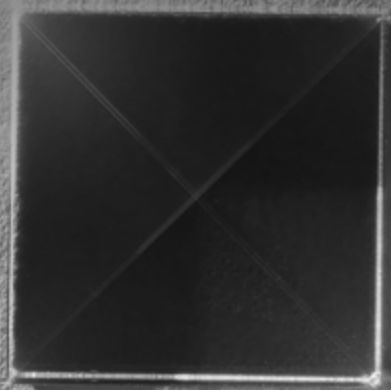
THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

ALTERNATIVE RISKS

Cyber risk for the financial services sector

ANTOINE BOUVERET



ALTERNATIVE CAPITAL MARKETS

#49 APRIL 2019

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

ALTERNATIVE MODELS

ALTERNATIVE RISKS

ALTERNATIVE MARKETS

DEAR READER,

Welcome to edition 49 of the Capco Institute Journal of Financial Transformation.

Disruptive business models are re-writing the rules of our industry, placing continuous pressure on financial institutions to innovate. Fresh thinking is needed to break away from business as usual, to embrace the more rewarding, although more complex alternatives.

This edition of the Journal looks at new digital models across our industry. Industry leaders are reaching beyond digital enablement to focus on new emerging technologies to better serve their clients. Capital markets, for example, are witnessing the introduction of alternative reference rates and sources of funding for companies, including digital exchanges that deal with crypto-assets.

This edition also examines how these alternatives are creating new risks for firms, investors, and regulators, who are looking to improve investor protection, without changing functioning market structures.

I am confident that you will find the latest edition of the Capco Journal to be stimulating and an invaluable source of information and strategic insight. Our contributors are distinguished, world-class thinkers. Every Journal article has been prepared by acknowledged experts in their fields, and focuses on the practical application of these new models in the financial services industry.

As ever, we hope you enjoy the quality of the expertise and opinion on offer, and that it will help you leverage your innovation agenda to differentiate and accelerate growth.

Lance Levy, **Capco CEO**

CYBER RISK FOR THE FINANCIAL SERVICES SECTOR

ANTOINE BOUVERET | Senior Economist, European Securities and Markets Authority[1]

ABSTRACT

Cyber risk has emerged as a major concern for the financial services sector. In this article, we outline the main channels through which cyber risk can affect a financial institution, and provide some insights based on recent cyber-attacks. We also outline a framework that can be used to estimate potential losses due to cyber risk for financial institutions.

1. INTRODUCTION: FINANCIAL INSTITUTIONS ARE HIGHLY EXPOSED TO CYBER RISK

Cyber risk has emerged as a systemic risk concern, following recent cyber incidents [IIF (2017), IMF (2017b), and OFR (2017)]. Indeed, recent surveys point to cyber risk as a main concern among market participants: it 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 they can lead to severe disruptions and major losses for the targeted firms.

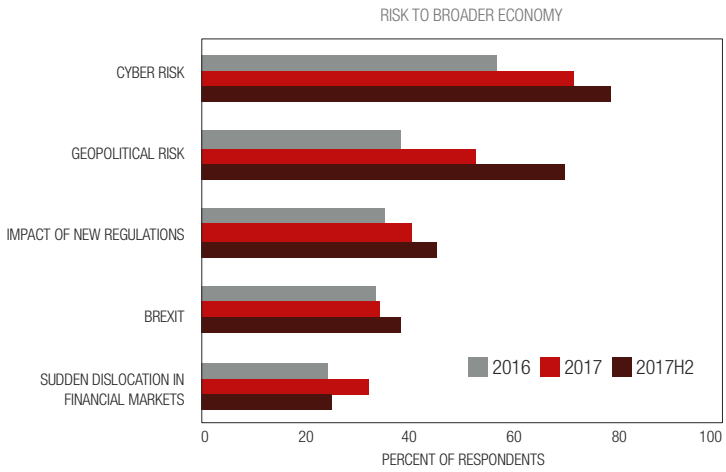
The financial services sector is highly exposed to cyber risk, across all types of countries. For illustrative purposes, we build an indirect measure of cyber risk by country for the financial services sector, using media coverage. An index is computed using the number of articles referring to cyber risk by country, divided by the number of articles referring to risk in the financial sector (Figure 3). 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.

Against that background, countries (and companies) have very different levels of cybersecurity. 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 4 shows the cross-country heterogeneity regarding cybersecurity, with most "advanced economies" and "emerging markets" having a high value on the cybersecurity index (above the median), while middle income and low-income countries tend to have lower values.

In that context, it is crucial to understand how cyber risk can affect financial institutions and why the financial sector is particularly vulnerable to cyber-attacks.

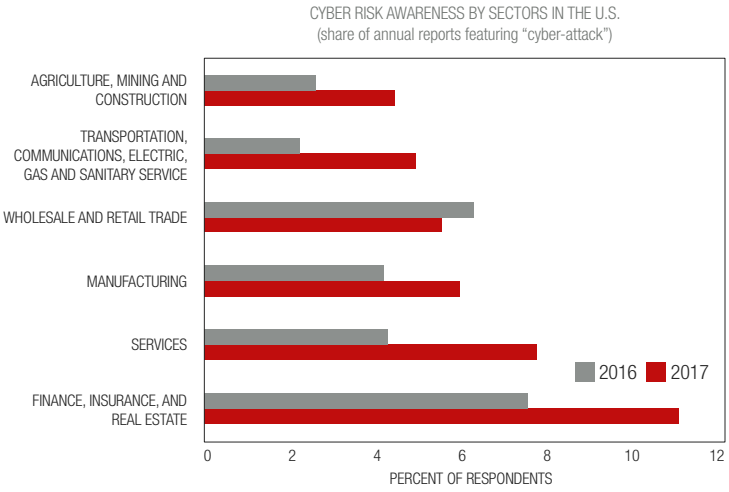
[1] The author alone is responsible for the content and writing of the paper. This article is based on work done by the author while he was at the International Monetary Fund. The views expressed are those of the author and do not necessarily represent the views of the IMF, its Executive Board, or IMF management. The views expressed are those of the author and do not represent the views of the European Securities and Markets Authority.

Figure 1: Survey of risks to financial stability



Source: DTCC Systemic Risk barometer

Figure 2: Reporting of cyber risk



Sources: SEC form 10-K; and staff calculations

2. HOW CAN CYBER RISK AFFECT FINANCIAL INSTITUTIONS?

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)]. 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 the misuse of the systems, as is the case for fraud. Finally, availability issues are linked to business disruptions.

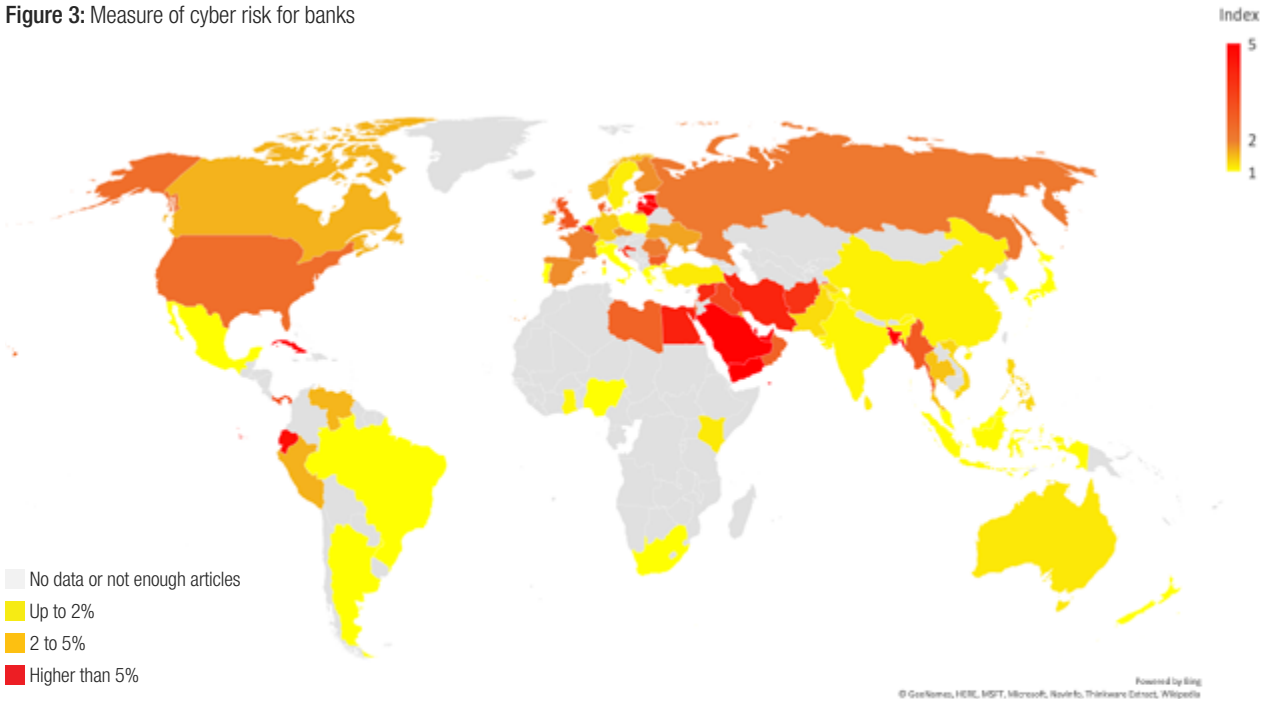
The three types of cyber-attacks have different direct impacts on the targets: business disruptions prevent firms from operating, resulting in lost revenue; fraud leads to direct financial losses; while the effects of data breaches take more time to materialize, through reputational effects as well as litigation costs. More generally, the risk of a loss of confidence following cyber-attacks could be high for the financial services 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 mainly impact the targeted firm in the short term.

2.1 "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 (Figure 2). 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. In that context, the ECB recently established the 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)].

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 system 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, but not in the context of cyber risk. For example, Clarke and Hancock (2014) use

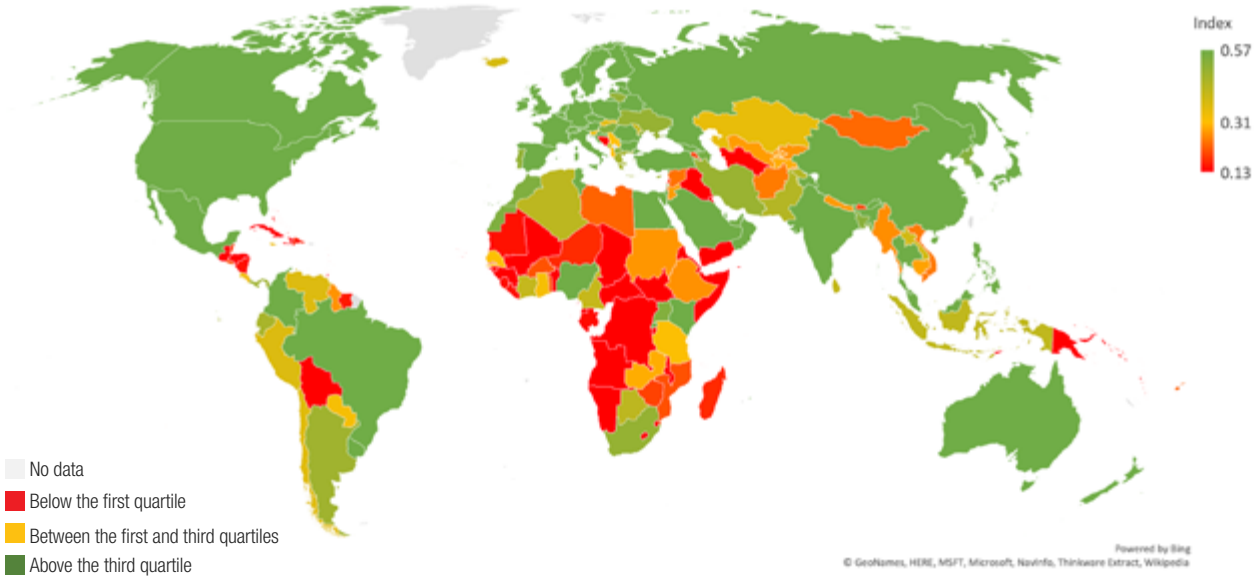
Figure 3: Measure of cyber risk for banks



Note: number of articles featuring "cyber-attack," "hack," "cyber risk," or "cybersecurity," and "banks," "bank," and "risk" divided by the number of articles featuring "banks," "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: January 2014-September 2017.

Sources: Factiva and author's calculations

Figure 4: Global cybersecurity index



Source: ITU (2017)

Table 1: Impact of disruption of infrastructures (all sectors)

SCENARIO	TARGET	LOSS (in U.S.$ bn)
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)

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.[2] 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) estimate 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), but again not in the context of cyber risk.[3] 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 studies estimate that a disruption of part of the U.S power grid could lead to up to U.S.$1 trillion in losses and a disruption of IT infrastructures up to U.S.$53 bn (Table 1).

2.2 Business disruptions in the financial services sector

DDoS attacks on multiple financial institutions

U.S.: in September 2012, the websites of Bank of America, PNC, JPMorgan, US Bancorp, and Wells Fargo were targeted and one month later the websites of BBT, Capital One, HSBC, Region Financial, and 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 U.S.$0.5 mn.

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

Finland: end of 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.

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 "distributed-denial of service" (DDoS) attack on the targeted firms' servers – when a very large number of requests are sent to the targeted servers, overloading the system and making it unable to operate. For example, on August 10 and 11, 2011, the news website of the Hong Kong stock exchange suffered DDoS attacks. 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 the 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 three to six days could lead to losses of around U.S.$24 bn [Lloyd's (2018)], with most losses occurring in the manufacturing and trade sectors, while losses for the financial services sector would be limited to U.S.$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% of the banks' total deposits and the bank had to use a liquidity assistance scheme provided by the authorities.[4]

Cyber-attacks can also target multiple financial institutions to disrupt the financial services 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).

[2] For example, in Switzerland the simulation of the disruption of the two largest participants would result in 50% of unsettled transactions, with contagion effects across banks [Glaser and Haene (2007)].
[3] See ESMA (2018) for details about the methodology and stress test results.
[4] In this case and in the following examples, the information on cyber risk is based on data provided by ORX News sourced from publicly available information.

2.3 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 ORX dataset, cyber-related fraud accounts for 90% of reported losses.

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 U.S.$1,450 mn in losses due to fraud since 2013 (Table 3).

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

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 U.S.$336 mn, while actual losses were around U.S.$87 mn, as some orders were frozen and some money was recouped.

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

INSTITUTIONS	DATE	INITIAL LOSSES (U.S.$ MN)	CURRENT ESTIMATED LOSSES* (U.S.$ MN)
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

* Current estimated losses are based on publicly available information. Targeted institutions are in the process of recovering the losses through legal proceedings.

Sources: ORX News, Financial Times

Table 3: Cyber-attacks on fintech firms)

INSTITUTION	DATE	ESTIMATED LOSSES (U.S.$ 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

ransomware targeting Ukraine lead to losses of at least U.S.$1.3 bn for multinational firms across sectors (transportation, construction, or food) linked to Ukrainian companies.[5] 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.

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

2.4 Data breaches

Financial institutions are also particularly vulnerable to data breaches. Given their reliance on customers' data to conduct business, the financial services sector suffered the most incidents with data loss in recent years – including the Equifax data breach where hackers may have stolen 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 services sector (Figure 5). The Ponemon Institute estimates that the average cost per stolen record was U.S.$141 in 2017 [Ponemon (2017)]. Applying the Ponemon estimates, losses due to data breach over the last three years would be around U.S.$38 bn for U.S. financial firms alone.

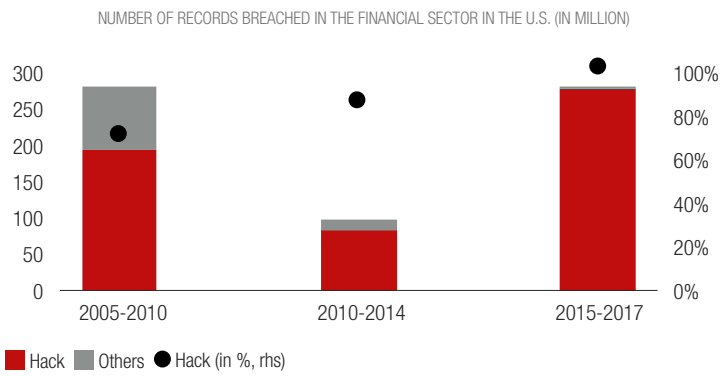
3. POTENTIAL LOSSES FOR FINANCIAL INSTITUTIONS DUE TO CYBER RISK

3.1 Background

Given the high degree of vulnerability of financial institutions to cyber risk, it is crucial for policymakers, risk managers, and executives to have a view of potential losses that financial institutions could face. Unfortunately, providing precise estimates of cyber loss is difficult for a variety of reasons. First, data on cyber-attacks are scarce, as it can take several weeks or months before the targeted institution is aware of the attack. Second, estimating the direct and indirect losses (reputational risk for example) is complicated and subject to uncertainties. Third, there is no common reporting template for cyber-attacks that would allow for a consistent collection of data. Finally, the modeling of cyber risk is still at an early stage.

Existing estimated of cyber losses range from U.S.$100 bn to close to U.S.$600 bn. Symantec (2013) reports an annual cost of cybercrime of U.S.$113 bn, using a survey to measure cyber-attacks and the average cost per attack. Anderson et al. (2013) estimate direct and indirect losses of around U.S.$215 bn using data from 2007-2012 on different types of cybercrime (online banking fraud, tax fraud, etc.), mainly from the U.K. and then extrapolated to the world. McAffee (2014) estimates global costs to be between U.S.$375 bn and U.S.$575 bn. However, most existing studies use very different data source and methodology to estimate losses, some of which are not directly tractable.

Figure 5: Data breaches in the U.S.



Source: Privacy Rights Clearinghouse

3.2 Overview of the model

Recently, I outlined a model that could be used to estimate losses due to cyber risks [Bouveret (2018, 2019)]. I applied an approach commonly used for operational risk assessment for banks, and the pricing for insurance contracts to cyber risk. The method is related to the Advanced Measurement Approach used by banks 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. The intuition is as follows: once we know the frequency of cyber-attacks per year and the distribution of losses due to cyber-attacks, it is possible to estimate the aggregated losses due to cyber-attacks.

The aggregate losses Z due to cyber risk are given by: $Z = X_1 + \cdots + X_N$

where the frequency N is a discrete random variable – the number of cyber-attacks per year – and $X_1, \cdots, X_N$ 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).

I assume that the frequency of cyber-attacks follows a Poisson distribution, and that losses are independent. Since $X_1, \cdots, X_N$ are independent and identically distributed, and independent of N, the expected aggregated losses E[Z] are given by: $E[Z] = E[N] \times E[X]$

And since N follows a Poisson distribution, then $E[N] = \lambda$, 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.

The next step is to determine the distribution of losses. Based on loss data provided by ORX news, I assume that most losses follow a lognormal distribution and that large losses follow a generalized Pareto distribution typically used to model fat tails (blackout scenarios). Once all the parameters of the models are estimated, I use 1 million Monte Carlo simulations to estimate the aggregate loss distribution [See Bouveret (2019) for technical details]. This amounts to 1 million years of data to ensure that the aggregate distribution cover a wide range of outcomes.

3.3 Results

Once the aggregate distribution of losses is obtained, it is possible to estimate directly the average losses due to cyber risks and compute risk indicators such as the Value-at-Risk (VaR, how much an institution might lose due to a cyber-attack over a given frequency and a given probability (i.e., 95%) and the expected shortfall (ES, average losses above the VaR).

In the baseline case, average losses due to cyber-attacks amount to almost U.S.$100 bn per year and median losses are at around U.S.$88 bn (Table 4). To put those figures in perspective, that would correspond to around 10% of banks' net income in 2016 (based on a sample of 7,947 banks). Those estimates point to sizeable potential aggregated losses in the financial services sector, far above publicly reported losses by financial institutions. However, estimated losses due to cyber risk are a fraction of operational risk losses for banks, which amounted to U.S.$260 bn in 2007 and U.S.$375 bn in 2009 [Hess (2011)].

Table 4: Distribution of aggregate losses

	BASELINE	SEVERE SCENARIO
AVERAGE	100	276
MEDIAN	88	254
95% VAR	167	405
95% ES	283	617
99% VAR	291	637
99% ES	599	1189

Source: Bouveret (2019)

Risk measures such as VaR and ES reflect the heavy tail of cyber losses with a 95% VaR at U.S.$167 bn and an ES at almost U.S.$283 bn in the baseline scenario. Losses would be even larger under the severe scenario, where the frequency of cyber-attacks would increase from around 990 attacks per year (baseline) to close to 2,800 attacks (twice the peak observed in 2013).

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 U.S.$3 bn in premium globally in 2017 and is expected to reach U.S.$12 bn to U.S.$20 bn in the next decade [Fitch Ratings (2017)].

However, most institutions do not have cyber insurance – with take-up rates of less than 30% across sectors – and coverage is limited: the average coverage limit purchased in 2016 was around U.S.$3 mn [CIAB (2016)], which is far below the average and median losses observed in our dataset. Finally, it is challenging for insurers to price cyber risk due to uncertainty about exposures and risks of correlated exposures, as analyzed by Eling and Wirfs (2016) in the context of the insurability of cyber risk.

4. CONCLUSION

Cyber risk is a major concern for financial institutions given the vulnerability of the financial services sector to cyber-attacks. In this article, we have outlined the main transmission channels through which a successful cyber-attack can impact a financial institution, and we also documented some recent cyber-attacks. Finally, we provide a framework that could be used to estimate losses due to cyber risk (and showed that the estimates are far above reported losses by financial institutions). Looking forward, more needs to be done to improve cyber awareness in organizations and improve cyber resilience.

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 Böhme, R. (ed.), The economics of information security and privacy, Springer

Bank of England, 2017, "Systemic risk survey results – 2017 H2," November, https://bit.ly/2EX2ET6

Bouveret, A., 2018, "Cyber risk for the financial sector: a framework for quantitative assessment," IMF Working paper No. 18/143

Bouveret, A., 2019, "Estimation of losses due to cyber risk for financial institutions," Journal of Operational Risk, forthcoming

Cebula, J. J., and L. R. Young, 2010, "A taxonomy of operational cybersecurity risks," Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University

Clarke, A., and J. Hancock, 2013, "Payment system design and participant operational disruptions," Journal of Financial Market Infrastructures 2:2, 53-76

Council of Insurance Agents & Brokers, 2016, "Cyber insurance market watch survey: executive summary," Council of Insurance Agents & Brokers, April

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

ESMA, 2018, "EU-wide CCP stress test 2017," European Securities and Markets Authority

European Central Bank, 2018a, "Establishment of a euro cyber resilience board for pan-European financial infrastructures," press release, 23 February

European Central Bank, 2018b, "Cyber resilience oversight expectations (CROE) for financial market infrastructures," Public Consultation Document, April

Fitch Ratings, 2017, "Cyber insurance – risks and opportunities," 13 November

FSB, 2017, "Financial stability implications from FinTech," Financial Stability Board June

Glaser, M., and 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

Hess, C., 2011, "The impact of the financial crisis on operational risk in the financial services industry: empirical evidence," Journal of Operational Risk 16:4, 364-382

IIF, 2017, "Cybersecurity and financial stability: how cyber-attacks could materially impact the global financial system," Institute of International Finance September.

IMF, 2017a, "Fintech and financial services: initial considerations," Staff Discussion Notes No. 17/05, International Monetary Fund

IMF, 2017b, "Is growth at risk?" Global Financial Stability Report, International Monetary Fund, October

ITU, 2017, "Global cybersecurity index (GCI) 2017," International Telecommunication Unit, July

Kopp, E., L. Kaffenberger, C. Wilson, 2017, "Cyber Risk, Market Failures, and Financial Stability," working paper no. 17/185, International Monetary Fund

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

McAffee, 2014, "Net losses: estimating the global costs of cybercrime," Center for Strategic and International Studies, June

OFR, 2017, "Cybersecurity and financial stability: risks and resilience," OFR Viewpoint, Office of Financial Research, February

Ponemon Institute, 2017, "2017 cost of data breach study," June

Shevchenko, P., 2010, "Calculation of aggregate loss distributions," Journal of Operational Risk 5:2, 3-40

Symantec, 2013, "Norton report 2013"

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO