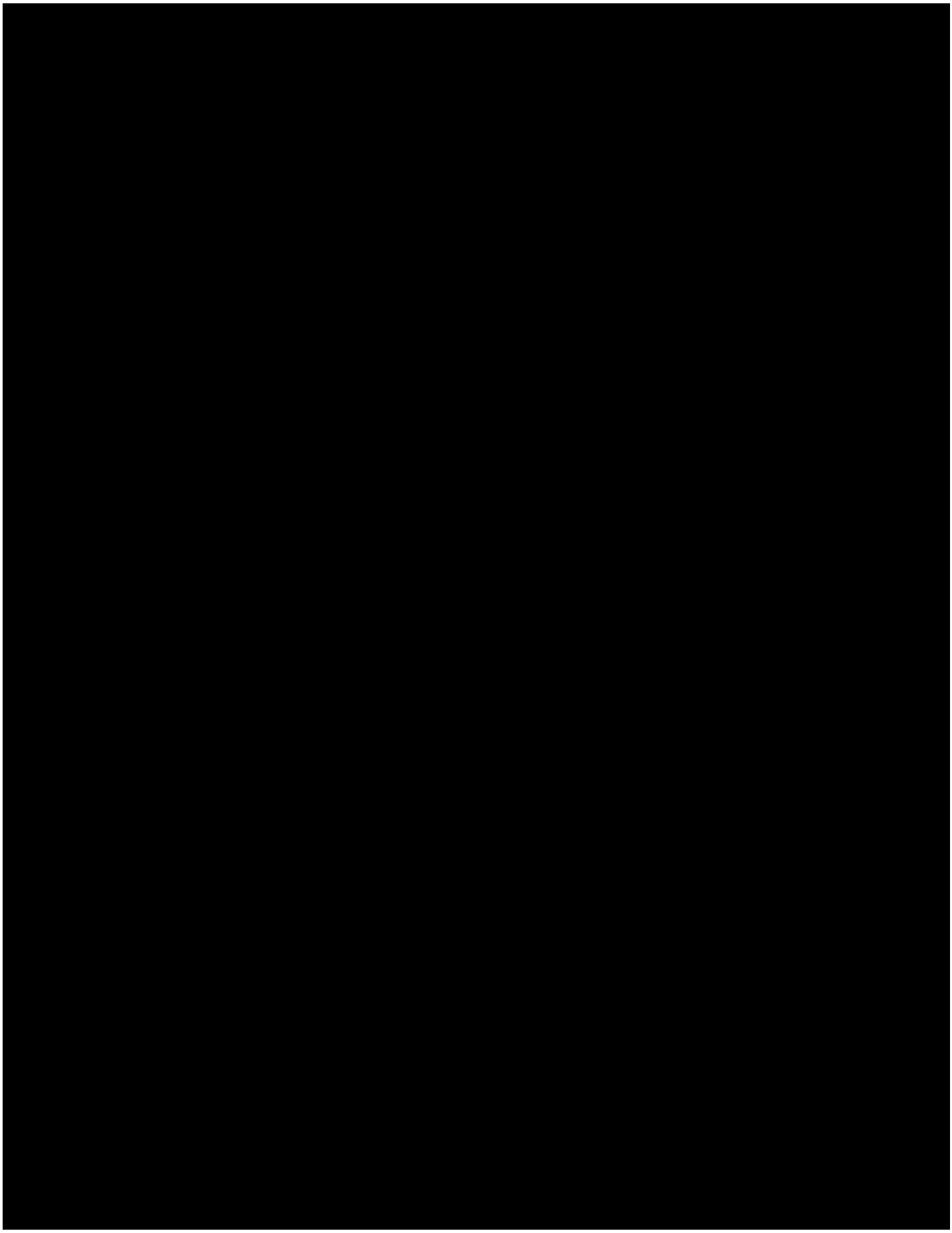


 WP/18/143

IMF Working Paper

Strategy, Policy & Review Department

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment

Prepared by Antoine Bouveret*

Authorized for distribution by Vikram Haksar

June 2018

Abstract

Cyber risk has emerged as a key threat to financial stability, following recent attacks on financial institutions. This paper presents a novel documentation of cyber risk around the world for financial institutions by analyzing the different types of cyber incidents (data breaches, fraud and business disruption) and identifying patterns using a variety of datasets. The other novel contribution that is outlined is a quantitative framework to assess cyber risk for the financial sector. The framework draws on a standard VaR type framework used to assess various types of stability risk and can be easily applied at the individual country level. The framework is applied in this paper to the available cross-country data and yields illustrative aggregated losses for the financial sector in the sample across a variety of scenarios ranging from 10 to 30 percent of net income.

JEL Classification Numbers: E44, G11, G21, G22

Keywords: Cyber risk, systemic risk, operational risk, risk management.

Author's E-Mail Address: abouveret@imf.org.

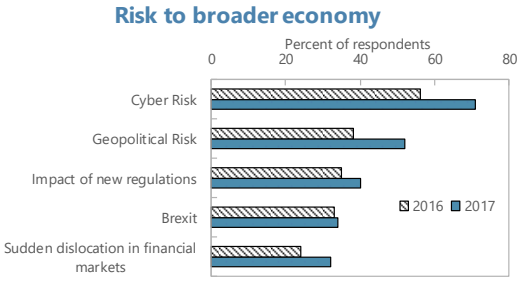
* Antoine Bouveret is an economist in the Macro-Financial Unit in the Strategy, Policy & Review Department. The author would like to thank Luke Carrivick from ORX, Sanjay Christo, Tamas Gaidosch,Vikram Haksar, Emmanuel Kopp, Rodolfo Maino, Manasa Patnam, Celine Rochon, Helene Poirson-Ward, Natalia Stetsenko, Aminata Touré, Andrew Tiffin, Christopher Wilson and Kevin Wiseman for helpful comments.

Contents Page

I. INTRODUCTION

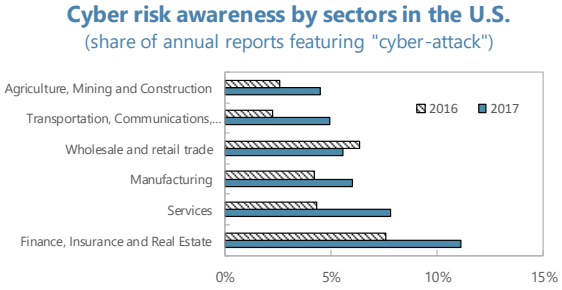
Cyber risk has emerged as a systemic risk concern, following recent cyber incidents (IIF (2017), IMF (2017b), OFR (2017)). Recent surveys point to cyber risk as a main concern among market participants ranked first in the DTCC Systemic Risk Barometer (Figure 1), and second in the 2017 H2 systemic risk survey by the Bank of England (Bank of England (2017)). Successful cyber-attacks such as Wannacry in May 2017 or NoPetya in June 2017 have shown that cyber-attack can lead to severe disruptions and major losses for the targeted firms.

Figure 1: Survey of risks to financial stability



Source: DTCC Systemic Risk barometer 2017Q1

Figure 2: Reporting of cyber risk



Sources: SEC form 10-K; and staff calculations.

Data on cyber incidents is scarce and there have been very few quantitative analyses of cyber risk.[1] Data on cyber risk is notoriously scarce, since there is no common standard to record them, and firms have no incentives to report them. For example, in the U.K. only 49 cyber-attacks were reported in 2017 to U.K. Financial Authorities, pointing to a material under reporting of successful cyber-attacks in the financial sector (Butler (2017)).[2] Moreover, international sharing of data reported to domestic regulators also has to take into account — beyond the typical privacy and other constraints— that there might be national security considerations in sharing and reporting of data.

In the U.S., the SEC released in 2011 guidance on disclosure of cyber risk for listed firms (SEC (2011)), which was revised in 2018 to provide additional details on how and when firms should disclose the information to investors (SEC (2018)). However, there is scope to provide a framework to report cyber-attacks, which could better address existing data gaps.

For example, among around 4,000 annual reports for U.S firms ('form 10-K') published in 2017, only 7 percent included a reference to cyber-risk, mainly in the finance and services sectors (Figure 2).

[1] Recent empirical work includes Biener et al. (2015) and Romanosky (2016).

[2] It is useful to make a distinction between cyber incidents and cyber-attacks. Incidents cover a broader category, while cyber-attacks cover malicious use of Information and Communication Technologies (ICT). This paper, and the data used, focus on cyber-attacks.

In the European Union, the General Data Protection Regulation (GDPR), which will enter into force in May 2018, requires firms to report breaches to the competent supervisory authority within 72 hours. Failure to comply with the reporting requirements could lead to fines up to EUR 20 Mn or 4 percent of global annual turnover (whichever is higher).

This paper provides a framework for assessing cyber risk for financial institutions complemented by a qualitative and quantitative overview. The financial sector is one of the most targeted sectors due to its reliance on information and its central role in the credit intermediation process (Kopp et al. (2017)). Moreover, due to regulatory requirements regarding operational risk, financial institutions are more likely to collect data on cyber incidents than non-financial corporates.

The objective of this paper is to shed light on cyber risk for financial institutions using publicly available data and commercial data sets, with potential use by regulators, supervisors and financial institutions. Section II provides an overview of recent cyber-attacks on financial institutions. Section III describes channels through which cyber risk can impact financial stability. Section IV provides an operational framework and methodology to assess aggregate losses for the financial sectors and some quantitative estimates.

II. AN OVERVIEW OF CYBER-ATTACKS TARGETED AT FINANCIAL INSTITUTIONS

A. Cyber risk and types of cyber-attacks

Cyber risk can be defined as "*operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems*" (Cebula and Young (2010)). Compared to risk categories covered by insurance, cyber risk shares characteristics with both property and liability risk, as well as catastrophic and operational risk (Eling and Wirfs (2016)). On the one hand, cyber risk can impact first (the target) and third parties (a counterpart to the target). On the other hand, losses due to cyber risk are frequently small and independent but they could also have a low frequency and a high impact ('blackout scenario'). Cyber risk can be unrelated to cyber-attacks: for example, software updates or natural disasters can lead to the crystallization of cyber risk through business disruptions without any nefarious intent, as outlined in the definition of cyber incidents (see footnote 2).

Cyber-attacks can impact firms through the three main aspects of information security: confidentiality, integrity and availability. Confidentiality issues arise when private information within a firm is disclosed to third parties as in the case of data breaches. Integrity issues relate to misuse of the systems, as is the case for fraud.[3] Finally, availability issues are linked to business disruptions. The three types of cyber-attacks have different direct impacts on the targets: Business disruptions prevent firms from operating, resulting in loss revenue; fraud leads to direct financial losses; while the effects of data breaches take more time to materialize, through reputational effects as well as litigation costs. More generally, the risk of

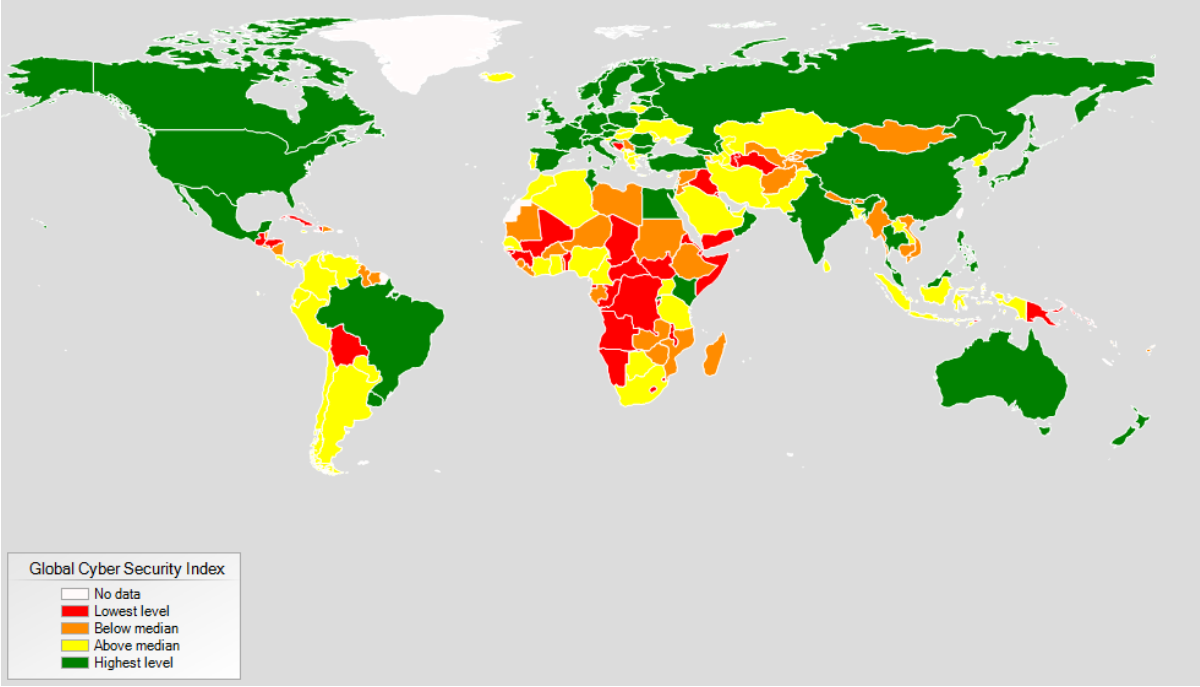
[3] We follow the taxonomy used by ORX, although other definitions exist. For example, the CRO forum (2016) considers data breaches, fraud, business disruptions and a fourth type of cyber-attack which occurs when the attacker is able to affect the integrity of the targeted institution by modifying its internal data. For simplicity, integrity attacks are included in the three main types of cyber-attacks referred above.

a loss of confidence following cyber-attacks could be high for the financial sector, given the reliance of financial institutions on the trust of their customers. Regarding the financial system, business disruptions are more likely to have direct short-term contagion effects than fraud or data breach, which tend to impact mainly the targeted firm in the short-term.

B. Which countries are more exposed to cyber risk?

The financial sector is highly exposed to cyber risk, across all types of countries. The International Telecommunication Unit (ITU)— an agency of the United Nations— provides a global cybersecurity index for the world. Their index is based on a range of factors, including legal, technical and organizational arrangements as well as capacity building and cooperation (ITU (2017)). Figure 3 shows the cross-country heterogeneity regarding cybersecurity, with most Advanced Economies and Emerging Markets having a high value of the cybersecurity index (above the median), while middle income and low-income countries tend to have lower values.

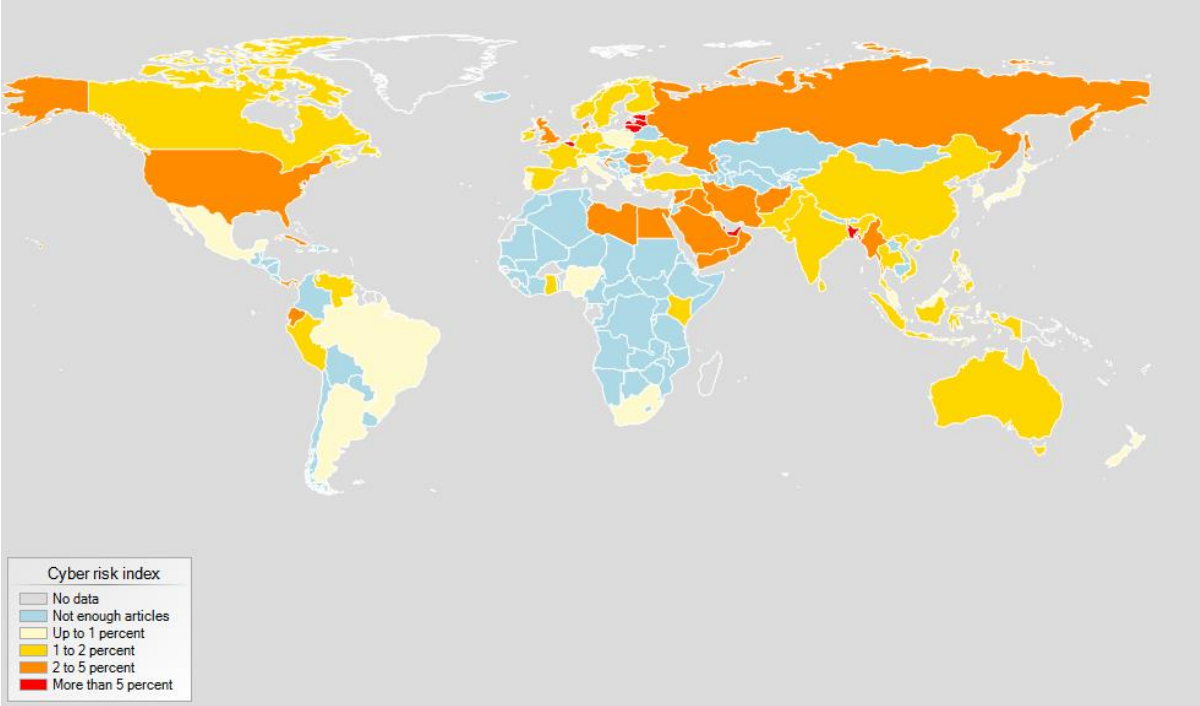
Figure 3: Global Cybersecurity Index



Source: ITU (2017).

Since there is no quantitative measure of cyber risk by country for the financial sector, we build an indirect measure using media coverage. An index is computed using the number of articles referring to cyber risk by country, divided by the number of articles referring to risk in the financial sector (Figure 4). As shown in the map, almost all countries are covered. The index is highest in countries that recently suffered from cyber-attacks such as Bangladesh and the Baltic states.

Figure 4: Measure of cyber risk for banks



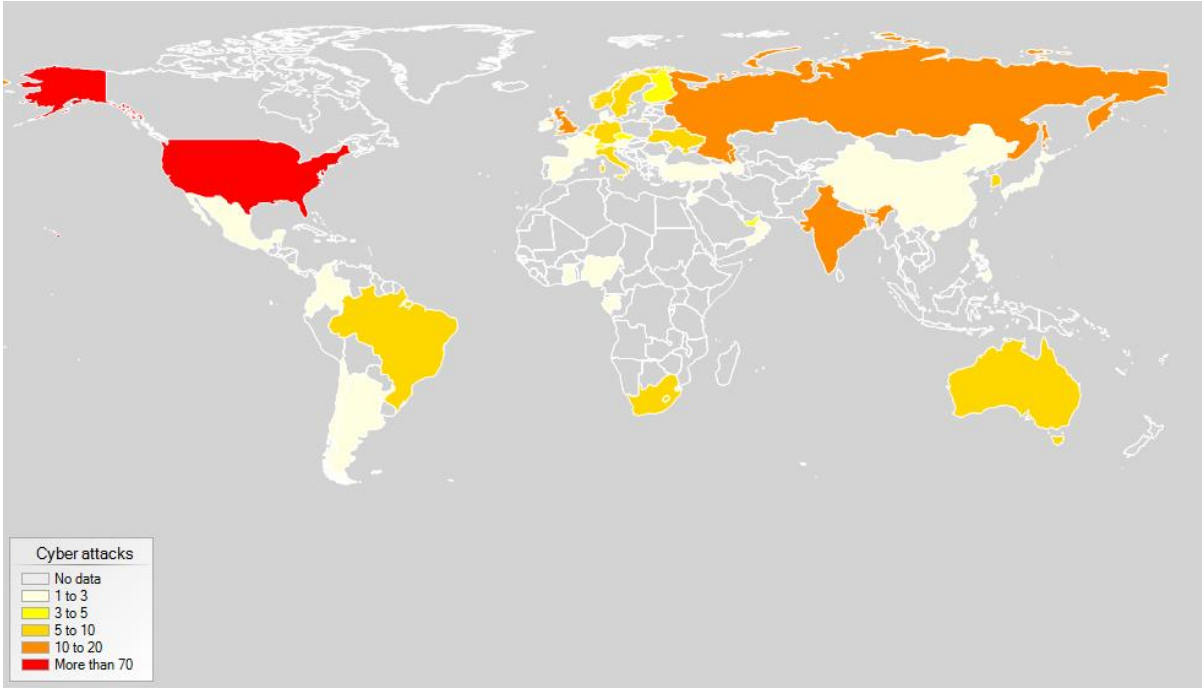
Note: Number of articles featuring "cyber-attack" or "hack" or "cyber risk" or "cyber security" and "banks" or "bank" and "risk" divided by the number of articles featuring "banks" or "bank" and "risk" by country. The index is not computed for countries with fewer than 25 articles on cyber risk (light blue). Only articles in English were included. Period range: Jan-2014-Sep. 2017. Sources: Factiva; and author's calculations.

Complete data on cyber-attacks is notoriously scarce. Available public and commercial datasets exist but they are incomplete, have different coverage and use different definitions of cyber-attacks, which makes the analysis of cyber losses difficult.[4] Moreover, data on losses are gathered from different sources and using different methods (actual costs, estimated costs etc.) making their comparability difficult. Among non-public datasets, two main types are available: commercial data and consortium data. Commercial data providers such as SAS or IBM collect data on operational risk events— which includes cyber events based on publicly available information. Niche providers such as Advisen cover 37,000 cyber events. Consortium data is provided by ORX, a consortium of financial institutions that gathers data on operational risk events. ORX members provide anonymized data covering around 600,000 risk events which is available to members only. ORX also provides a dataset based on publicly available data, ORX News, which covers around 6,000 events, including cyber events related to cyber-attacks. Data on losses includes only direct losses— although indirect losses (reputation, business recovery and remediation etc.) account for more than 90 percent of total losses (Deloitte (2016)).

[4] Private sector initiatives have been launched to foster the harmonization of data related to cyber-attacks, such as the proposal by the Chief Risk Officer Forum (see CRO (2016)).

ORX News data on cyber events is the main source used in this paper. The data cover 341 cyber risk events that impacted financial institutions and reported over 2009-2017. Around 1/3 of the events provide loss data which amounts to USD 6.5 billion overall.
Based on the limited dataset, advanced economies are the main targets of cyber-attacks but EM and developing economies are also exposed to cyber risk (Figure 5), based on data from ORX News.[5] AEs account for 80 percent of successful attacks, mainly in the U.S. (39 percent) and UK (7 percent) as shown in Figure 6. Among EMs, the BRICS account for most of the attacks (17 percent), mainly in Russia (6 percent), China (4 percent) and India (3 percent). Overall, financial institutions in more than 50 countries have been victims of cyber-attacks over the last few years according to reports in the public media.

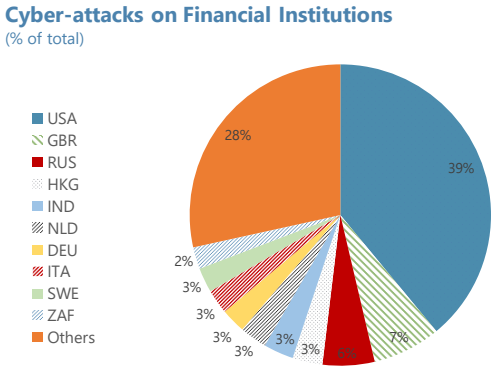
Figure 5: Number of cyber-attacks by country in the ORX database



Sources: ORX News; www.orx.org.

[5] The dataset is potentially biased towards Advanced Economies and English-speaking countries, given that the data is based on media reports in English, more likely to be available in countries with free press.

Figure 6: Share of cyber-attacks by country

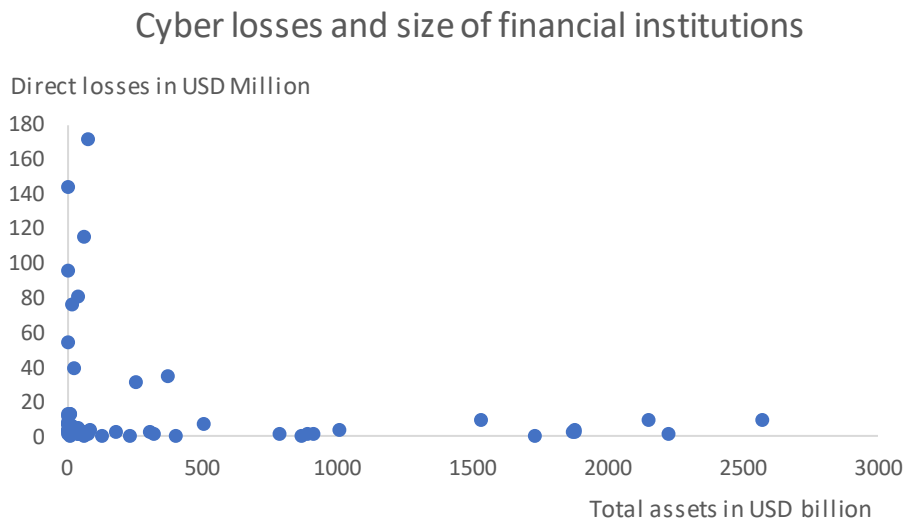


Sources: ORX News; IMF staff calculations

Among financial institutions, banks account for the bulk of the attacks (91 percent of the attacks), followed by insurance companies (7 percent). Among banks, retail banking activities (39 percent of the total) and credit cards services (25 percent) were the main business lines targeted.

Direct losses due to cyber-attack are generally unrelated to the size of the financial institution targeted (Figure 7). The largest losses recorded have been concentrated among smaller institutions, possibly due to lower absolute investment in IT security.

Figure 7: No relationship between size and losses due to cyber attacks



Sources: ORX News, SNL.

Central banks in AEs and EMs have also been the victims of cyber-attacks. In AEs, attacks were either data breaches (U.S., Italy) or business disruptions (Norway, Sweden), while in EMs, most attacks were related to fraud, resulting in losses of USD 117 million (Table 1).

Table 1: Recent cyber-attacks on central banks

Institution	Year	Type of attack	Details
Federal Reserve Bank of Cleveland	2010	Data breach	Theft of 122,000 credit cards
Federal Reserve Bank of New York	2012	Data breach	Theft of proprietary software code worth USD 9.5 Million
Sveriges Riksbank	2012	Business Disruption	Distributed Denial of Service (DDoS) attack left the website offline for 5 hours
Banco Central del Ecuador	2013	Fraud	USD 13.3 Million stolen from the account of the city of Riobamba at the central bank
Federal Reserve Bank of Saint Louis	2013	Data breach	Publication of credentials of 4,000 US bank executives by Anonymous
Central Bank of Swaziland	2014	Fraud	Theft of USD 688,000
ECB	2014	Data breach	20,000 email addresses and contact information compromised
Norges Bank	2014	Business Disruption	DDoS attack on seven large financial institutions, resulting in suspended services during a day.
Central Bank of Azerbaijan	2015	Data breach	Theft of thousands of bank customers' information
Bangladesh Bank	2016	Fraud	The SWIFT credentials of the Bangladesh central bank were used to transfer USD 81 Million from its account at the FRBNY. Hackers tried to steal USD 951 Million.
Bank of Russia	2016	Fraud	21 Cyber-attacks aimed at stealing USD 50 Million from correspondent bank accounts at the central bank, resulted in a loss of USD 22 Million.
Bank of Italy	2017	Data Breach	Hack of email accounts of two former executives.

Source: ORX News

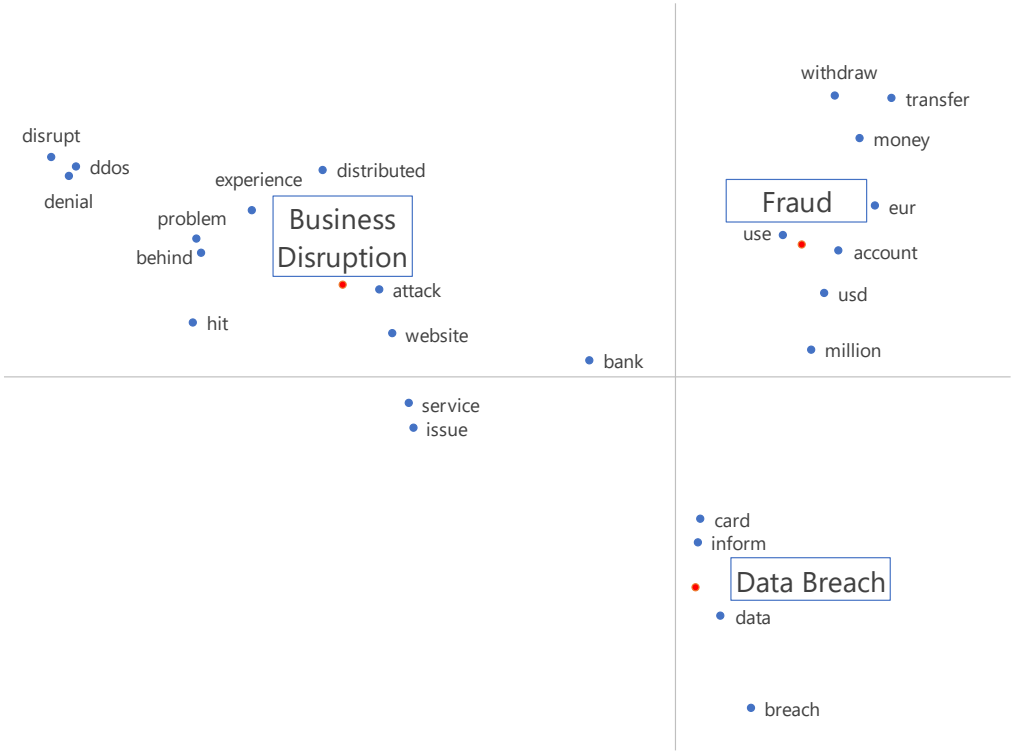
Among cyber-attacks, fraud and data breaches are more prevalent, yet business disruption is also significant. In the ORX News dataset, fraud accounts for 43 percent of events, data breaches 34 percent and disruption 23 percent. While business disruptions are known immediately, the other types of cyber-attacks can take place for months or years before being noticed and reported, which could lead to a downward bias in the dataset.

Patterns can be identified for each type of cyber-attacks using text-mining techniques (see Bholat et al. (2015) for an overview) applied to the ORX News dataset, which provides for each case background information in text form. More precisely, correspondence analysis — a statistical technique to provide a graphical representation of the structure of a dataset— is used to identify the words which tend to cluster around the three types of cyber-attacks (Figure 7).[6] Business disruption is associated with DDoS attacks which typically impact the website of the target— when a very large number of requests are sent to the targeted servers, overloading the system and making it unable to operate. Data breaches are linked with credit card information, and fraud is associated with money transfers, and a loss amount — since around 80 percent of the events with loss data are cyber-related fraud. The word "bank" is in the middle of the chart since banks are the main targets of all three types of attacks. The x-axis can be interpreted as a measure of the informational content regarding losses (with most

[6] Text-mining techniques are particularly useful when applied on very large datasets (thousands or millions of observations). The findings presented here are therefore limited by the small size of the sample.

events in the business disruption category having no loss information), while the y-axis measures whether the impact of the cyber-attack is immediate (business disruption or fraud) or takes more time to materialize, as in the case of data breaches.

Figure 8: Correspondence analysis (terms contributing the most by types of attack)



Sources: ORX News, author's calculations

III. A FRAMEWORK TO ASSESS CYBER RISK FOR FINANCIAL INSTITUTIONS

A. Why are financial institutions highly exposed to cyber risk?

In information security risk management, risk is defined as a combination of *consequences* and likelihood (ISO (2011)), where likelihood is a function of *threat* levels and the ease of exploitation of existing *vulnerabilities*:

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequences})$$

In this context, financial institutions are highly exposed to cyber-risk due to a combination of factors. Kopp et al. (2017) show that *threat* levels are particularly high for financial institutions due to cybercrime, hacktivism, proxy organizations—sophisticated attackers conducting espionage on behalf of a beneficiary— and surveillance of communication by third parties. *Vulnerabilities* to cyber incidents (including cyber-attacks) can be considered high because financial institutions are dependent on highly interconnected networks and critical infrastructures. Moreover, many institutions have legacy systems which might not be resilient to cyber-attacks (Friedman (2016)). The increased level of sophistication of cyber

criminals, along with the decline in the cost of launching cyber-attacks, make institutions with legacy systems all the more vulnerable. *Consequences* of cyber-attacks are also high because financial activity is dematerialized and therefore highly dependent on technology.

B. Vulnerabilities in the financial sector

Single Point of Failure and critical infrastructures

Financial institutions are particularly exposed to cyber risk due to their reliance on critical infrastructures and their dependence on highly interconnected networks. Critical financial market infrastructures include payment and settlement systems, trading platforms, central securities depositories, and central counterparties. The critical infrastructures represent a Single Point of Failure and any successful attack could have wide-ranging consequences.[7]

A business disruption of a financial market infrastructure or a set of large financial institutions could have a significant impact due to risk concentration (Kopp et al. (2017)) and the lack of substitutes in the case of Financial Market Infrastructures (FMIs). If a payment and settlement systems goes offline during the day, market participants would be unable to process transactions and therefore be exposed to liquidity and solvency risk. Similarly, if one or several large banks are disrupted and unable to process transactions, their counterparts would be subject to liquidity and solvency risk.

Several papers have already looked at the impact of a disruption of a large market participant on FMIs. For example, Clarke and Hancock (2014) use the Bank of Finland payment simulator to analyze the impact of operational disruptions of the largest fifteen participants on intraday liquidity in the Australian Real Time Gross Settlement system. Their results show that the amount of unsettled payment varies according to the time of disruption and the participants size.[8] Similarly, as part of their risk management framework, Central Counterparties (CCPs) — and their supervisors—regularly assess the impact of events that could be the result of a cyber-attack leading to the business disruption of clearing members. For example, the recent stress tests of CCPs run by the European Securities and Markets Authority (ESMA) estimates the impact of the default of two large clearing members on the CCP (credit risk) and the consequences of the failure of a custodian (liquidity risk).[9] To some extent, the stress test framework can also be used to model the impact of a successful cyber-attack on market participants.

The disruption of material infrastructures such as power grids and IT infrastructures (Cloud providers or operating systems) could also have a large macroeconomic impact. Recent

[7] In that context, the ECB recently established a Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECB (2018a)) and launched a public consultation on cyber resilience oversight expectations for FMIs (ECB (2018b)).

[8] For example, in Switzerland the simulation of the disruption of the two largest participants would result in 50 percent of unsettled transactions, with contagion effects across banks (Glaser and Haene (2007))

[9] See ESMA (2018) for details about the methodology and stress test results.

studies estimate that a disruption of part of the U.S power grid could lead to up to USD 1 trillion in losses and a disruption of IT infrastructures up to USD 53 billion (Table 2).

Table 2: Impact of disruption of infrastructures (all sectors)

Scenario	Target	Losses (in billion of USD)
Electricity blackout	Energy infrastructures	243-1,024
Cloud Service Providers hack	Cloud Providers	5-53
Mass vulnerability attack	Operating System	10-29

Sources: Lloyd's (2015, 2017)

Business disruptions in the financial sector

Successful attacks on a financial institution could result in significant disruptions, although to date attacks have not caused large damages, based on publicly available information. A common method to disrupt firm business operations is to launch a DDoS attack on the targeted firms' servers. For example, on August 10 and 11, 2011, the news website of the Hong Kong stock exchange suffered a Distributed Denial of Service (DDoS) attack. The stock exchange had to suspend trading in the shares of seven companies due to make interim results announcements as the result of the attack. No significant damages have been reported so far, as business disruptions were short-lived (from a few hours to a day or two) and only affected part of banks' business operations (website and sometimes online payments). A recent report by Lloyd's estimates that a disruption of the top cloud provider in the U.S. for 3 to 6 days could lead to losses of around USD 24 billion (Lloyd's (2018)), with most losses occurring in the manufacturing and trade sectors, while losses for the financial sector would be limited to USD 450 Mn.

Cyber-attacks can also be used to undermine customers' confidence in an institution. For example, on June 27, 2014, Bulgaria's largest domestic bank FIB experienced a depositor run, amid heightened uncertainty due to the resolution of another bank— following phishing emails indicating that FIB was experiencing a liquidity shortage. Deposits outflows on that day amounted to 10 percent of the banks' total deposits and the bank had to use a liquidity assistance scheme provided by the authorities.

Cyber-attacks can also target multiple financial institutions to disrupt the financial sector. Several countries have been exposed to coordinated cyber-attacks on the banking sector using DDoS, although no significant damages have been reported so far (Box 1).

Box 1: DDoS attacks on multiple financial institutions

US: In September 2012, the websites of Bank of America, PNC, JPMorgan, US Bancorp, Wells Fargo were targeted and one month later the websites of BBT, Capital One, HSBC, Region Financial, SunTrust were also disrupted.

Czech Republic: On March 6, 2013, the websites of the central bank, three large banks and the stock exchange were disrupted, with limited damages estimated at USD 0.5 Million.

Norway: On July 8, 2014, seven major financial institutions were attacked, leading to disrupted services during the day.

Finland: End-2014, three banks (Op Pohjola, Danske Bank and Nordea) suffered DDoS attacks that rendered their online services unavailable and for one bank prevented customers from withdrawing cash and making card payments.

Fraud

Cyber-attacks can be used for fraudulent purposes, as evidenced recently by theft using SWIFT (Box 2). Access to confidential information, including clients' credentials used for online payment can be used by cyber-criminals. In the dataset, cyber-related fraud accounts for 90 percent of reported losses.

Box 2: Recent cyber-attacks using SWIFT

Over the last three years, at least ten attacks were based on the SWIFT system— a messaging system used by financial institutions for financial transactions. Hackers accessed the victims' SWIFT credentials and sent fraudulent payment orders on behalf of the target (EM banks) to the hackers' bank accounts—in some cases transiting through AE banks and central banks. Initial losses amounted to USD 336 Million, while actual losses were around USD 87 Million, as some orders were frozen and some money was recouped.

Table 3: Cyber-attacks using SWIFT

Institutions	Date	Initial losses (USD million)	Current estimated losses* (USD million)
Banco del Austro (Ecuador)	Jan. 2015	12.2	9.4
Bangladesh Central Bank	Feb. 2016	81	66
Union Bank of India	Jul. 2016	171	0
TP Bank (Vietnam)	May 2016	1	0
Akbank (Turkey)	Dec. 2016	4	4
Far Eastern International Bank (Taiwan, Province of China)	Oct. 2017	60	0.5
NIC Asia Bank (Nepal)	Oct. 2017	4.4	0.6
Globex (Russia)	Dec. 2017	1	0.1
Unidentified bank (Russia)	Dec. 2017	Unknown	6
City Union Bank (India)	Jan. 2018	2	Unknown

Sources: ORX News, Financial Times. * Current estimated losses are based on publicly available information. Targeted institutions are in the process of recovering the losses through legal proceedings.

Emerging technologies such as Fintech are also particularly exposed to cyber-attacks given their reliance on technology. Technological innovations may increase vulnerabilities to cyber-attacks, as specialized firms might have fewer controls and risk management procedures than large, vertically integrated regulated intermediaries (IMF (2017a)). Greater

use of technology could also expand the range and numbers of entry points into the financial system, which hackers could target. Fintech activities could also increase third-party reliance, where firms outsource activities to a few concentrated providers. In this case, the disruption of a provider could increase systemic risk due to the centrality of the provider in the financial system (FSB (2017)). Cyber-attacks on Fintech firms (mainly online exchanges allowing the trading of Bitcoins and providing wallet services) have resulted in at least USD 1,450 Million in losses due to fraud since 2013 (Table 4).

Table 4: Cyber-attacks on Fintech firms

Institution	Date	Estimated losses (USD Mn)
Inputs.io	Oct. 2013	1.3
GBL	Oct. 2013	5
Bitcoin Internet Payment Services	Nov. 2013	1
MT Gox	Jan. 2014	470
BitPay	Dec. 2014	1.9
EgoPay	Dec. 2014	1.1
Bitstamp	Jan. 2015	5.3
Bitfinex	May. 2015	0.3
Gatecoin	May 2016	2
DAO Smart Contract	Jun. 2016	50
Bitfinex	Aug. 2016	72.2
CoinDash	Jul. 2017	7
Tether	Nov. 2017	31
NiceHash	Dec. 2017	64
Coincheck	Jan. 2018	534
BitGrail	Feb. 2018	170
Coinsecure	Apr. 2018	33

Sources: ORX News, Financial Times

The high degree of interconnectedness across firms can lead to rapid contagion effects. For corporates, due to the high interconnectedness across supply chains, a successful attack on part of the network could spread rapidly to other firms. For example, in June 2017, a ransomware targeting Ukraine lead to losses of at least USD 1.3 billion for multinational firms across sectors (transportation, construction or food) linked to Ukrainian companies.[10] For financial institutions, a disruption of one large bank, making it unable to process transactions and post margins could spread quickly to its counterparties and the financial market infrastructures, resulting in heightened liquidity and solvency risk.

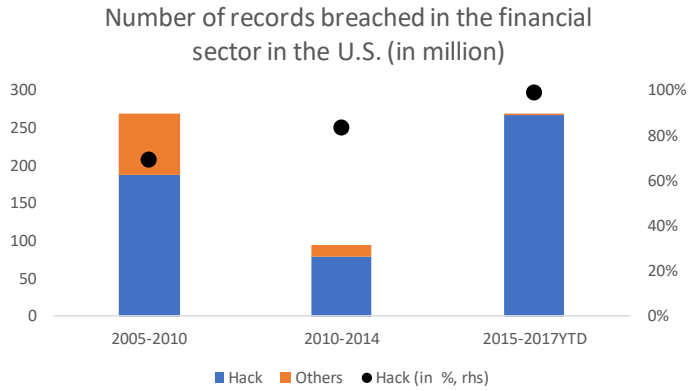
Data breaches

Financial institutions are also particularly vulnerable to data breaches. Given their reliance on customer's data to conduct business, the financial sector suffered the most incidents with data loss in recent years— including the Equifax data breach where hackers may have stolen

[10] This estimate is based on the financial statements of listed firms following the attack. Saint Gobain estimates losses of around USD 350 Mn in July 2017, A.P. Møller-Mærsk of USD 200-300 Mn, Merck for USD 310 Mn, Mondelez for USD 100 Mn, and Fedex TNT Express for USD 300 Mn

personal information of more than 145 million U.S customers. The economic impact of data breaches is hard to assess since indirect effects (loss of clients, reputation risk) are likely to be more material than direct effects (recovery and litigation costs). In the U.S. alone, more than 260 million records were breached due to hacking over the last three years in the financial sector (Figure 9). The Ponemon Institute estimates that the average cost per stolen record was USD 141 in 2017 (Ponemon (2017)). Applying the Ponemon estimates, losses due to data breach over the last three years would be around $38 billion for U.S. financial firms alone.

Figure 9: Data breaches in the U.S.



Source: Privacy Rights Clearinghouse

IV. A QUANTITATIVE FRAMEWORK FOR ANALYSIS OF CYBER RISK FOR FINANCIAL INSTITUTIONS

A. Overview of the methodology

This section aims to illustrate how models employed for operational risk assessment for banks and the pricing for insurance contracts can also be applied to developing a framework for an analysis of cyber risk**.** This analysis yields estimates and distribution of aggregate financial system losses due to cyber-attacks. The results are particularly important for the financial services sector, since regulators require banks and insurance companies to hold risk capital for operational losses which might result from cyber-attacks. The usefulness of these results for policymakers, regulators, and practitioners is illustrated in two applications (with and without contagion across firms).

The empirical strategy is to define cyber risks as a sub-group of operational risk, allowing us to clearly identify relevant data. The data on cyber-attacks is extracted from ORX News.[11] All losses are expressed in U.S. dollars, and in the following analysis adjusted for inflation to make them comparable over time.

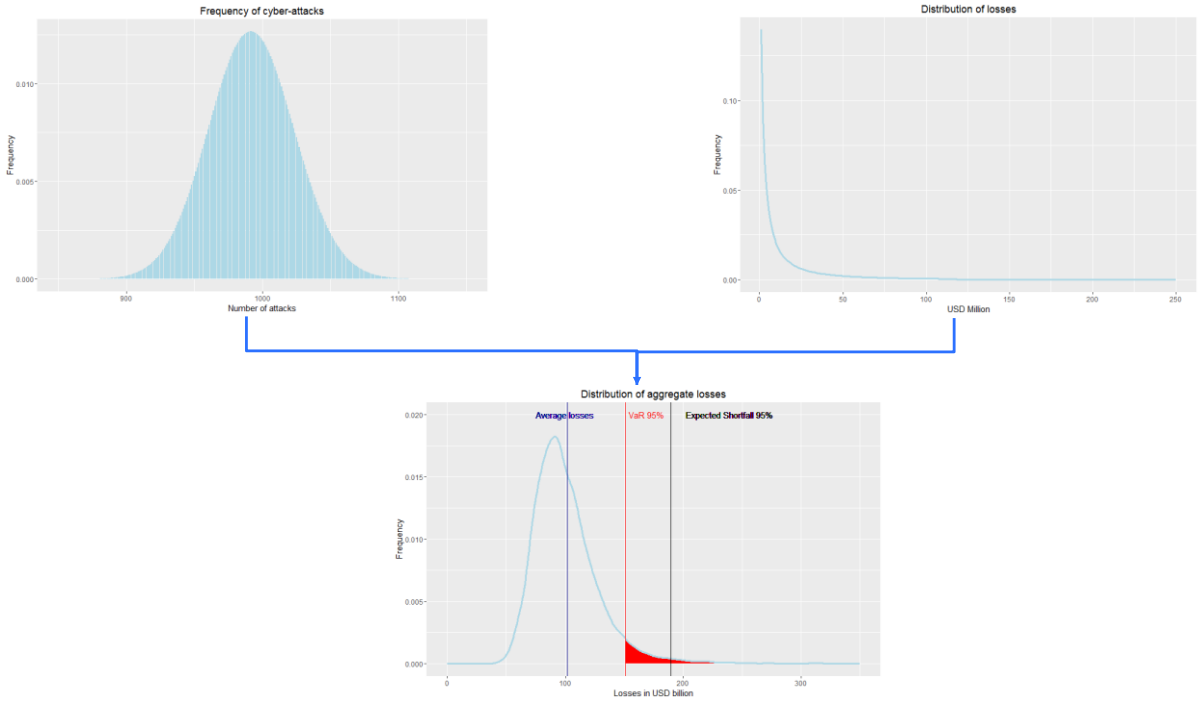
[11] The dataset provides estimates of direct economic losses; however, reputational loss due to an operational risk event is not covered since this sort of loss is typically excluded from operational risk.

To analyze the statistical properties of cyber-attacks we use tools from actuarial science. First, we fit the data on losses from ORX News using a lognormal distribution for the body of the distribution and extreme value theory for the tail, following the standard approach in actuarial science to model losses. After having estimated the distribution and frequency of losses, the average loss and risk measures (value at risk (VaR), and expected shortfall (ES)) are estimated.[12] Risk measures show how much capital a firm needs to cover the losses with a given confidence level. Second, aggregated losses are computed with Monte Carlo simulations, assuming that the frequency of each cyber event follows a Poisson distribution.

B. Estimation of aggregated losses due to cyber risk

The approach taken to estimate aggregate loss distribution follows approaches used in actuarial science to model insurance claims, and to assess operational risk for banks under the Advanced Measurement Approach in the Basel II framework (Shevchenko (2010)). The method is based on i) the frequency of events, ii) the distribution of losses, and iii) the aggregate distribution of losses, considering the frequency and loss distribution. Figure 10 shows the different components of the method. Once the frequency (top-left panel) and distribution of losses due to cyber-attacks are estimated (top-right panel), it is possible to estimate the distribution of aggregated losses (bottom panel).[13]

Figure 10: Estimation of aggregated losses



Formally, the aggregate losses Z due to cyber risk are given by:

[12] The VaR measures how much an institution might lose due to a cyber-attack over a given frequency and a given probability (i.e .95 percent). The expected shortfall is the average of losses above the VaR.

[13] Appendix 1 provides an overview of an application of the framework in the context of country surveillance.

$$Z = X_1 + \cdots + X_N$$

where the frequency N is a discrete random variable — the number of cyber-attacks per year— and X_1, …, X_N are positive random severities (losses). The aggregate losses are equal to the sum of individual losses due to cyber risk over the time horizon (one-year).

We also assume that N and X_i are independent, i.e. the frequency and severities of cyber incidents are independent.

In the remainder of the paper, we focus on particular distributions for the frequency of cyber-attacks and distribution of losses. In practice, both the frequency and the distribution of losses are likely to evolve over time as cybercrime expands and cybersecurity is strengthened. As such, the distributions used in this paper can be seen as a point-in-time assessment rather than a definitive assessment on how cyber-losses should be estimated. Additionally, distributions could also be different by types of attacks, types of targets and types of countries affected. Policy interventions and further efforts on cybersecurity could also change the shape of the distributions.

Distribution of the frequency of cyber events

To model the frequency of cyber-attacks in a given year, we assume that N follows a Poisson distribution: $N \sim Poisson(\lambda)$. This distribution implies that losses happen randomly through time, so that in any short period of time Δt there is a probability $\lambda \Delta t$ of a loss occurring.[14] The probability that k cyber incidents arise over a year is given by:

$$p_k = Pr[N = k] = \frac{\lambda^k}{k!} e^{-\lambda}$$

The parameter λ is based on the average number of cyber events per year over the period 2011-2016, which is approximately 990 in the data provided by Advisen, a commercial provider specialized in cyber risk. In the extreme scenario, it is assumed that the frequency of attacks is equal to twice the peak observed in 2013 (1373 events), resulting in 2746 attacks. Since X_1, …, X_N are independent and identically distributed, and independent of N, the expected aggregated losses are given by:

$$E[Z] = E[N] \times E[X]$$

Since N follows a Poisson distribution, $E[N] = \lambda$, which leads to:

$$E[Z] = \lambda E[X]$$

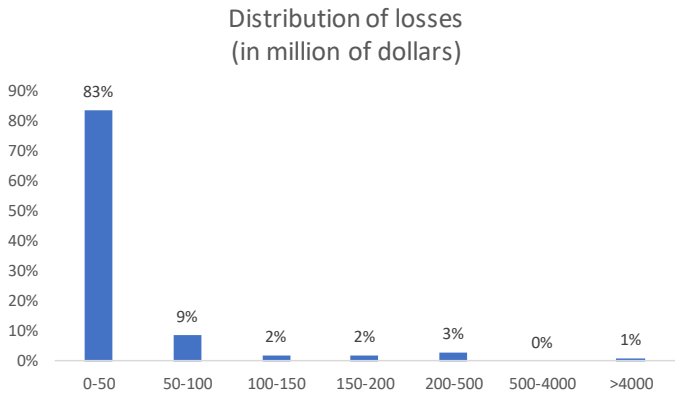
The average aggregate expected losses are entirely determined by the average frequency of cyber-attacks and the average losses per attack.
Ideally, the parameter λ should vary positively according to the threat and sophistication level of cyber-attackers, and negatively to the level of cybersecurity among financial institutions.

[14] In the case of intentional targeted attacks, the assumption of randomness would not hold.

Distribution of losses

Average losses are around USD 66 million in dataset, with a median at USD 4.7 million. Most losses are below USD 200 million, with an outlier at around $4,010 million (Figure 11).[15]

Figure 11: Histogram of losses



Source: ORX News.

We chose to model the distribution of losses by using two distributions depending on the level of losses (spliced distribution). The choice of a spliced distribution provides flexibility to model differently small and large losses, while using one simple distribution would be too restrictive (Cruz et al. (2015)). The body of the distribution ('bulk') follows a lognormal distribution and the right tail follows a Generalized Pareto Distribution (GPD), commonly used in extreme value theory to model fat tails (Coles (2001) and Scarrott and MacDonald (2012)). The GPD is used to model potential large losses due to cyber-attacks, although such events have not yet occurred.

For the bulk of losses, where $x \leq u$ the distribution is lognormal, $X \sim LN(\mu, \sigma)$ and its probability density function f is given by:

$$f(x) = \frac{1}{x\sqrt{2\pi\sigma^2}} exp\left(-\frac{(\ln(x)-\mu)^2}{2\sigma^2}\right)$$

For the tail, where $x > u$ the distribution is given by $X \sim GPD(\xi, \alpha, \beta)$, with the shape parameter ξ, the scale parameter β, and threshold parameter α and the density function is:

$$f(x) = \frac{1}{\beta}\left(1 + \frac{\xi(x-\alpha)}{\beta}\right)^{\left(-\frac{1}{\xi}-1\right)}$$

[15] The losses refer to a cyber-attack which affected more than 30 Brazilian banks with estimated losses of USD 4.0 billion in 2014 (RSA (2014)) in 2017-dollar terms. Fraudsters collected credentials from victims which were then used to process half a million of fraudulent transactions using "boleto bancario", a method of payment similar to a money order in the U.S.

The parameters of the spliced distribution $(\mu, \sigma, \xi, \alpha, \beta, u)$ are estimated by maximum likelihood using the evmix package in R (Hu and Scarrott (2017)).[16] The estimate for u yields \$119 million, implying that losses below this threshold follow a lognormal distribution and above a GPD.

Aggregate distribution of losses

Since the distribution of aggregate losses is based on a spliced distribution for which closed-form solutions might not be available, we use numerical methods to estimate aggregate losses (Shevchenko (2010)). We use Monte Carlo simulations to estimate the aggregate distribution of losses, with 10,000 simulations. The algorithm is as follows:

1) for $k = 1, \dots, K$
    a. Simulate the number of events N from the Poisson distribution
    b. Simulate independent severities $X_1, \dots, X_N$ from the severity distribution
    c. Calculate $Z_k = \sum_{i=1}^{N} X_i$
2) next $k = k + 1$

From the distribution of aggregated losses, we can compute the average, median, Value-at-Risk (95 or 99 percentile) and the Expected shortfall (average losses above the VaR).
The Value-at-Risk for a given threshold q is given by:

$$VaR(q) = F^{-1}(q)$$

Where F^{-1} is the inverse of the distribution function of Z.

The expect shortfall is given by:

$$ES(q) = \frac{1}{1-q}\int_q^1 F^{-1}(l)dl$$

or equivalently:

$$ES(q) = E(Z|Z > VaR(q))$$

Contagion

Contagion is introduced in the model by assuming that each cyber-attack has a probability to affect one or several firms (Lindskog and McNeil (2003))— although other methods are also possible such as the use of copulas to model dependence (Böhme et al. (2017)).
The frequency of events does not change, but for a given event there is a probability that this event leads to several losses. Formally, each event can result in one or more losses, where the probability of having multiple losses follows a geometric distribution with parameter $p = 0.8$. Therefore, there is a 20 percent probability that each attack impacts several firms.
The expected aggregate losses are given by:

$$E[Z] = E[G] \times E[X]$$

where G is the total number of loss events. We know that G is equal to the initial number of losses N and the losses due to contagion effects M:

[16] The R code is available upon request.

$$E[G] = E[N] + E[N] \times E[M]$$

Under the assumptions of Poisson geometric distributions, we get:

$$E[G] = \lambda + \lambda \times \frac{1-p}{p}$$

For the contagion case $p = 0.8$, hence:

$$E[G] = 1.25 \times \lambda$$

and

$$E[Z] = 1.25 \times \lambda \times E[X]$$

In this case, average losses are 25 percent higher when contagion is introduced.

The algorithm used is as follows:

1) for $k = 1, \ldots, K$
    a. Simulate the number of events N from the Poisson distribution
    b. Simulate the number of losses M related to the N events from the Geometric distribution to get the total number of losses $G = M + N$
    c. Simulate independent severities X_1, …, X_G from the severity distribution
    d. Calculate $Z_k = \sum_{i=1}^{G} X_i$
2) next $k = k + 1$

For specific type of attacks and targets such as business disruption targeted at highly interconnected entities —such as Financial Market Infrastructures— the contagion would be expected to be very high and would affect multiple firms at the same time. One modelling option would be to assume a lower frequency of attack for FMIs, coupled with a high probability of contagion conditional on a successful attack. Additionally, the contagion might be more likely for large losses than for small losses. In that case, the probability of contagion would be conditional on the loss occurred. For example, if losses would be higher than the 90th percentile, the probability of contagion would jump from 20 to 60 percent.

C. Results

In the baseline case, average losses due to cyber-attacks for the countries in the ORX sample amount to USD 97 billion or 9 percent of banks net income (Table 5).[17] The VaR would range between USD 147 and 201 billion (14 to 19 percent of net income) and the expected shortfall between USD 187 and 281 billion. Those estimates point to sizeable potential aggregated losses in the financial sector, far above publicly reported losses by financial institutions in these jurisdictions. However, estimated losses due to cyber risk are a fraction of operational risk losses for banks— which amounted to USD 260 billion in 2007 and 375 billion in 2009 (Hess (2011)).

[17] Net income data is taken for 2016 for a sample of 7,947 banks worldwide.

In the severe scenario— where the frequency of events is twice the peak observed in 2013— average losses would amount to USD 268 billion (26 percent of net income) and risk indicators would range between USD 352 and 539 billion (34 to 52 percent of net income).

The introduction of contagion effects across financial institutions would increase aggregate losses by around 20 percent, in line with the assumptions used in the modelling of contagion effects.

Table 5: Aggregate losses due to cyber risk

	Baseline		**Scenario 2 (severe)**	
	Independence			
	% net income	USD bn	% net income	USD bn
Average	9	97	26	268
VaR (95%)	14	147	34	352
ES (95%)	18	187	40	409
VaR 99%	19	201	41	427
ES (99%)	27	281	52	539
	Assuming 20% dependence*			
Average	12	127	34	351
VaR (95%)	18	184	43	446
ES (95%)	22	229	49	509
VaR 99%	24	248	51	529
ES (99%)	32	329	62	642

Note: VaR is the Value-at-Risk, ES is the Expected Shortfall. Net income data based on a sample of 7,947 banks for 2016.
*It is assumed that each cyber attack has a 20% probability to affect two or more firms.
Sources: ORX News, SNL, and staff calculations.

The estimates provided in this paper are broadly in line with existing estimates. Symantec (2013) reports an annual cost of cybercrime of USD 113 billion, using a survey to measure cyber-attacks and the average cost per attack. Anderson et al. (2013) estimate direct and indirect losses around USD 215 billion using data from 2007-2012 on different types of cyber-crime (online banking fraud, tax fraud etc.), mainly from the UK and then extrapolated to the world. McAffee (2014) estimates global costs to be between USD 375 and 575 billion.[18] However, most existing studies use very different data source and methodology to estimate losses, some of which are not directly tractable, while this paper provides a tractable framework to estimate the cost of cyber risk.

The estimated losses are several orders of magnitude higher than what the cyber insurance market can so far cover. The insurance market for cyber risk has grown recently to reach around USD 3 billion in premium globally in 2017 and is expected to reach USD 12 to 20

[18] Estimates from market participants might be subject to a potential upward bias, since insurers or sellers of cybersecurity products might have an incentive to increase estimated cyber losses.

billion in the next decade (Fitch Ratings (2017)). However, most institutions do not have cyber insurance— with take-up rates of less than 30 percent across sectors—, coverage is limited and it is challenging for insurers to price cyber risk due to uncertainty about exposures and risks of correlated exposures.[19,20]

D. Robustness and sensitivity analysis

Applying the framework faces a number and of challenges and the methodology used is subject to caveats. Therefore, the estimated losses should be considered illustrative, rather than a definitive estimation of losses due to cyber-attacks.

First, the data used is incomplete. Data on losses is partial and the sample might be biased towards certain countries such as the U.S. Given the delays in reporting and disclosing cyber-attacks, the data used might not represent accurately the current level of cyber risks.[21] The estimation also mixes two different datasets: ORX News for the losses and Advisen for the frequency of events. A consistent framework to collect data on cyber risk could alleviate this bias. Relatedly, it is assumed that all financial institutions are subject to the same risk of cyber-attacks, although in practice institutions are exposed to varying degrees. The degree of financial institutions' exposure could be linked to the criminal and geopolitical environment, access to cybersecurity human capital (of both defenders and attackers), degree of connectivity to the global financial system, and degree of complexity and reliance on IT systems.

Second, the results are dependent on the modelling assumptions for the distribution of losses and contagion. For example, a lognormal distribution provides a better fit than the spliced distribution for the historical data used. If a lognormal distribution is used, average losses amount to USD 38 billion (against USD 97 billion) and the 95% VaR and Expected Shortfall would be USD 51 billion and USD 60 billion respectively. Appendix 2 compares results obtained by using different spliced distributions for losses. More generally, the framework outlined in the paper is flexible enough so that different modelling assumptions can be tested.

Finally, losses might vary according to the type of attack: business disruption is more likely to cause contagion than fraud for example. Ideally, for each type of cyber-attack one would estimate a different loss distribution. Richer datasets would allow the estimation of different distributions by type of cyber-attack.

V. CONCLUSION

Cyber risk has emerged as a main concern among market participants and policymakers recently, yet very few papers provide details on the extent and cost of cyber risk. This paper reviews and documents available evidence on cyber-attack for financial institutions. The

[19] The average coverage limit purchased in 2016 was around USD 3 million (CIAB (2016)) which is far below the average and median losses observed in the ORX News dataset.

[20] See Eling and Wirfs (2016) for an assessment of the insurability of cyber-risk.

[21] A possible way to mitigate uncertainty regarding cyber losses is to use Bayesian methods (Makov (2005)).

analysis shows that cyber-risk is an emerging threat for all types of financial institutions, including central banks as well as fintech firms. Additionally, we provide a quantitative tractable framework that can be used by institutions and supervisors to assess cyber risk in the financial sector. More granular and complete data could be used to improve the estimates— while acknowledging potential national security constraints to data sharing—, in particular by disentangling aggregate losses according to the type of cyber-attacks (data breach, fraud and business disruptions) and modelling contagion effects more precisely.

Looking forward, the design and assessment of possible policy interventions (private and public) to mitigate cyber-risk should be further explored. Possible options include updating the regulatory and supervisory frameworks to account for cyber risk, and developing capacity to assess key vulnerabilities. Public intervention through the design of possible contingency plans— if large-scale attacks would occur— warrant further analysis.

REFERENCES

Anderson, R, C. Barton, R. Böhme. M. J. van Eeten, M. Levi, T. Moore and S. Savage, 2013, "Measuring the Cost of cybercrime", in R. Böhme (ed.), The Economics of Information Security and Privacy (Springer), Chapter 12.

Bank of England, 2017, "Systemic Risk Survey Results – 2017 H2", November, London.

Biener, C., M. Eling and J. Wirfs, 2015, "Insurability of Cyber Risk: An Empirical Analysis", The Geneva Papers, Vol. 40.

Bholat, D., S. Hansen, P. Santos and C. Schonhardt-Bailey, 2015, "Text mining for central banks", Centre for Central Banking Studies Vol. 33.

Böhme, R., S. Laube and M. Riek, 2017, "A Fundamental Approach to Cyber Risk Analysis", Variance Journal, Article in Press.

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

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

Chief Risk Officer Forum, 2016, "Concept Paper on a proposed categorization methodology for cyber risk", June.

Clarke, A. and J. Hancock, 2013, "Payment System Design and Participant Operational Disruptions", Journal of Financial Market Infrastructures, Vol. 2(2).

Coles, S., 2001, An Introduction to Statistical Modelling of Extreme Values, Springer Series in Statistics, Springer-Verlag, London.

Council of Insurance Agents & Brokers, 2016, "Cyber Insurance Market Watch Survey: Executive Summary", Council of Insurance Agents & Brokers, April.

CPMI-IOSCO, 2012, "Principles for Financial Markets Infrastructures", April.

Cruz, M., G. Peters and P. Shevchenko, 2015, Fundamental Aspects of Operational Risks and Insurance Analytics: A Handbook of Operational Risk, Wiley Handbooks in Financial Engineering and Econometrics, Hoboken.

Deloitte, 2016, "Beneath the Surface of a Cyberattack", Deloitte U.S.A., Cyber Risk Services.

Eling, M. and J. H. Wirfs, 2016, "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", Institute of Insurance Economics, University of St. Gallen.

European Central Bank, 2018a, "Establishment of a Euro Cyber Resilience Board for pan-European Financial Infrastructures", Press release, 23 February 2018.

European Central Bank, 2018b, "Cyber resilience oversight expectations (CROE) for Financial Market Infrastructures", Public Consultation Document, April.

European Securities and Markets Authority, 2018, "EU-wide CCP Stress Test 2017".

Financial Stability Board, 2017, "Financial Stability Implications from FinTech", June.

Fitch Ratings, 2017, "Cyber Insurance — Risks and Opportunities", 13 November 2017.

Friedman, S., 2016, "Taking cyber risk management to the next level— Lessons learned from the front lines at financial institutions", Deloitte Insight, June.

Glaser, M., P. Haene, 2007, "Simulation of participant-level operational disruption in Swiss Interbank Clearing: Significant systemic effects and implications of participants' behavior", Payment and settlement simulations seminar, Helsinki, 28 August 2007.

Hess, C., 2011, "The impact of the financial crisis on operational risk in the financial services industry: empirical evidence", Journal of Operational Risk, Vol. 6 (1).

Hu, Y. and C. Scarrott, 2017, "evmix: an R package for Extreme Value Mixture Modelling. Threshold Estimation and Boundary Corrected Kernel Density Estimation", retrieved from http://www.math.canterbury.ac.nz/~c.scarrott/evmix/HuScarrott_Submitted.pdf

Institute of International Finance, 2017, "Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system", September.

International Communication Unit, 2017, "Global Cybersecurity Index (GCI) 2017", July.

International Monetary Fund, 2017a, "Fintech and Financial Services: Initial Considerations", Staff Discussion Notes No. 17/05, Washington D.C.

———, 2017b, "Is Growth at Risk?", Global Financial Stability Report, October, Washington D.C.

International Organization for Standardization, 2011, "ISO/IEC 27005: 011 Information technology -- Security techniques -- Information security risk management".

Kopp, E., L. Kaffenberger, C. Wilson, 2017, "Cyber Risk, Market Failures, and Financial Stability", IMF Working Paper No. 17/185.

Lindskog, F. and A. J. McNeil, 2003, "Common Poisson Shock Models: Applications to Insurance and Credit Risk Modelling", Astin Bulletin: The Journal of the International Actuarial Association, Vol. 33 (2).

Lloyd's, 2015, "Business Blackout", Emerging Risk Report 2015.

Lloyd's, 2017, "Counting the costs—Cyber exposure decoded", Emerging Risks Report 2017.

Lloyd's, 2018, "Cloud Down—Impacts on the U.S Economy", Emerging Risks Report 2018.

Makov, U., 2005, "Principal Applications of Bayesian Methods in Actuarial Science", North American Actuarial Journal Vol. 5.

Office of Financial Research, 2017, "Cybersecurity and Financial Stability: Risks and Resilience", OFR Viewpoint, February.

Ponemon Institute, 2017, "2017 Cost of Data Breach Study", June.

RSA Research Group, 2014, "RSA Discovers massive boleto fraud ring in Brazil", July.

Romanosky, S., 2016, "Examining the costs and causes of cyber incidents", Journal of Cybersecurity, Vol. 2 (2).

Scarrott, C.J. and MacDonald, 2012, "A Review of Extreme Value Threshold Estimation and Uncertainty Quantification", REVSTAT - Statistical Journal Vol. 10 (1).
Securities and Exchange Commission, 2011, "CF Disclosure Guidance: Topic No.2—Cybersecurity".

Securities and Exchange Commission, 2018, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures".

Shevchenko, P., 2010, "Calculation of aggregate loss distributions", Journal of Operational Risk, Vol. 5 (2).

Symantec, 2013, "Norton Report 2013".

APPENDIX 1: APPLICATION OF THE FRAMEWORK FOR COUNTRY SURVEILLANCE

This appendix provides a high-level overview on how to use the framework to assess cyber-risk for financial institutions in a given country.

Identification of vulnerabilities

The first step consists in identifying the components of the financial sector that could be more vulnerable to cyber-attacks. FMIs and significant financial institutions are a starting point.

Publicly available data on recent attacks on institutions located in the country as well as information provided by supervisory authorities could be used to gather information on cyber-attacks. Data on losses and frequency of events are particularly crucial.

Scenario design

Impact of a business disruption on financial market infrastructures
Once the mapping of cyber exposures is done, different scenarios can be designed. For example, a scenario could look at the impact of a business disruption of a systemic bank on the payment system. The map of exposures will provide some information on the payment network. Existing stress tests done for payment and settlement systems can be used to gauge the impact of a business disruption on a large market participant.

Impact of a cyber-attack on several banks
A scenario can be run to assess the impact of a coordinated attack on multiple banks. In such a case, the contagion in the model is assumed to be very high. Additionally, the degree of contagion can be made dependent on the magnitude of losses, reflected in the tail dependence.

Mitigation of cyber-attacks

The ITU index of cyber security could be used to provide an overview of the level of cyber security in a given country and possible gaps identified by the different components of the overall score.

APPENDIX 2: ROBUSTNESS CHECKS FOR AGGREGATE LOSS DISTRIBUTION

In this appendix, we provide robustness checks for the models used to quantify losses.

Number of simulations

We increase the number of Monte Carlo simulations—in the case of independence of losses— and we obtain results which are very similar.

Table 1: Aggregated losses in the baseline case (in USD billion)

	10,000 simulations	100,000 simulations	1 million simulations
Average	97	102	101
Median	92	96	96
VaR (95%)	147	152	151
VaR (99%)	201	204	202
ES (95%)	187	190	190
ES (99%)	281	277	276

Alternative distributions

Using other distributions for the body such as normal distribution and Gamma distribution yield roughly similar results for the average and the mean, while there is more heterogeneity for risk indicators. This difference is partly explained by different parameters for the tail distribution which impact the VaR and ES.

Table 2: Aggregated losses in the baseline case (in USD billion)

	Lognormal GPD	Normal GPD	Gamma GPD
Average	97	114	90
Median	92	112	87
VaR (95%)	147	146	129
VaR (99%)	201	163	159
ES (95%)	187	157	150
ES (99%)	281	173	191
Parameters of the distribution			
Tail threshold	0.12	0.03	0.08
Bulk distribution parameters			
Average μ	1.72	12.6	0.46 (shape)
Standard deviation σ	1.89	15.7	45.6 (scale)
GPD parameters			
Shape ξ	0.45	0.24	0.39
Scale β	857	852	838
Threshold α	0.05	0.09	0.05