing. Looking forward, these efforts are increasingly important to protect levels of remote working that will likely remain higher than they were prior to the Covid-19 pandemic. ■

## References

Aldasoro I., Frost. J., Gambacorta L. and D. Whyte (2020). "Covid-19 and cyber risk in the financial sector", BIS Bulletin, forthcoming.

Aldasoro I., Gambacorta L., Giudici P. and Leach T. (2020a). "Operational and cyber risks in the financial sector", *BIS Working Papers*, 840, February.

Aldasoro I., Gambacorta L., Giudici P. and Leach T. (2020b). "The drivers of cyber risk", *BIS Working Papers*, 865, May.

Basel Committee on Banking Supervision (BCBS) (2018). "Cyber-resilience: range of practices", December.

Basel Committee on Banking Supervision (BCBS) (2018). "Sound Practices: implications of fintech developments for banks and bank supervisors", February.

Basel Committee on Banking Supervision (BCBS) (2020). "Principles for operational resilience", August.

Biener C., Eling M. and Wirfs J. (2015). "Insurability of cyber risk: An empirical analysis", *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1): 131–58.

*continued*

Boer M. and Vazquez J. (2017). "*Cyber security and financial stability: how cyber-attacks could materially impact the global financial system*", Institute of International Finance, working paper.

Bouveret A. (2018). "Cyber risk for the financial sector: A framework for quantitative assessment", *IMF Working Papers*, 18/143.

Brenner J. (2017). "Keeping America safe: toward more secure networks for critical sectors", MIT Center for International Studies and MIT Internet Policy Research Initiative, March.

Butler M. (2017). "Effective global regulation in capital markets", speech at the ICI Conference, London, 5 December.

Carr B., Pujazón D. and Vazquez J. (2019). "*CSPs and criticality: potential treatments and solutions",* Institute of International Finance, working paper.

Carstens A. (2019). "A handful of cyber – five key issues for international cooperation", speech, 10 May.

CERT-EU (2020). "COVID-19 Cyber Bulletin #9", 6 May 2020.

Chande N. and Yanchus D. (2019). "The cyber incident landscape", Bank of Canada, Staff Analytical Note, 32.

Clarke A. and Hancock J. (2013). "Payment system design and participant operational disruptions", *Journal of Financial Market Infrastructures*, 2(2).

Cœuré B. (2019). "Cyber resilience as a global public good", speech, 10 May 2019.

Committee on Payments and Market Infrastructure (CPMI) (2020). "Handling stress events during a pandemic", 23 July.

Committee on Payments and Market Infrastructure (CPMI) (2018). "Reducing the risk of wholesale payments fraud related to endpoint security", May.

Committee on Payments and Market Infrastructure (CPMI) (2019). "Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit", October.

Committee on Payments and Market Infrastructures (CPMI) and Board of the International Organization of Securities Commissions (IOSCO). (2016). "Guidance on cyber resilience for financial market infrastructures", June.

Crisanto J.C. and Prenio J. (2020). "Financial crime in times of Covid-19 – AML and cyber resilience measures", FSI Brief, no 7.

Curti F., Gerlach J., Kazinnik S., Lee M. and Mihov A. (2019). "Cyber risk definition and classification for financial risk management", Federal Reserve Bank of St Louis, mimeo.

Danielsson J. and Macrae R. (2019). "Systemic consequences of outsourcing to the cloud", VoxEU, 2 December.

Dreyer P., Jones T., Klima K., Oberholtzer J., Strong A., Welburn J. and Winkelman Z. (2018). "Estimating the global cost of cyber risk", Research Report, no RR-2299-WFHF, Rand Corporation.

Duffie D. and Younger J. (2019). "Cyber runs", *Hutchins Center Working Papers*, 51, Brookings Institution, 2019.

Eisenbach T., Kovner A. and Lee M. (2019). "Cyber risk and the U.S. financial system: a pre-mortem analysis", Federal Reserve Bank of New York, December 2019.

European Systemic Risk Board (ESRB) (2020). "Systemic cyber risk", February 2020.

*continued*

Financial Services Information Sharing and Analysis Center (FS-ISAC) (2020). "COVID-19 effects on cybersecurity survey", July.

Financial Stability Board (FSB) (2017). "Stocktake of publicly released cybersecurity regulations, guidance and supervisory practices", October.

Financial Stability Board (FSB) (2019). "Third-party dependencies in cloud services: Considerations on financial stability implications", December.

Financial Stability Board (FSB) (2020). "Effective practices for cyber incident response and recovery", April.

Group of seven (G7) (2018). *Fundamental elements for third party cyber risk management in the financial sector*, October.

International Association of Insurance Supervisors (IAIS) (2016). "Issues paper on cyber risk to the insurance sector", August.

International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) (2018). "Information technology - Security techniques - Information security management systems", February.

Kopp E. and Kaffenberger L. (2019). "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment", Carnegie Endowment Cyber Policy Initiative Working Paper, 4, September.

Kopp E., Kaffenberger L. and Wilson C. (2017). "Cyber risk, market failures, and financial stability", *IMF Working Papers*, 17/185.

Mester L. (2019). "Perspectives on Cybersecurity, the Financial System and the Federal Reserve", speech, April.

McAfee (2020). "Cloud adoption and risk report", May.

Monetary Authority of Singapore (MAS) (2018). *Financial stability review*, November.

Monetary Authority of Singapore (MAS) (2019). *Financial Stability Review*, November.

Romanosky S. (2016). "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, 2: 121–13.

Snow (2020). "How the 'new normal' is changing cloud usage and strategy", 16 June.

SWIFT (2019). "Three years on from Bangladesh - Tackling the adversaries", April.

US National Institute of Standards and Technology (NIST) (2018). "Framework for improving critical infrastructure cybersecurity", 16 April.

US Treasury (2019). "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups", September.

Welburn J. and Strong A. (2019). "Systemic cyber risk and aggregate impacts", Working Paper, WR-1311, RAND Corporation.

Zakrzewski A., Tang T., Appel G., Fages R., Hardie A., Hildebrandt N., Kahlich M., Mende M., Muxí F. and Xavier A. (2019). "Global Wealth 2019: Reigniting Radical Growth", Boston Consulting Group, 20 June.

ZDNet (2020). "RDP and VPN use skyrocketed since coronavirus onset", June.

## About the authors

**Iñaki Aldasoro** is an economist at the Monetary and Economic Department of the Bank for International Settlements. Before joining the BIS he worked for the European Systemic Risk Board. He holds a PhD in Economics from Goethe University Frankfurt.

**Jon Frost** is a Senior Economist in the Innovation and the Digital Economy unit of the BIS. In this role, he conducts policy-oriented research on fintech and digital innovation. He has published research on big tech in finance, macroprudential policy and inequality. He is a research affiliate of the Cambridge Centre for Alternative Finance at the University of Cambridge.

**Leonardo Gambacorta** is the Head of the Innovation and the Digital Economy unit at the BIS. His main interests include the monetary transmission mechanisms, the effectiveness of macroprudential policies on systemic risk, and the effects of technological innovation on financial intermediation.

**Thomas Leach** is a PhD student at the University of Pavia, his main interests are in financial technologies and the impact of digitalisation on the economy.

**David Whyte** is currently the Deputy Head of Corporate Security and the Head of the Cyber Resilience Coordination Centre (CRCC) at the Bank for International Settlements. In his role as the head of the CRCC, he is responsible for leading and developing cyber resilience coordination activities for the central bank community. He holds a PhD in Computer Science from Carleton University as well as a Master's degree from the Massachusetts Institute of Technology in System Design and Management.

## SUERF Policy Notes (SPNs)

| | | |
|---|---|---|
| No 201 | Central banks' response to the "tragedy on the horizon" | by François Villeroy de Galhau |
| No 202 | Policy revolution | by Elga Bartsch, Jean Boivin, Stanley Fischer and Philipp Hildebrand |
| No 203 | Tracking Covid: What Worked? | by Markus Guetschow |
| No 204 | Lessons from the Swedish anti-corona strategy | by Lieven Noppe |
| No 205 | Retail CBDC Remuneration: The Sign Matters | by Christian Pfister |

SUERF
THE EUROPEAN MONEY AND FINANCE FORUM

SUERF is a network association of central bankers and regulators, academics, and practitioners in the financial sector. The focus of the association is on the analysis, discussion and understanding of financial markets and institutions, the monetary economy, the conduct of regulation, supervision and monetary policy. SUERF's events and publications provide a unique European network for the analysis and discussion of these and related issues.

SUERF Policy Notes focus on current financial, monetary or economic issues, designed for policy makers and financial practitioners, authored by renowned experts.





SUERF Secretariat
c/o OeNB
Otto-Wagner-Platz 3
A-1090 Vienna, Austria
Phone: +43-1-40420-7206
www.suerf.org • suerf@oenb.at