CH &Co.

The Return on Investment of Cybersecurity

May 2021

Sebastien Meunier, Director US & Leader Cybersecurity Practice
Cindy Wang, Consultant US
Katya Guez, Consultant Canada

Contents

A board-level question

No week passes without the news of a new cybersecurity incident or data breach at a major company. The most severe incidents result in millions of dollars in losses for the impacted companies, up to an extreme 1.4 billion dollars in the case of Equifax[1]. On the other hand, large financial institutions spend millions of dollars on both projects and run-the-bank activities to protect themselves from cybersecurity risks. Questions may arise at the board about the cybersecurity budget: **"Are we investing enough to protect the firm and its customers"**? or on the contrary **"Are we spending too much on cybersecurity"**? Those are legitimate questions, as firms could spend extravagant amounts of money on cybersecurity, but the probability of an incident would never reach zero. Common sense tells us that there is a minimum amount of money that should be spent on baseline security measures, and a maximum amount above which the cost outweighs the benefits. The purpose of this article is to help financial institutions frame and address this issue.

Financial impact of cybersecurity events

The average financial impact of a cybersecurity event is challenging to estimate: it depends on the nature and criticality of the incident (volume of data breached, downtime, criticality of impacted process, etc.), but also on the methodology used to assess such costs (cost items considered, controls for the size and location of the firm, etc.). However, it is possible to provide a range. According to different studies, the average cost of an incident for a financial institution is **between USD 628k and USD 5.85M**:

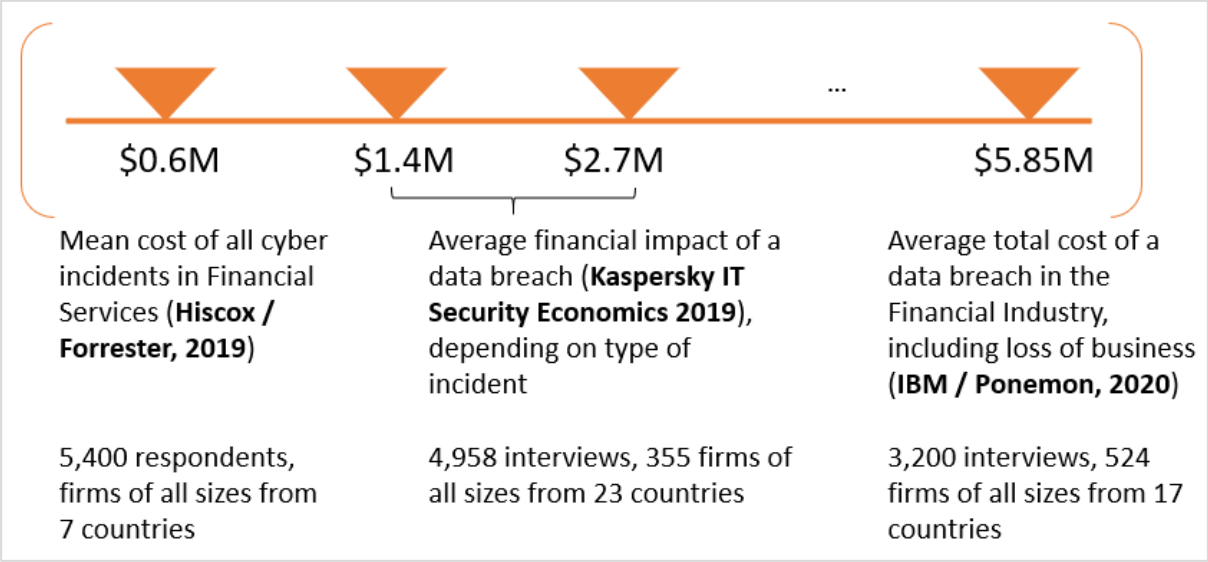

Figure 1: Range of average cost of a cybersecurity incident

Individual incidents can cost much less or much more than the average. IBM estimates that a breach of 1M records can cost a large company up to USD 300M. That figure seems high, but recent critical incidents did cost financial institutions more than USD 100M:

Company	Year of Incident	Incident and Impact	Size of Breach	Cost (USD)
Capital One	2019	An employee from Amazon Web Services, the cloud hosting company that Capital One was using, gained access to sensitive data by exploiting a misconfigured web application firewall. The cost does not include a $80 million fine by the Office of the Comptroller of the Currency (OCC).	100 million credit card applications and accounts	Between 100 and 150 million[2]
Desjardins	2019	A malicious insider accessed the personal data of 4.2 million accounts.	4.2 million individual records	108 million[3]
Postbank	2019	The bank discovered an internal breach leading to 25K fraudulent transactions over the course of 2 years. Postbank had to replace its 12M cards.	8-10 million beneficiaries	58 million[4]
EQUIFAX	2017	An application vulnerability led to the compromise of personal information of almost 150M Americans. The fine by US regulators amounted to $275M. Legal fees are not counted in the total cost.	148 million customers	1.4 billion[1]
BANGLADESH BANK Central Bank of Bangladesh	2016	30 SWIFT requests were made by attackers using Bangladesh Bank's SWIFT code, successfully stealing funds. The cost to enhance the Swift network security, including enhancements by each bank in the network, is not included in the total.	n/a	81 million stolen through transfer[5]

Regulators are increasingly issuing fines for failure to comply with cybersecurity or data protection regulations. Some high-profile cases involve cybersecurity incidents leading to data breaches of personal information falling under the General Data Protection Regulation in Europe. Regulators in the US are also actively auditing financial institutions and fining them whenever they find inadequate cybersecurity practices:

Company	Year of fine	Reason for fine	US Regulator	Fine (USD)
RMS Residential Mortgage Services	2021	Failure to conduct an appropriate investigation into the data breach and to provide a data breach notice to consumers or any state agency	NY State Department of Financial Services (NYS DFS)	1.5 million[6]
National a B. Riley Financial company	2021	Failure to implement multi-factor authentication, falling victim to four cyber breaches that exposed its customers' private data	NYS DFS	3 million[7]
Capital One	2020	Failure to establish effective risk assessment processes when migrating operations to public cloud environment, and failure to correct the deficiencies in a timely manner	OCC	80 million[8]
citi	2020	Deficiencies in data governance, risk management, and internal controls	OCC	400 million[9]
Morgan Stanley	2020	Failure to properly decommission hardware containing sensitive data	OCC	60 million[10]
USAA	2020	Unsafe and unsound practices related to USAA's compliance risk management program and IT risk governance program	OCC	85 million[11]

Focus on Ransomware

Cyber criminals increasingly use ransomware to infect their target with a malware that locks access to computers or encrypts their files to render them useless, demanding a ransom be paid to release them. In its 2020 Global Security Attitude Survey, Crowdstrike found that among US firms hit by a ransomware, **27% chose to pay ransoms, averaging USD 1.1 million**. The highest ransom to have ever been paid is believed to be USD 10M by the firm Garmin (which did not confirm). An advisory from the U.S. Department of the Treasury last Oct. 2020 warns that **ransom payments may risk violating the Office of Foreign Assets Controls (OFAC) regulations**[12], regardless of whether the victim or a third party (such as a cyber insurance company) arranged the payment.

Cost of Cybersecurity

The industry average internal cost to steer and run a cybersecurity program is equally difficult to estimate, because it varies depending on the methodology used to measure it, and on the nature of the firm (size, cybersecurity maturity, etc.). Cybersecurity **spending is generally estimated to be between ~5% and ~15% of the overall IT budget**. Kaspersky goes so far as to estimate the percentage to be ~29%, but it is an outlier compared to other studies:

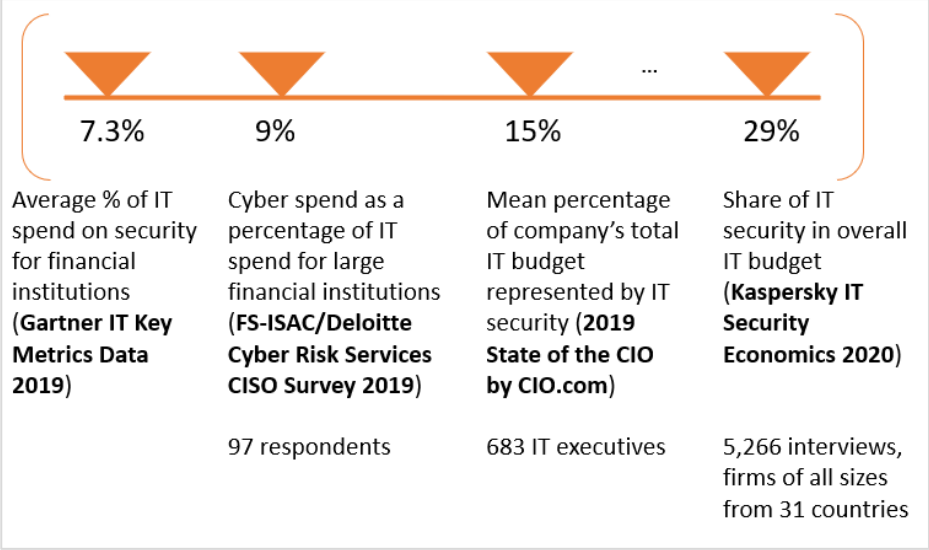

Figure 2: Average share of cybersecurity in IT budget (%)

Even though cybersecurity costs are generally expressed as a percentage of the total IT budget, cybersecurity goes beyond information technology. Users are very often the cause of incidents, making anti-phishing and cybersecurity awareness training, tabletop exercises, third-party cybersecurity risk management, and user monitoring controls key components of a cybersecurity program.

Two other metrics can be used to assess the cost of cybersecurity:

- **The average cost per employee**, which is estimated to be **$2,162** by Gartner and **$2,700** by FS-ISAC/Deloitte.
- **The cost in percentage of revenues**, which is estimated to be **0.56%** by Gartner, **0.4%** by FS-ISAC/Deloitte, and **0.16%** by Protiviti.

Some of the financial institutions' cybersecurity budgets were publicly communicated:

Company	Year	Cybersecurity Budget (USD)	Metric
BANK OF AMERICA	2018	660 to 680 million[13]	~$3,284 per employee
J.P.Morgan	2018	~600 million[14]	~$2,344 per employee[14]

The investment some banks had to make after a severe incident are also known:

- ~$1 billion over 2 years for HSBC[15] in 2016-2017;
- $150 million in 2020 and $250 million in 2021 for Desjardins[16].

Return is Risk Reduction

The average figures summarized above are useful figures to benchmark your financial institution against the industry. A more precise answer to the question in the introduction – the amount of money firms should invest in cybersecurity – depends on the maturity of the firm's cybersecurity program and risk appetite. Indeed, cybersecurity investment decisions should be decided using a risk-based approach. Based on a cybersecurity risk assessment, financial institutions should invest first in areas where the residual risk is high, to lower it to an acceptable level. The return on investment will be the reduction in operational risks for the organization, the associated release of risk capital, and the business growth it indirectly enables in a cost/risk effective manner.

Chappuis Halder & Co. recommends using the FFIEC Cybersecurity Assessment Tool (CAT) and/or the NIST Cybersecurity Framework (CSF) to perform this type of risk analysis. There are also quantitative approaches that can be used to estimate the monetary impact from cybersecurity risks, and to inform cybersecurity investment decisions. Simply stated, if a security investment can reduce the probability of a USD 100M incident from 1 every 3 years to 1 every 9 years, and the probability of a USD 1M incident from 1 every year to 1 every 3 years, it would "save" the organization USD 206M over 9 years, or USD ~23M per year. One model used to assess probable losses that Chappuis Halder & Co. recommends is the methodology developed by the FAIR[17] Institute:

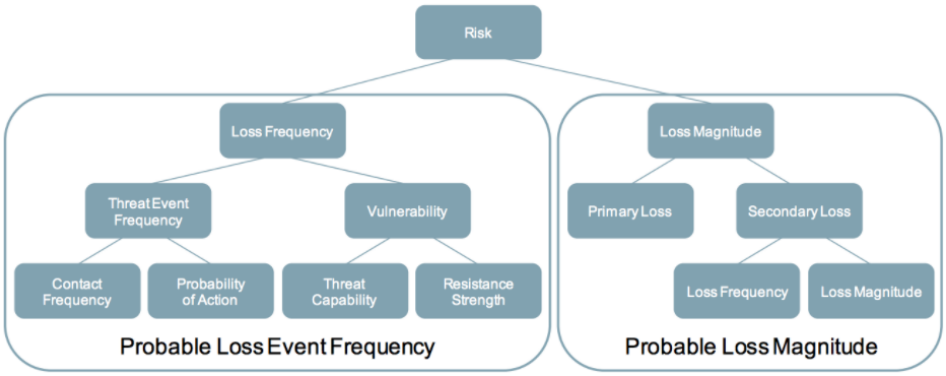

Figure 3: FAIR Risk tree

This approach can be applied focusing on two or three main threat scenarios ("what can go wrong"?) tailored to the organization's structure and maturity.

Actuarial models can also be used to assess probable losses. Cyber risk modelling is indeed maturing: a data schema standard was produced by the Cambridge Centre for Risk Studies[18] to report and monitor cyber risk exposure, and a Global Cyber Industry Loss Index is published by Property Claim Services since Sept. 2018[19]. We will deep dive on cybersecurity risk quantitative modelling in the next Chappuis Halder & Co. cybersecurity paper. Stay tuned!

Appendix 1: Cybersecurity at CH&Co.

CH&Co. is a **consultancy dedicated to Financial Services**, with 200 consultants in 6 offices worldwide. We have **excellent references in cybersecurity**:

- ~10% of CH&Co. revenues comes from cybersecurity projects in the US, France & Asia
- 15 projects in 2018-20, from strategy to security solution implementation (CyberArk, Box, Boldon James…)
- Management of cybersecurity programs with budgets of more than USD 15M

Strategic cybersecurity challenges with which we can help:

- Answer questions from the board about cyber threats, risk exposure & funding strategy:
  - Is the cybersecurity strategy aligned with our business objectives?
  - Are we spending appropriately on cybersecurity priorities?
  - What are our "crown jewels" and how well are they protected?
- Transform the cybersecurity function:
  - From a tactical function to a strategic and advisory function
  - From a reactive posture to proactive threat hunting & cyber risk management
- Develop a granular vision of cybersecurity risks along business' value chains (risk heatmap by line of business).
- Ensure security by design, from requirements to deployment, to maintenance of business solutions.
- Bring security closer to the data, by discovering, classifying, and securing the data from creation to deletion.
- Develop a cybersecurity culture across the organization.

We believe that **cybersecurity, technology, and data privacy risks** should be managed just like any other risk categories in the bank:

- Define the target operating model and governance across the 3 lines of defense.
- Model security threats to the organization.
- Assess inherent risks, accounting for existing vulnerabilities.
- Assess residual risks based on the effectiveness and coverage of existing security controls.
- Identify gaps between residual risks and the organization's risk appetite.
- Address residual risks by remediating each gap through mitigation, avoidance, transfer, or acceptance.

Appendix 2: Sources

Studies / White papers

Crowdstrike Global Security Attitude Survey 2020

Hiscox / Forrester Cyber Readiness Report 2019

Kaspersky IT Security Economics 2020

Kaspersky IT Security Economics 2019

IBM / Ponemon Cost of a Data Breach Report 2020

Gartner IT Key Metrics Data 2019

FS-ISAC/Deloitte Cyber Risk Services CISO survey 2019

2019 State of the CIO by CIO.com

Protiviti's view on Emerging Risks July 2019

Web articles / news

[1] bankinfosecurity.com/equifaxs-data-breach-costs-hit-14-billion-a-12473
[2] cnn.com/2019/07/29/business/capital-one-data-breach/index.html
[3] cbc.ca/news/business/desjardins-breach-cost-1.5476855
[4] cpomagazine.com/cyber-security/south-africas-postbank-replaces-12-million-bank-cards-after-internal-security-breach-exposes-master-key/
[5] reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR
[6] dfs.ny.gov/reports_and_publications/press_releases/pr202103031
[7] dfs.ny.gov/reports_and_publications/press_releases/pr202104141
[8] occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html
[9] occ.treas.gov/news-issuances/news-releases/2020/nr-occ-2020-132.html
[10] occ.gov/news-issuances/news-releases/2020/nr-occ-2020-134.html
[11] occ.gov/news-issuances/news-releases/2020/nr-occ-2020-135.html
[12] home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
[13] spglobal.com/marketintelligence/en/news-insights/trending/o9fc_uwerjjky-gq7phq7q2#:~:text=Against%20that%20backdrop%2C%20Bank%20of,of%20Fintech%20conference%20June%2020
[14] jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/ceo-letter-to-shareholders-2018.pdf
[15] krcl.com/articles/cyber-security/big-banks-invest-huge-sums-in-cybersecurity/
[16] blogues.desjardins.com/press_release/2020/12/desjardins-protection.php
[17] fairinstitute.org/what-is-fair
[18] jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-data-schema-v1.0.pdf
[19] verisk.com/press-releases/2018/september/pcs-launches-global-cyber-industry-loss-index/