Founding Partner
OPTUS

MACQUARIE University
SYDNEY·AUSTRALIA

# Governance of cyber security:

## STATE OF PLAY

Vincent McGrath, Elizabeth Sheedy, and Fan Yu
Acknowledgements: Optus-Macquarie Cyber Security Hub
Date: January 2022

## EXECUTIVE SUMMARY

With cyber losses mounting worldwide, the need for effective cyber security governance has never been greater. The objective of this paper is to identify what is currently known about this important topic and what remains to be further investigated. We examine both the academic and industry literature and draw upon several recent cases involving malicious external attackers and loss of customers' financial information, as these characteristics are associated with more significant loss of shareholder wealth.

### SECTION 1: CASE STUDIES

We discuss the following case studies: Equifax, Marriott, and two Canadian financial institutions (Bank of Montreal and Simplii, a subsidiary of CIBC). In the cases affecting a large number of customers (Equifax and Marriott), indirect costs dwarf the direct costs associated with the attack. Direct costs include investigating the attack, upgrading security after the attack, fines, and customer remediation. Indirect costs (sometimes called reputational costs) occur when customers and other stakeholders take their business elsewhere or demand a change in the terms of doing business.

### SECTION 2: WHAT AND WHY OF CYBER GOVERNANCE

This section considers cyber governance in the broader context of risk governance. Drawing on existing research on risk governance, we identify key structural elements: effective board of directors with cyber security skills and an appropriate committee to focus on cyber security; specialist senior executive expertise with access to the board, such as a Chief Information Security Officer (CISO); risk, compliance, and assurance functions that are adequately resourced with cyber security expertise; executive accountability for cyber security, with appropriate rewards and sanctions; and disclosure of cyber security risks and risk management practices.

### SECTION 3: DISCLOSURE OF CYBER RISK

Evidence suggests that disclosure expands following a damaging cyber attack. There is, however, no clear evidence to suggest that expanded disclosure of cyber risk is associated either with greater likelihood of attack or with superior cyber resilience. Of our case study firms, the one with the most expansive cyber disclosure, Equifax, suffered the most severe cyber attack. New research that uses machine-learning to analyse the text of cyber disclosures and quarterly earnings calls offers some promise in this regard.

### SECTION 4: BOARD STRUCTURES/COMMITTEES AND CYBER RISK

The effectiveness of governance structures in relation to cyber risk outcomes is not yet well understood. Very few papers have been published in this area and those that exist are quite recent. Kamiya et al. (2021) find that the existence of a board risk committee reduces the likelihood of an attack, although Akey et al. (2021) find no association. There is, however, some evidence to suggest that cyber risk governance is reformed following a cyber attack. Risk governance is also transformed after cyber attack on a peer firm.

### SECTION 5: EXECUTIVE COMPENSATION AND CYBER RISK

Analysis of the four cases reveals remarkably little executive accountability following even severe cyber attacks. Lack of serious consequences for senior executives is a problem because it may encourage lack of diligence in cyber risk management processes. We also identify opportunities to better design executive compensation practices to promote better cyber risk management.

### SECTION 6: CYBER SECURITY GOVERNANCE SCORES

ESG ratings play an increasingly important role in the financial system. Within the broad 'governance' category, a several providers now offer cyber security governance scores. We conduct a preliminary investigation of the scoring system provided by S&P Global, considering large banks in Australia, Canada, the UK, and the US. We find that while cyber security governance scores are correlated with past cyber attacks, they have no value for predicting future cyber attacks. This raises questions about the methodologies used by ESG ratings providers that warrant further investigation.

## 1. CASE STUDIES

In this section, we analyse several illustrative cyber security breaches: Equifax, Marriott International Inc., and breaches at two Canadian Banks. These cases are selected because they occurred within the last five years and represent multiple industries, jurisdictions, and levels of severity. All these events involve malicious external attackers and resulted in the loss of financial information of customers, factors that are associated with more significant impact.

For each case study we discuss the key facts, the direct costs, and the stock market reaction. The stock market reaction is evaluated using the cumulative abnormal returns (CAR)[1] of the target firm to that of their industry peers from one month before the public disclosure to one year after the public disclosure. The stock market reaction is important because it helps to measure the total cost of the attack including indirect as well as direct costs. The direct or out-of-pocket costs (system upgrades, investigation and remediation costs, legal and regulatory costs) can be dwarfed by indirect or reputational costs, causing significant loss of shareholder wealth (Kamiya et al., 2021; Lending et al., 2018). Stakeholders adjust their estimate of the likelihood and impact of further attacks, and downgrade their assessment of the quality of risk governance, and are no longer willing to transact with the organisation on the same terms.

A customer, for example, may switch to a competitor or require a discounted price to remain with the same firm. If new executives with greater cyber expertise are brought in to clean up the mess, they may demand higher remuneration. An insurer may require higher premiums on cyber policies, a provider of debt capital may require a higher rate of interest to reflect the perceived increase in risk, auditors may demand higher fees, and some shareholders may respond by withdrawing their capital. This is particularly true in an environment where ESG investors, who place high importance on effective governance, play an increasingly important role in capital markets.

According to Xu et al. (2019), additional indirect costs arise due to higher rates of real earning management. Following a data security breach, firms are more likely to engage in cutting discretionary expenses and reducing the cost of goods sold through overproduction, especially when the breach involves loss of financial information, when disclosure of the breach is delayed, or if there is low analyst coverage. These activities lead to lower subsequent performance.

1 CAR adjusts share price movements to take account of movements in the broader market at the time. In other words, if the broader market was also falling at the time of the cyber attack for other reasons, then CAR would measure only the change in share price that cannot be explained by the broader market.

### 1.1 EQUIFAX

Equifax is a US based consumer credit reporting agency with operations in 24 countries worldwide. On the 7th of September 2017, the company disclosed that hackers had gained access to its IT system, compromising the personal records of around 143 million US customers and an undisclosed number of impacted customers in the UK and Canada. The compromised information included names, addresses, dates of birth, social security numbers, and the credit card information of up to 209,000 of its US customers.

In the days after the disclosure of the cyber security breach, Equifax's share price fell from $141.39[2] to $92.98[3], wiping over $5.8 billion from its market capitalisation. Advisen[4] estimates the direct cost of the breach at $1.35 billion, including $83 million in technology and security costs, $12.5 million in legal and investigative fees, and $690 million in pre-tax legal accruals. As of July 2019, the actual legal costs totalled approximately $700 million, $425 million in consumer compensation, and $275 million in fines (Leonhardt, 2019). Comparing the stock market reaction to the direct costs incurred by the firm, the indirect costs to Equifax were significantly greater and dominated the direct costs.

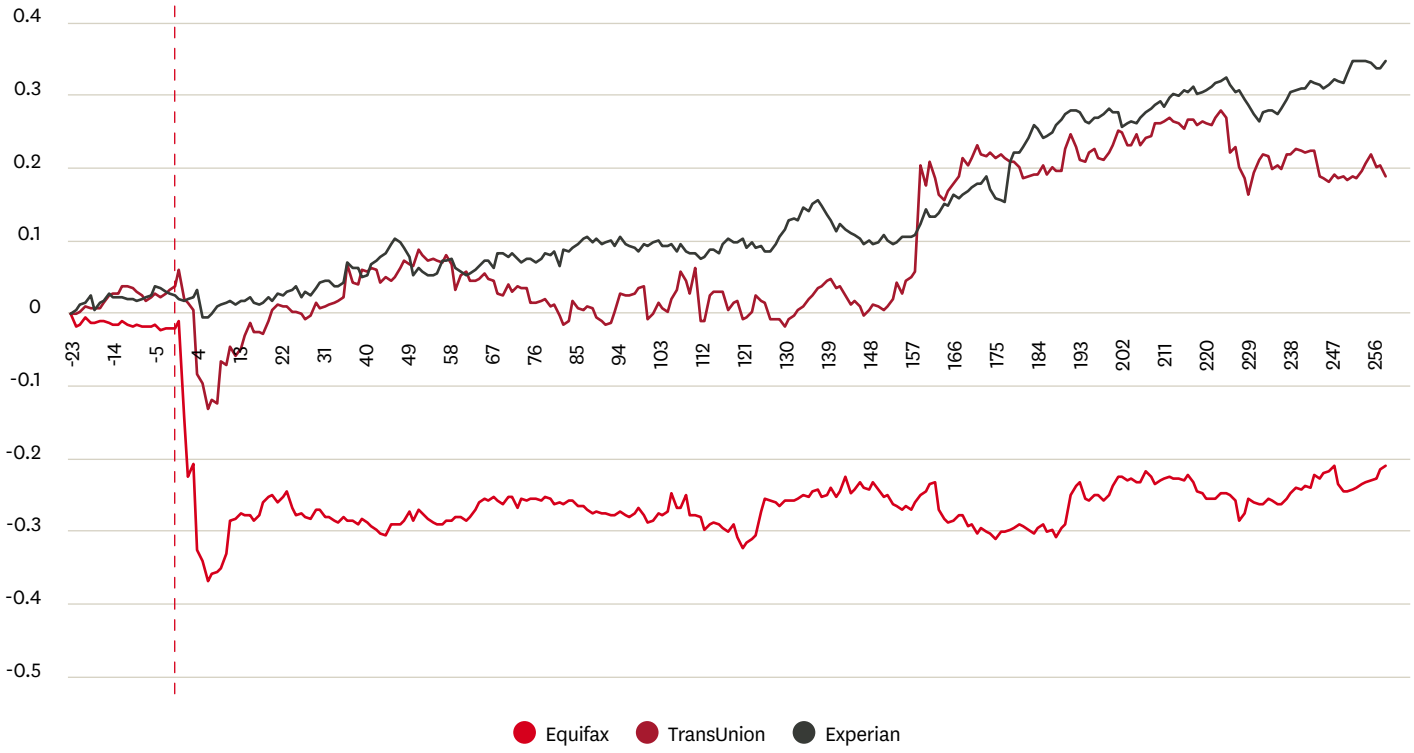


FIGURE 1. CARS OF EQUIFAX AND ITS PEERS PRE- AND POST-CYBER SECURITY BREACH DISCLOSURE
This figure shows the cumulative abnormal returns (CAR) of Equifax, TransUnion, and Experian from one month before the public disclosure of the cyber security breach to 12 months after the breach. CAR is equal to actual return – expected return, where expected return is estimated using the market model (ie, expected return = $\alpha + \beta$*(return on the benchmark). The estimation period for $\beta$ is the 250 trading days prior to the beginning of our sample. The benchmark for Equifax and TransUnion is the S&P 500, while the benchmark for Experian is the FTSE 100.

The massive loss in shareholder wealth can be explained by reputational effects as customers and other stakeholders took their business elsewhere or adjusted their terms of doing business. Providers of debt capital, for example, are likely to have required higher rates of interest as they re-evaluated the risk management skill of the attacked firm. Empirically, Sheneman (2017) reveals that the cost of debt is higher for breached firms relative to non-breached firms by an average of 25 basis points. Sheneman suggests the cost of debt increases because of increased monitoring costs and changes in lenders' credit risk assessments of firms.

Figure 1 shows the CAR for Equifax and two peers, TransUnion and Experian, from one month before the disclosure of the breach to one year after the disclosure. In the lead up to the public disclosure, Equifax's share price underperformed its peers, suggesting some information leakage in the days prior to the official announcement of the cyber security breach. On the announcement of the breach, Equifax's share price fell sharply, as did the share price of its domestic rival TransUnion. This suggests that a breach has an impact on shareholders' perceptions regarding the cyber security of peer firms[5]. Both Equifax and TransUnion share prices continued to fall in the week post the cyber security breach. The share price of the UK based Experian appeared unaffected by the announcement of the breach. Further, in the year after the breach, the share price of Equifax underperformed its peers, suggesting the cyber security breach had a lasting effect on its share price.

2 Closing price on 6th of September 2017, the day prior to the announcement day.

3 Closing price on 15th of September 2017.

4 Advisen is a provider of data for the insurance industry. Its cyber loss data provides a historical view of more than 90,000 cyber events collected from reliable and publicly verifiable sources. These records are limited, however, to direct costs.

5 Empirical research has also looked at how cyber security breaches impact the share price of peer firms. Haislip et al. (2019) show that the share price of peer firms may be affected by the disclosure of a cyber security breach, suggesting an increase in the perceived probability that other firms in the same industry will suffer future cyber security breaches or that they have already suffered cyber security breaches that they have not reported.

### 1.2 CANADIAN BANKS (BANK OF MONTREAL AND SIMPLII FINANCIAL)

On the 28th of May 2018, two Canadian financial institutions, the Bank of Montreal and Simplii Financial, a subsidiary of the Canadian Imperial Bank of Commerce (CIBC), disclosed cyber security breaches. The personal information of 113,151 Bank of Montreal and 10,101 CIBC customers was stolen. The breaches cost the Bank of Montreal and the CIBC $6.85 million and $1.8 million respectively in client remediation and up to $21 million and $1.8 million respectively in legal settlements (Yolles, 2021). On the announcement of the cyber security breaches the shares of both the Bank of Montreal and CIBC went down slightly, as did the shares of the other big Canadian banks, with the Bank of Nova Scotia falling the most.

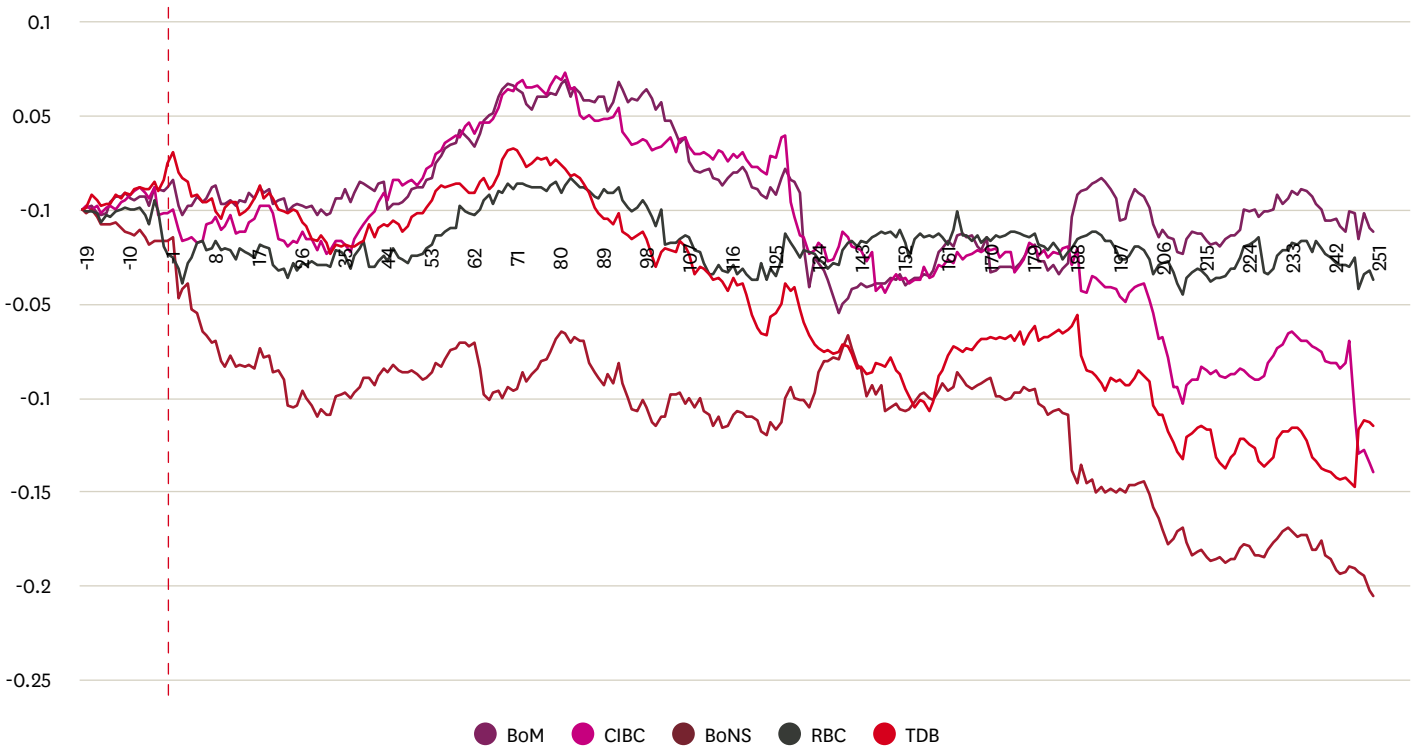


FIGURE 2. CARS OF BANK OF MONTREAL AND CIBC AND THEIR PEERS PRE- AND POST-CYBER SECURITY BREACH DISCLOSURE
This figure shows the cumulative abnormal returns (CAR) of Bank of Montreal (BoM), Canadian Imperial Bank of Commerce (CIBC), Bank of Nova Scotia (BoNS), Royal Bank of Canada (RBC), and Toronto-Dominion Bank (TDB) from one month before the public disclosure of the cyber security breach to 12 months after the breach. CAR is equal to actual return - expected return, where expected return is estimated using the market model (ie, expected return = $\alpha + \beta$*(return on the benchmark). The estimation period for $\beta$ is the 250 trading days prior to the beginning of our sample. The benchmark for BoM, CIBC, BoNS, RBC and TDB is the TSX60.

Figure 2 shows the CAR of the Bank of Montreal and the CIBC, along with three peers, the Bank of Nova Scotia, the Royal Bank of Canada (RBC), and the Toronto-Dominion Bank, from one month before the disclosure of the cyber security breach to one year after the breach. On the day after the disclosure of the cyber security breach, the share prices of all the Canadian banks fell slightly. In the days and weeks that followed, the share prices of both the breached banks (ie, Bank of Montreal and CIBC) performed similarly to their peers. This suggests that the disclosure of the breaches was not considered material by the market; reputational damage was limited, and this is likely due to relatively small number of affected customers. To put this in perspective, the attacks at Bank of Montreal and CIBC together affected fewer than 0.33% of the Canadian population (123,252 out of 37 million). In contrast, the Equifax attack affected 44% of the much larger US population (143 million out of 325 million).

### 1.3 MARRIOTT

Marriott International Inc., is an American multinational company that operates, franchises, and licenses hotel, residential, and timeshare properties. On the 30th of November 2018, the firm disclosed that a breach of the reservation database of its Starwood subsidiary exposed the private information of up to 500 million customers. This information included names, addresses, phone numbers, credit card numbers, passport numbers, and travel arrangements.

On the day the breach was announced, Marriott's share price fell from $121.84 to $115.03, while the S&P 500 index increased by 0.82%. Although it rebounded the next day, by the end of the year the Marriott share price was $100.99 (representing a 17.1% decrease from the date of the breach) while the S&P 500 decreased by 9.2% over the same period. This equates to a $2.4 billion fall in market capitalisation the day after the breach was announced and a $7.4 billion fall in market capitalisation by the end of the year. Advisen estimates the direct expenses related to the breach totalled $198 million, of which $77 million was covered by insurance. Marriott was also fined $19 million by the UK's Information Commissioner's Office. Comparing the stock market reaction and the costs incurred by the firm, it appears Marriott suffered some reputational damage because of the breach.

Figure 3 shows the CARs of Marriott and its peers, Hilton Worldwide Holdings Inc. and Hyatt Hotels Corporation, from one month before the disclosure of the cyber security breach to one year after the disclosure. In the days before the public disclosure, the cumulated abnormal return was negative, suggesting some information leakage prior to the public disclosure. On the day of the disclosure, Marriott's share price fell sharply. Although it rebounded slightly the following day, it kept falling afterwards and it underperformed relative to its peers for several weeks. The share prices of the peer firms also fell on the day of the public disclosure, but they rebounded the following day. In the year after the breach, Marriott outperformed Hyatt and underperformed Hilton in regard to CAR. It is unclear whether the cyber security breach had a lasting impact on its share price.

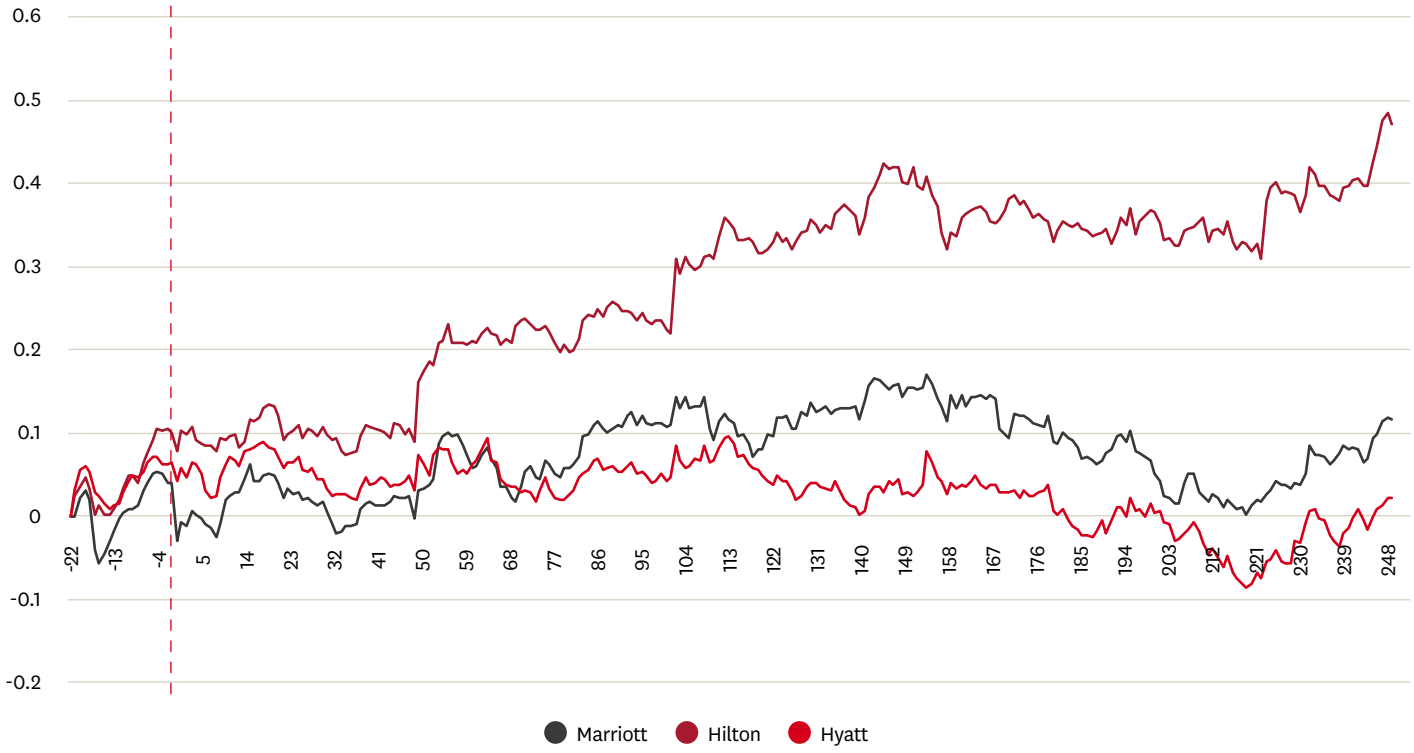


FIGURE 3. CARS OF MARRIOTT AND ITS PEERS PRE- AND POST-CYBER SECURITY BREACH DISCLOSURE

This figure shows the cumulative abnormal returns (CAR) of Marriott, Hilton, and Hyatt from one month before the public disclosure of the cyber security breach to 12 months after the breach. CAR is equal to actual return - expected return, where expected return is estimated using the market model (ie, expected return = $\alpha + \beta^*$ (return on the benchmark). The estimation period for $\beta$ is the 250 trading days prior to the beginning of our sample. The benchmark for Mariott, Hilton, and Hyatt is the S&P 500.

### 1.4 GENERAL TRENDS

Empirical research on the impact of cyber security breaches on share prices has produced mixed results. Kamiya et al. (2020) analyse data breach events reported to the Privacy Rights Clearinghouse (PRC) over the period 2005 to 2017, considering only successful malicious external actions, such as hacking and malware. In this sample, the short-term loss in shareholder wealth is measured over the three-day period including the announcement. The three-day window CAR(-1,1) (ie, the cumulative abnormal return from the trading day prior to the announcement date to the trading day after) is significant and negative in cases where an attack leads to a loss of personal financial information as in the case of Equifax. An attack with no loss of financial information does not, on average, produce a significant short-term stock reaction measured by CAR(-1,1). The loss in value is greater for older firms and those that do not have a board risk committee.

Hogan et al. (2020) use the more comprehensive proprietary data set developed by Advisen. They confirm that attacks involving personal financial information are associated with significantly negative short run returns. Long term results of their entire sample show significantly negative results for up to 250 trading days from the announcement date of up to -7.46%.

Table 1 shows that both Equifax and Marriott suffered a large and negative CAR(-1,1) around the time of the attack, especially in comparison to peer firms. Notably, neither firm had a board risk committee at the time of the attack. It is interesting to note that the Canadian banks both had board risk committees at the time of the attack and were well respected for excellence in risk governance generally (Sheedy & Griffin, 2018). This recognised strength is likely to have contributed both to the small scale of the breaches and the modest market reaction.

TABLE 1: SHORT-TERM IMPACT OF CYBER ATTACKS ON SHAREHOLDER WEALTH

This table shows the abnormal returns (AR) the day before the cyber breach disclosure, the day of the disclosure, and the day after the disclosure in addition to the cumulative abnormal returns from the day before to the day after the disclosure of the cyber breach (CAR(-1,1)). Breached firms are in bold and their peers are not. Note that the Canadian Big 5 Banks comprise the Bank of Montreal (BoM), Canadian Imperial Bank of Commerce (CIBC), Bank of Nova Scotia (BoNS), Royal Bank of Canada (RBC), and Toronto-Dominion Bank (TDB).

| | **Credit rating agencies** | | | **Canadian big 5 banks** | | | | | **US hotel companies** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Equifax** | TransUnion | Experian | **BoM** | **CIBC** | BoNS | RBC | TDB | **Marriott** | Hilton | Hyatt |
| **AR -1** | **-0.11%** | 0.61% | -0.08% | **0.20%** | **-0.02%** | -0.07% | -0.38% | 0.92% | **0.05%** | -0.43% | 0.19% |
| **AR 0** | **0.94%** | 2.13% | -0.48% | **0.45%** | **0.19%** | 0.19% | -0.19% | 0.55% | **-6.99%** | -2.17% | -2.26% |
| **AR +1** | **-13.24%** | -4.01% | -0.40% | **-1.37%** | **-1.10%** | -3.18% | -0.60% | -1.09% | **2.43%** | 2.38% | 1.48% |
| **CAR(-1,1)** | **-12.42%** | -1.26% | -0.96% | **-0.73%** | **-0.93%** | -3.05% | -1.17% | 0.38% | **-4.52%** | -0.23% | -0.59% |

## 2. WHAT AND WHY OF CYBER GOVERNANCE

Risk governance is one of the most noticeable governance trends of this century, and nowhere is the need more obvious than in the domain of cyber risk. According to Shevchenko et al. (2021), the frequency of reported cyber risk events has increased substantially over time, and it is likely that many events are not publicly reported. While most losses from cyber events are small, there is a small number of extremely damaging cyber events: 1.4% of direct cyber related losses exceed $100 million, and 0.17% of events cause direct losses greater than $1 billion. More than 60% of companies that report cyber related losses have experienced multiple costly attacks.

The rationale for risk governance is drawn from an understanding that humans are prone to numerous cognitive biases that impede their ability to manage risk (Sheedy, 2021). Short-termism, availability bias, and overconfidence are just some of the biases that often prevent managers from taking costly short-term actions that might produce longer-term benefits, especially when the costs are unequivocal yet the benefits are ambiguous. These biases are often compounded by incentives that encourage a short-term perspective, causing risk management functions to be chronically under-resourced.

The domain of cyber risk is rapidly evolving, has a high degree of technological complexity, with jargon terminology poorly understood by most directors and senior executives, and a shortage of skilled workers. These factors, combined with the inherent challenge of risk governance, creates some unique governance challenges that deserve special attention. According to international standards, the goal of risk management is the creation and protection of value; it is not to eliminate risk but to ensure that the organisation achieves its objectives[6]. Certain organisational structures are considered important in risk governance (Sheedy, 2021) and these are summarised in Table 2.

While these structures appear to support better risk outcomes, they can be undermined by an organisational culture that does not prioritise risk management. This is particularly true in highly regulated industries, such as financial services, where the structures of risk government are mandated. If risk governance structures are not truly valued by the organisation, then they can lose their effectiveness. Therefore, the structures need to be combined with a favourable 'risk culture', defined as the behavioural norms that hinder or help effective risk management. Assessing risk culture can be challenging, especially for external stakeholders (see Institute of Internal Auditors of Australia, 2021).

The Australian Securities and Investments Commission (ASIC) provides useful information for boards in relation to cyber resilience. The legal and compliance requirements relating to cyber security are explained in Report 429, Appendix 2.[7]

TABLE 2: STRUCTURES OF RISK GOVERNANCE

| | |
|---|---|
| **The role of the board** | A board with an appropriate level of cyber security skill is important for:<br>• Formulating strategy and risk appetite (ie, the amount of risk acceptable and consistent with strategic objectives).<br>• Approving risk policy (ie, the risk management framework established by executives).<br>• Supervising the executive with appropriate challenge<br>• Providing accountability (ie, rewards and sanctions should reflect risk outcomes). |
| **Board committee** | A board committee should be explicitly assigned responsibility for cyber security, advising the main board. It should be chaired by an independent director and ideally comprised of independent directors with relevant expertise. Often this is called the Risk Committee, or the Audit, Risk and Compliance Committee. |
| **Senior executive** | Specialist senior executive expertise with access to the board, eg, Chief Information Security Officer (CISO) |
| **Specialist functions** (risk, compliance, IT) | While cyber risk should be owned and controlled by the business itself, specialist functions (risk, compliance, and IT) are needed to advise, support, and review. |
| **Audit** | Both external and internal auditors provide independent assurance to the board that the risk management framework is working as intended and that the organisation is operating within the specified risk appetite. |
| **Executive compensation** | Remuneration systems should promote prudent risk management and sustainable outcomes, rather than short-term orientation. |
| **Risk disclosures** | Investors and other external stakeholders should be provided with sufficient accurate information about the organisation's risks and how they are managed. |

6 See ISO31000: Risk Management (2018).

7 ASIC 'Report 429: Cyber Resilience Health Check' available at https://asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf
See also resources available at: https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/

## 3. DISCLOSURE OF CYBER RISK

Risk disclosure is considered an important aspect of risk governance, as indicated in Table 2. Concerns exist about the quality and sufficiency of risk disclosures since executives may have incentives to understate vulnerability to cyber risk and overstate defences against it. Disclosing negative information about cyber security could increase the cost of capital and reveal confidential information to both competitors and attackers. On the other hand, insufficient disclosure could leave a firm vulnerable to litigation and loss of reputation.

Since 2005, the US Securities and Exchange Commission (SEC) has required firms to provide investors with information about the material risks to securities of the issuer. No quantitative information is required, so disclosures in the annual 10-K filings[8] are often vague, simply listing the relevant risks. These risk disclosures are viewed by many as a legislative shield, designed more to protect the firm from shareholder class actions than to provide useful information to shareholders. In 2011 the SEC produced guidance on the topic of cyber risk disclosure and this was further developed in 2018. Nevertheless, firms retain discretion over whether and how to disclose cyber risk. Concerns remain that cyber security disclosure is typically uninformative and boilerplate (Li et al., 2018). Li et al. (2018) find that both the presence and the length of cyber security risk disclosure is informative (ie, positively associated with future cyber incidents). However, since 2011, when the SEC guidance came out, the relationship has become insignificant.

In this section, we analyse formal cyber security disclosure for each of the case study companies described in Section 1. In each case, we compare the firm's cyber security disclosure with its peers. For example, when we analyse disclosures at Equifax, they are compared to disclosures at Experian and TransUnion, the other two big consumer credit rating agencies.

In a similar manner to Klemash et al. (2020) and Heroux and Fortin (2020), we analyse the firms' 10-K disclosures on cyber security and identify important information in four categories (cyber risks description, cyber risks identified, potential impacts identified, and cyber risks mitigation) as shown in Table 3. If a firm discloses the information for the corresponding sub-category, it receives a point. For example, Equifax identified three potential impacts of cyber security failings in its 10-K report for the fiscal year 2016, so it receives a score of 3 for the year. The scores for each selected firm in the periods pre and post the cyber events are illustrated in Table 4. Table 5 presents average cyber disclosure scores in each of the sectors we investigate.

Our findings are as follows. First, cyber security disclosure expands following a breach for both the event firms and their peers. This expansion is generally more pronounced for breached firms. This finding suggests a peer effect in cyber disclosure.

Second, jurisdiction may matter. In our sample, disclosure is generally more expansive in the US. For example, the US-listed firms Equifax and TransUnion have higher cyber disclosure scores than their UK-listed peer Experian. In 2017, the year before the Equifax breach, TransUnion received a score of 22 while Experian received a score of 12. Table 5 shows that scores for the Canadian banks are much lower than those in the US consumer credit rating agencies, despite the fact that all these firms are likely targets of cyber attacks.

Third, cyber disclosure scores vary across industries (see Table 5). If we compare only the US-listed consumer credit rating agencies and US-listed firms in the hotel industry, we find that the scores are higher for the consumer credit rating agencies in almost all the dimensions except for "potential impacts identified".

Fourth, even within a homogenous group of firms such as the Canadian Banks, the quality and scope of disclosure varies widely (see Table 4). The score ranges from 2 to 7 in the dimension "cyber risks mitigation".

There is no clear evidence to suggest that expanded disclosure of cyber risk, either of the potential risks or of mitigation strategies, is associated with greater cyber resilience. Of our breached case study firms, the one with the most expansive cyber disclosure, Equifax, suffered the most severe cyber attack.

8 A 10-k filing is a comprehensive annual report made to the SEC.

### 3.1 CYBER DISCLOSURE COVERAGE

There are no specific regulations to guide cyber disclosure, nor is there any evidence base to suggest what constitutes 'good' disclosure. We can, however, categorise different elements or categories of disclosure. Based on our analysis of the cyber disclosures of our case study firms and their peers, we identify four categories of cyber disclosure: a general overview of a firm's cyber security risks; a description of specific types of cyber security risks; a description of the potential negative consequences of a cyber security event; and finally, a description of a firm's cyber risk mitigation techniques.

Many firms provide an overview of the cyber security risks they face. This might include discussion of the source of cyber security risks, eg, *"Given our pervasive use of the internet and reliance on advanced digital technologies, we face common banking information security risks"* (Bank of Montreal, 2020). This section might also outline why the firm faces risks around information privacy, ie, *"We own and host a large amount of sensitive and confidential consumer information including financial information, personally identifiable information and protected health information"* (TransUnion, 2018). It would also acknowledge the risks around dealing with third parties, ie, *"those of our third-party vendors and other service providers could be vulnerable"* (Equifax, 2018). It would acknowledge the risk of changing cyber security regulations, ie, *"These regulations are complex, change frequently, have tended to become more stringent over time, and are subject to administrative interpretation and judicial construction in ways that could harm our business"* (Equifax, 2018). Finally, the firm may describe the potential perpetrators, ie, *"cyberattacks can originate from a wide variety of sources, including sophisticated threat actors involved in organized crime, sponsored by nation-states, or linked to terrorist or hacktivist organizations"* (TransUnion, 2018).

A second category relates to the specific cyber security risks the disclosing firm faces. An exhaustive list of risks would be infeasible; however, the firm may acknowledge some of the most common, including human error, hacking, computer virus, malware, phishing, denial of service attacks, and unauthorised disclosure of private information. A good example is Equifax, who in 2018, one year after its major breach, acknowledged the following cyber security risks in its 10k report *"computer viruses, denial-of-service attacks, employee or insider malfeasance, human error", "unauthorized access, misuse, malware, phishing"*, and *"sensitive data may be accessed, stolen, disclosed or lost."*

The third category discusses the potential negative impacts from a cyber event. Again an exhaustive list of risks would be infeasible; however the firm may acknowledge that cyber events have financial, operational, legal, and reputational consequences and may lead to remedial and increased security costs. A good example is Marriott, who in 2019, one year after the discovery of a major breach at its subsidiary, Starwood Hotels, acknowledged the following potential impacts from cyber events *"adversely impact our reputation and could result in legal, regulatory and other consequences, including remedial and other expenses, fines, or litigation"* and could lead to *"operational inefficiencies and a loss of profits"*.

Finally, disclosing firms may report on how they mitigate cyber risk. Examples include investments in IT, investment in staff training, benchmarking and industry best practices, cyber insurance, dedicated cyber security teams, working with external experts, preparedness tests and simulations, disaster and continuity plans, and outlining cyber security frameworks, policies, and procedures. A comprehensive example comes from TransUnion's 2018 10K, which states *"We have a written information security program based on the ISO/IEC 27001:2013 standard with dedicated personnel charged with overseeing that program"*, and *"safeguards include firewalls, intrusion protection and monitoring, anti-virus and malware protection, vulnerability threat analysis, management and testing, advanced persistent threat monitoring, forensic tools, encryption technologies, data transmission standards, contractual provisions, customer credentialing, identity and access management, data loss, access and anomaly reports and training programs for associates. We… share cyber threat and attack information through our participation in the Financial Information Sharing and Analysis Council ("FS-ISAC") … We undergo SSAE 16 reviews annually, and several of our major customers routinely audit our security controls. We conduct an annual Payment Card Industry Data Security Standard (PCI-DSS) compliance program and remain PCI certified. Additionally, we also hire third parties to conduct independent information security assessments"*.

TABLE 3: CYBER EVENT DISCLOSURE

This table illustrates disclosure topics around the cyber events in three groups: 1) Equifax breach in 2017 with peer firms Experian and TransUnion; 2) Bank of Montreal (BoM) and a subsidiary of the Canadian Imperial Bank of Commerce (CIBC) breach in 2018 with peer firms Bank of Novia Scotia (BoNS), Royal Bank of Canada (RBC), and Toronto-Dominion Bank (TDB); and 3) Marriott breach in 2018 with peer firms Hilton, Hyatt, and Wyndham. The names of breach firms are bolded, and those of peer firms selected are non-bolded. If a firm discloses corresponding information in its 10-K in a year, we indicate it as "Yes". Otherwise, it is indicated as "No".

| | | **Credit rating agencies** | | | | | | **Canadian big 5 banks** | | | | | | | | | | **US hotel companies** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **Equifax** | | Experian | | TransUnion | | **BoM** | | **CIBC** | | BoNS | | RBC | | TDB | | **Marriott** | | Hilton | | Hyatt | | Wyndham | |
| | | 2016 | 2018 | 2016 | 2018 | 2016 | 2018 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2020 | 2017 | 2019 | 2017 | 2019 | 2017 | 2019 | 2017 | 2019 |
| **Cyber risks description** | Cyber security risk | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Privacy issue | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | No | No | No | No | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Third parties | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Changing regulations | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No | No | Yes | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Potential perpetrators | No | No | No | No | Yes | Yes | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No | No | No | No | No | No |
| **Cyber risks identified** | Human error | Yes | Yes | No | No | Yes | Yes | No | No | No | No | No | Yes | No | No | No | No | Yes | Yes | No | No | Yes | Yes | Yes | Yes |
| | Hacking/breach etc | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Virus/malware/ransomware | Yes | Yes | No | No | Yes | Yes | No | No | Yes | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| | Phishing | No | Yes | No | No | No | No | No | Yes | No | No | No | No | No | No | Yes | Yes | No | Yes | No | No | No | No | No | No |
| | Denial of service attack | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No | No | Yes | Yes | No | No | No | No | No | No | No | No |
| | Disclosure of private information | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **Potential impacts identified** | Financial | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Operational | No | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Reputation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Legal/fines etc | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| | Increased security costs | No | Yes | No | No | No | No | No | No | No | No | No | No | No | No | Yes | Yes | No | Yes | No | No | No | No | No | No |
| | Remedial costs | No | Yes | No | No | No | No | No | No | No | No | No | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| **Cyber risks mitigation** | IT investment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No | No | No | No | No | No | No | No | No | No | Yes | Yes | No | No |
| | Insurance | Yes | Yes | Yes | Yes | No | No | No | No | Yes | Yes | Yes | Yes | No | No | No | Yes | Yes | Yes | No | No | Yes | Yes | Yes | No |
| | Staff training | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | No | No | No | No | Yes | No | No | No | No | No | No | No | No | No | No |
| | Policies | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes |
| | Benchmarking | No | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes | No | No | Yes | No | No | No | No | No | No | No | No |
| | Dedicated teams | No | No | No | Yes | Yes | Yes | No | Yes | No | No | No | Yes | No | Yes | No | Yes | No | No | No | No | No | No | No | No |
| | Simulation/preparedness tests | No | No | No | No | Yes | Yes | No | No | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | No | No | No | No | No | No | No | No |
| | Recovery/continuity plans | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | No | Yes | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No | No |
| | Work with third parties | No | No | No | No | Yes | Yes | Yes | Yes | No | No | No | No | Yes | Yes | No | No | No | No | No | No | No | No | No | No |

TABLE 4: CYBER DISCLOSURE SCORES

This table shows the scores in each disclosure dimension illustrated in Table 2. If a firm discloses information on two aspects in a dimension, it receives a score of 2. The colours represent score rank from dark green (best) to red (worst). The names of breach firms are bolded, and those of peer firms selected are non-bolded. Note that the Canadian Big 5 Banks comprise the Bank of Montreal (BoM), Canadian Imperial Bank of Commerce (CIBC), Bank of Nova Scotia (BoNS), Royal Bank of Canada (RBC), and Toronto-Dominion Bank (TDB). The colours represent score rank from dark green (best) to red (worst).

| | **Credit rating agencies** | | | | | | **Canadian big 5 banks** | | | | | | | | | | **US hotel companies** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Equifax** | | Experian | | TransUnion | | **BoM** | | **CIBC** | | BoNS | | RBC | | TDB | | **Marriott** | | Hilton | | Hyatt | | Wyndham | |
| | **2016** | **2018** | **2016** | **2018** | **2016** | **2018** | **2017** | **2020** | **2017** | **2020** | **2017** | **2020** | **2017** | **2020** | **2017** | **2020** | **2017** | **2019** | **2017** | **2019** | **2017** | **2019** | **2017** | **2019** |
| Cyber risks description | 4 | 4 | 4 | 4 | 5 | 5 | 2 | 3 | 1 | 1 | 3 | 3 | 1 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| Cyber risks identified | 5 | 6 | 1 | 1 | 5 | 5 | 2 | 4 | 3 | 4 | 2 | 3 | 2 | 2 | 5 | 5 | 4 | 5 | 3 | 3 | 3 | 4 | 4 | 4 |
| Potential impacts identified | 3 | 5 | 3 | 3 | 4 | 4 | 2 | 2 | 3 | 3 | 4 | 3 | 3 | 4 | 5 | 5 | 5 | 6 | 5 | 5 | 5 | 5 | 4 | 4 |
| Cyber risks mitigation | 4 | 4 | 4 | 6 | 8 | 8 | 5 | 7 | 4 | 5 | 3 | 4 | 3 | 5 | 2 | 5 | 1 | 2 | 1 | 1 | 3 | 3 | 2 | 1 |
| **Total score** | 16 | 19 | 12 | 14 | 22 | 22 | 11 | 16 | 11 | 13 | 12 | 13 | 9 | 14 | 15 | 18 | 14 | 17 | 13 | 13 | 15 | 16 | 14 | 13 |

TABLE 5: AVERAGE CYBER DISCLOSURE SCORES

The table compares the average scores shown in Table 3 in each industry calculated using the breach and peer firms only shown in Table 3. The values are calculated as an average of the scores in all the selected firms in the pre- and post-event years. The colours represent score rank from dark green (best) to red (worst).

| | **Credit rating agencies** | **Canadian big 5 banks** | **US hotel companies** |
|---|---|---|---|
| Cyber risks description | 4.33 | 2.30 | 4.00 |
| Cyber risks identified | 3.83 | 3.20 | 3.75 |
| Potential impacts identified | 3.67 | 3.40 | 4.88 |
| Cyber risks mitigation | 5.67 | 4.30 | 1.75 |
| **Total score** | 17.50 | 13.20 | 14.38 |

### 3.2 FINDING INFORMATION IN DISCLOSURES

Section 3, thus far, has produced little if any evidence that cyber disclosure is informative or associated with superior cyber governance. Two recent studies suggest possible solutions to the disclosure conundrum that offer hope.

Florakis et al. (2020) also exploit cyber security disclosures in corporate filings, but develop a firm-level measure of cyber risk using textual analysis. This measure predicts future cyber attacks, suggesting that there is informational value in the cyber risk disclosures. The researchers also provide evidence that stocks with higher cyber risk, according to this measure, perform poorly when there is heightened concern about cyber risk in the market. Over time, higher cyber risk stocks earn a higher return than their lower cyber risk peers, to compensate for this risk.

Jamilov et al. (2021) also employ textual analysis but focus on quarterly earnings calls. Regulatory filings are carefully prepared, checked by multiple parties, and likely to be subject to impression management. Earnings calls, in particular the Q&A component, are less exposed to stage management and therefore potentially offer richer insights. With quarterly frequency, they also provide more timely updates. This team also provides evidence that their cyber risk measure predicts future cyber attacks. Some evidence is provided about the firms that are at higher risk. Typically such firms are larger and older, have lots of liquidity, and have a high ratio of intangible assets. The IT and services sectors are particularly vulnerable, followed by the financial sector. Jamilov et al. (2021) also confirm that high cyber risk stocks earn a higher return to compensate for the additional risk.

## 4. BOARD STRUCTURES/COMMITTEES AND CYBER RISK

In the field of risk governance, researchers have found that certain structures improve risk outcomes. The strength and independence of the risk management function are important (Aebi et al., 2012; Ellul & Yerramilli, 2013; Magee et al., 2019). The presence of an active board risk committee, along with the experience of its members, also help to improve risk outcomes (Ellul & Yerramilli, 2013; Magee et al., 2019).

The effectiveness of governance structures in relation to cyber risk outcomes is not yet well understood. Very few papers have been published in this area and those that exist are quite recent. Kamiya et al. (2021) find that the existence of a board risk committee reduces the likelihood of an attack, although Akey et al. (2021) find no such association. Boards that are larger and have less financial expertise are associated with more data breaches, but independence, entrenchment, and busyness of the board are not (Lending et al., 2018).

According to Haislip et al. (2016), audit IT expertise helps to reduce weakness in IT controls. The potential role of auditors for reducing cyber incidents is also supported by Li et al. (2020) who find that firms pay higher audit fees after an incident but this then reduces the likelihood of subsequent incidents.

There is, however, evidence to suggest that reported risk governance is enhanced following a cyber attack. Risk governance is also enhanced following cyber attacks in peer firms, and the effect is greater for non-breached firms with more independent boards and those with cyber expertise on the board (Ashraf, 2021). The effect is also greater for more catastrophic breaches and those that emanate from an external actor.

Lending et al. (2018) find that after a data breach, changes often occur on the board: board size is reduced but the proportion of independent directors rises, while the entrenchment index falls and the busyness index rises. This suggests that longstanding directors are replaced with those considered to have more cyber expertise, and that this expertise is in short supply. The same study supports increased chance of CEO and Chief Technology Officer (CTO) turnover following a breach.

Kamiya et al. (2021) outline a model to explain why a firm might change its cyber risk governance following a cyber security breach. In the model, firms are assumed to evaluate cyber security risk as they would any other operational risk by estimating both the probability of a cyber security breach occurring and the potential loss once the cyber security breach has occurred. A firm's optimum level of cyber risk governance is then determined by weighing up the potential costs of a cyber security breach, which includes remediation, litigation, and reputational costs against the cost of implementing cyber risk governance measures. A successful cyber security breach, they argue, will only cause a firm to rethink its cyber security governance if it is severe enough to alter the firm's perceptions about the probability and scale of future cyber security breaches. As a result, we would expect to see more significant cyber risk governance changes associated with larger cyber security breaches.

Table 6 shows cyber risk governance information for our four case study firms that suffered cyber security breaches - Equifax, Bank of Montreal, CIBC, and Marriott - for the year before and after the cyber security breach. It is interesting to compare the pre-attack governance structures of the Canadian banks with the two firms that suffered much more severe cyber attacks: Equifax and Marriott. Pre-attack, the Canadian banks had less entrenched, and more diverse boards that met more often, especially in relation to cyber security. Both boards were receiving cyber security education. They had more than 90% independent directors and an independent chair as well as a board risk committee. Prior to the attack, only one of our case study firms listed cyber security as a director skill (Bank of Montreal). Only one had a CRO (Chief Risk Officer)/CTO or CISO as a named executive in relation to remuneration (also Bank of Montreal). The named executives are the top five most highly paid executives in the institution, which may be a proxy for status within the executive hierarchy.

It is interesting to consider the accuracy of reporting of director skills. In Table 6 the number of directors with cyber security skill is taken from the director skills matrix in the proxy statement/proxy information circular. In the case of The Bank of Montreal, the bank claims to have had five directors with cyber security skill prior to the breach but there is clearly some degree of subjectivity in this determination. It would be interesting to properly investigate the accuracy of the reported skills matrices.

We observe a few changes to reported board governance following the attacks. In our small sample size however, we only find limited support for Lending et al. (2018) that board size is reduced, and board entrenchment falls post cyber security breach. Equifax and CIBC both reduced their board size post cyber security breach, and the average director tenure fell for Equifax and Marriott. We also do not see any evidence that boards become more independent post breach, although independence was already at high levels. The two companies with the most significant cyber security breaches, Equifax and Marriott, increased their board gender diversity, which, according to Radu and Smaili (2021) may in turn be associated with expanded cyber security disclosure. In the case of Equifax, Heather H. Wilson (who has a technology background) was added to the board, and in the case of Marriott, Margaret M. McCarthy (a director with extensive experience in technology and cyber security) was added to the to the board.

Table 6 shows that Equifax made some significant changes to its cyber risk governance post breach. First, they separated the roles of CEO and the chair of the board. Second, the board was more active in the year after the breach, meeting 18 times compared to 6 times the year before the breach. Third, the responsibility for cyber security was extended to both the audit committee and the technology committee, having previously only been the responsibility of the technology committee. As a result, committees concerned with cyber security met 16 times in the year following the breach compared to just 4 times in the year before the breach. Fourth, cyber security expertise became a director skill actively sought by the board. Fifth, the firm disclosed for the first time that directors were engaged in cyber security education. Finally, Equifax hired both a Chief Information Security Officer (CISO) and a Chief Technological Officer (CTO). Both were among Equifax's named executive officers. The firm also disclosed that both the CISO and CTO, along with the internal audit department, must now meet regularly with the technology committee.

After the cyber security breach, Marriott delegated the audit committee with responsibility for the oversight of the company's cyber security and data privacy practices. The audit committee met 11 times during the year. The company also made several changes to its directors and executives. Margaret McCarthy was appointed to the board and her experience includes information security, data privacy, and technology. Marriott also hired a new Chief Information Security Officer who joined the executive committee. The Executive Vice President and Global Chief Commercial Officer was promoted to Group President of Consumer Operations, Technology, and Emerging Businesses.

In the year after the breach, the Bank of Montreal stated that the full board has responsibility for strategic planning related to cyber security. At the committee level, responsibility was extended to both the audit committee and the risk management committee, while the governance and nominating committee continued to have responsibility for director cyber security education. There were 19 meetings of committees with responsibility for cyber security, up from 11 the year before the cyber security breach when only the audit committee had responsibility for cyber security. Six months after the cyber security breach, the Bank of Montreal also replaced their Chief Technology and Operations Officer. The only significant change for CIBC was that their Chief Risk Officer (CRO) became a named executive.

In conclusion, we find some evidence to support the findings of Kamiya et al. (2021) that firms are more likely to change their cyber risk governance in the aftermath of a significant cyber security breach that causes the firm to rethink either the probability or scale of future cyber security breaches. The observed changes in risk governance following an attack suggest that either boards and directors believe that the changes will improve future cyber outcomes, or they are attempting to upgrade the litigation shield against possible shareholder suits, if not both. There is also a general uptrend in cyber governance as organisations respond to the heightened risk environment. Klemash et al. (2020) examine Fortune 100 companies, and find that more companies are disclosing director qualifications in the area of cyber security over time. The number including cyber security as an area of expertise sought or included in a director biography reached 58% in 2020, compared with only 39% in 2018.

TABLE 6: CHANGES IN CYBER GOVERNANCE FOLLOWING BREACH

This table presents key changes in cyber governance following breaches in our four case studies: Equifax, Bank of Montreal (BoM), Canadian Imperial Bank of Commerce (CIBC), and Marriott. The table shows the state of reported cyber governance in the year before and the year after the cyber events. In the case of Equifax and Marriott the information is sourced from Proxy Statements and Annual Reports. In the case of the Canadian Banks the information is sourced form Proxy Information Circulars, Annual Information Forms and Annual Reports.

| | Equifax | | BoM | | CIBC | | Marriott | |
|---|---|---|---|---|---|---|---|---|
| | **Pre** | **Post** | **Pre** | **Post** | **Pre** | **Post** | **Pre** | **Post** |
| % independent directors on board | 91.67% | 90.00% | 92.31% | 93.33% | 94.12% | 93.33% | 78.57% | 79.00% |
| Board size | 12 | 10 | 13 | 15 | 17 | 15 | 14 | 14 |
| % Female directors on board | 16.67% | 30.00% | 30.77% | 33.33% | 41.18% | 46.67% | 28.57% | 35.71% |
| Number of board meetings per annum | 6 | 18 | 10 | 10 | 11 | 10 | 4 | 4 |
| Independent chair | No | Yes | Yes | Yes | Yes | Yes | No | No |
| Average tenure of all directors in years | 9.5 | 4.96 | 7.38 | 8.3 | 6.9 | 8 | 12 | 11 |
| Cyber security mentioned as board responsibility in disclosures | Yes | Yes | No | Yes | No | No | Yes | Yes |
| Cyber security mentioned in report of audit committee | No | Yes | Yes | Yes | No | No | No | Yes |
| Cyber security mentioned in report of risk committee | No | No | No | Yes | Yes | Yes | No | No |
| Cyber security mentioned in report of governance committee | No | No | Yes | Yes | No | No | No | No |
| Cyber security mentioned in report of technology committee | Yes | Yes | No | No | No | No | No | No |
| Number of meetings of committees whose reports mention for cyber security | 4 | 16 | 11 | 19 | 11 | 7 | 0 | 11 |
| Existence of a board committee with risk in the name | No | No | Yes | Yes | Yes | Yes | No | No |
| IT listed as director skill in skills matrix | Yes | Yes | Yes* | Yes* | Yes | Yes | No | No |
| Number of directors with IT skill (self-reported in skills matrix) | 5 | 6 | 5* | 9* | 6 | 6 | 0 | 1† |
| Cyber security listed as director skill in skills matrix | No | Yes | Yes* | Yes* | No | No | No | No |
| Number of directors with cyber security skill (self-reported in skills matrix) | 0 | 6 | 5* | 9* | 0 | 0 | 0 | 1† |
| Board cyber education provided | No | Yes | Yes | Yes | Yes | Yes | No | No |
| CISO/CTO/CRO member of the executive | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| CISO/CTO/CRO named executive in relation to remuneration | No | Yes | Yes | No | No | Yes | No | Yes |

*The Bank of Montreal only reports director skills for non-employee directors.

†Marriott does not include IT or cyber security in its director skills matrix; however both are listed as skills in the director bio of Margaret M. McCarthy.

## 5. EXECUTIVE COMPENSATION AND CYBER RISK

Executive compensation is a crucial element in risk governance to ensure that executives are incentivised to take an appropriate amount of risk from the perspective of shareholders. A major cyber attack with significant adverse consequences for customers and shareholders is likely to be outside of the risk appetite for the majority of organisations. Therefore, compensation design should avoid any unintended encouragement of short-termism. Rather, compensation design should support executives in making costly investments in cyber controls, despite the adverse impact on earnings. Such short-term costs are important to prevent poor outcomes that may occur in the medium to longer-term.

As risk outcomes take time to become apparent, deferred compensation is one of the most important tools for promoting prudent risk management. Within this broad category are the following elements:

- Deferred cash, which will 'vest' to the executive on a future date. These cash awards can be subject to 'malus' clauses that allow the firm to withdraw or reduce the payment under certain conditions. This can include poor risk outcomes that should have been anticipated and prevented, and this is a feature of some of the new executive accountability regimes being used in the financial services sector.[9] In reality, the malus clauses usually relate only to fraud or serious misconduct.
- Restricted shares, which will 'vest' to the executive on a future date. Again, malus clauses can apply. Restricted shares are particularly effective for addressing risk since poor risk outcomes will be reflected in the share price. For example, the share price is likely to fall after a disastrous cyber attack and the executive's reward on vesting is therefore automatically adjusted in line with other shareholders.
- Restricted options, which will 'vest' to the executive on a future date. These are associated with greater executive risk-taking as discussed in Sheedy (2021) Chapter 4.

Clawback clauses are another possible avenue for promoting prudent risk-taking. Whereas malus clauses relate to payments that have been awarded but not yet paid, clawback clauses apply to payments after they have been paid. Similarly, they are usually used only for cases of fraud and extreme negligence, although they could be extended to include poor risk outcomes.

Any discussion of deferred compensation is incomplete without mentioning the length of the deferral period. Recent research suggests that longer deferrals discourage short-term behaviour by executives and better risk management (Gopalan et al., 2014; Kolasinski & Yang, 2018).

Aside from these questions of compensation design, it is important to consider how boards impose accountability on the executive through remuneration and other outcomes. What are the remuneration consequences following a badly managed cyber attack? The more that executives anticipate significant consequences for poor outcomes, the more likely it is that they will adopt effective risk management practices (eg, investing in cyber controls). New executive accountability regimes in the UK, Australia, and elsewhere indicate that greater accountability is leading to improved risk management practices and risk culture (Sheedy & Canestrari-Soh, 2020).

Executive termination is the most extreme response, along with the cancellation of benefits that would normally be made to 'good leavers'. There is increasing disquiet among shareholders and the broader community concerning termination payments that appear excessive, in circumstances that reflect careless management of risks that were foreseeable. These days there is little excuse for being unaware of cyber risk as a threat to almost all businesses. An example of this is the payment of bonuses to the Equifax CEO who departed shortly after the major 2017 data hack[10].

Less extreme, but still significant consequences would include cancellation of variable remuneration following a cyber event (eg, bonus payments and new share/option awards). Another possibility would be reduction in base pay.

Kamiya et al. (2021) find that CEO termination is quite rare following a cyber attack. Attacked firms typically respond to cyber attacks by reducing CEO bonuses as a proportion of total pay. The total amount of equity-based pay typically remains constant after an attack but the mix changes. In order to reduce risk-taking incentives for executives, the use of options is often reduced in favour of restricted shares. This suggests that following a cyber attack, boards belatedly reassess the vulnerability of the firm to cyber risk and adjust compensation settings to encourage better cyber risk management.

9 For more information about the Banking Executive Accountability Regime and other similar approaches, see Sheedy and Canestrari-Soh (2021).

10 Refer to the CBS News report for more details at https://www.cbsnews.com/news/equifax-data-breach-settlement-disgraced-former-ceo-getting-nearly-20-million-in-bonuses-after-the-hack/

### 5.1 EQUIFAX REMUNERATION (2016-2020)

Figure 4 shows the remuneration for the five most highly paid executives at Equifax from 2016 to 2020. In company disclosures, these are known as the 'named' executives. Short-term cash incentives (bonuses) were cut in 2017 (the year of the cyber event), but the total compensation increased because of an increase in deferred incentives (shares and options) and an increase in executive pension plans. Most controversially, this included $6.5 million in restricted shares, $1.3 million in options, and a $6.5 million change in pension plan for 'retiring' CEO and Chairman Richard F. Smith. The increase in total remuneration in 2018 in is also explained by the awarding of significant parcels of restricted shares and options to new executives. The spike in compensation levels post cyber event therefore reflects another cost to shareholders from such events.

Figure 4 shows that the reward structure in 2020 was broadly similar to that in 2016, both in quantum and mix. A difficulty in comparing the remuneration over time is that the composition of named executives changes at Equifax. Figure 5 shows the compensation for the two executives who remained throughout 2016-20 at Equifax: the CFO and the President of Workforce Solutions. It shows that short-term cash incentives fell to zero in 2017, but this was offset to a significant extent by an increase in deferred remuneration (restricted shares and options as well as pension plan entitlements). That is, the extent of executive accountability was limited. It's intriguing to note that allocation of options, which encourage greater executive risk-taking, increased following the cyber attack. For these two executives, total remuneration exceeded its 2016 levels in 2018, 2019, and 2020 (adjusted for inflation). In 2018 and 2019 there was a significant increase in awards of both restricted shares and options relative to 2016 levels, with short-term cash incentives also gradually recovering.

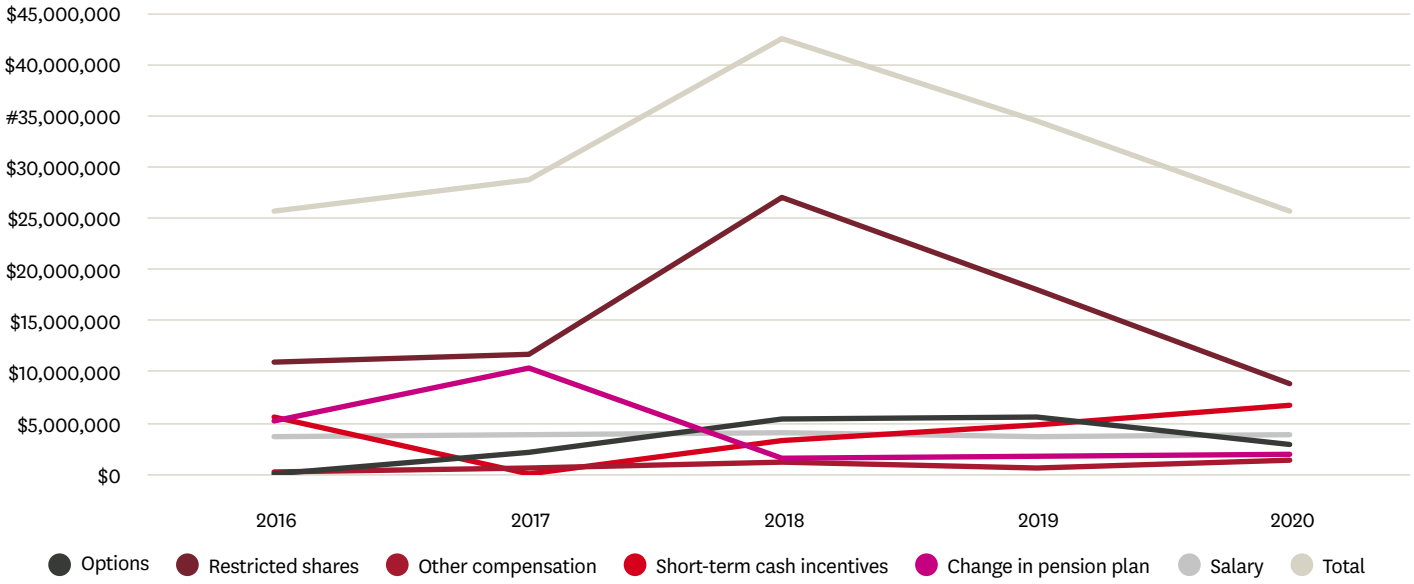


FIGURE 4. EXECUTIVE COMPENSATION AT EQUIFAX 2016-20

This figure shows the executive compensation at Equifax from 2016-20. Compensation figures are sourced form S&P Capital IQ. Salary refers to base salary earned during the year. Short-term cash incentives refer to any bonuses and non-equity incentives earned during the year. Other compensation refers to perquisites and benefits. Restricted shares refer to new grants of restricted shares awarded during the year. Options refer to new grants of restricted options during the year. Change in pension plan refers to changes to accumulated pension benefit accruals for the executives or changes in non-qualified deferred comp earnings.[11] Compensation is adjusted for inflation with 2016 as the base year. In the case of an executive being replaced mid-year, the compensation of both the old and new executive are included.

11 Non-qualified deferred comp earnings refer to compensation that has been earned by an employee but not yet received from the employer. It is therefore not included in taxable income.

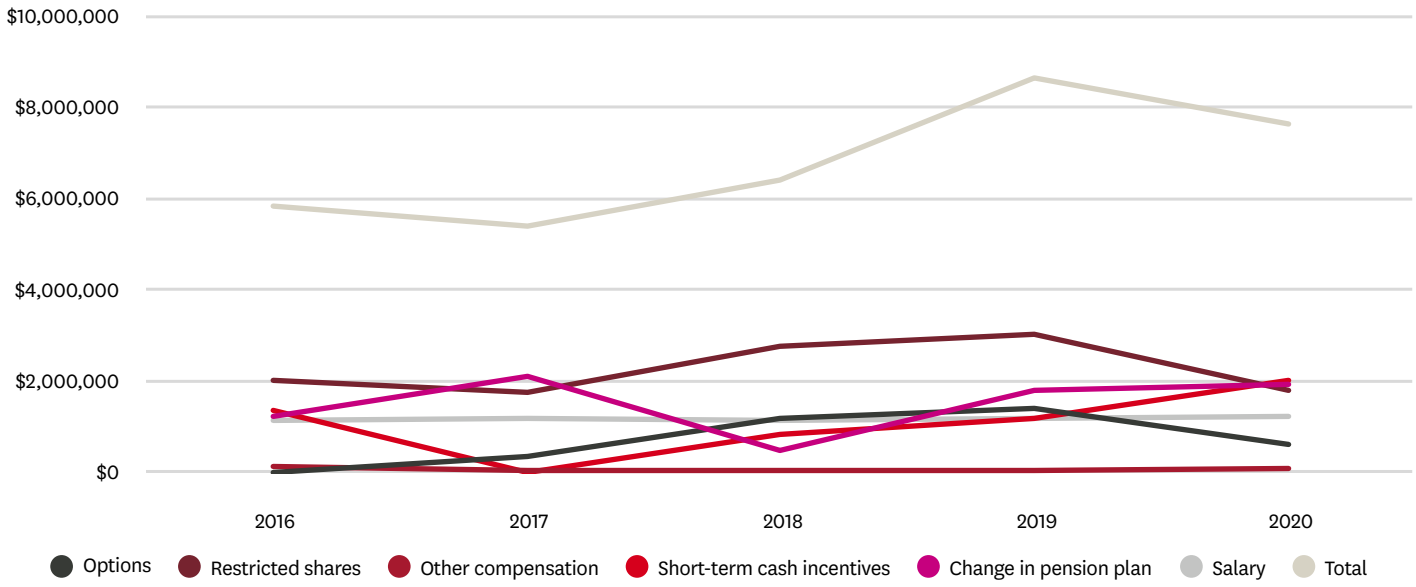


FIGURE 5. EVER PRESENT EXECUTIVE COMPENSATION AT EQUIFAX 2016-20

This figure shows the executive compensation at Equifax from 2016-20 for the two ever present executives over the period (CFO, John Gamble and President of Workforce Solutions Rodolfo Ploder). Compensation figures are sourced from S&P Capital IQ. Salary refers to base salary earned during the year. Short-term cash incentives refer to any bonuses and other non-equity incentives earned during the year. Other compensation refers to perquisites and benefits. Restricted shares refer to new grants of restricted shares during the year. Options refer to new grants of restricted options during the year. Change in pension plan refers to changes to accumulated pension benefit accruals for the executives or changes in non-qualified deferred comp earnings.[11] Compensation is adjusted for inflation with 2016 as the base year.

### 5.2 MARRIOTT REMUNERATION (2017-19)

Figure 6a shows the breakdown of pay at Marriott from 2017 to 2019 for the five most highly paid executives. These named executives remained constant throughout the period in question. In the aftermath of the cyber security event in 2018, Marriott's short-term incentive pay was down from nearly 32% of total pay to 21%. It remained at 21% in 2019. The CEO lost out on a $1 million dollar bonus in 2018 and 2019 as compared to 2017. The other named executives lost $500,000. Total executive pay was reduced slightly, however, due to a compensating increase in restricted shares and options. Overall, the adverse consequences for executives were marginal following the cyber attack.

Compared to Hilton (Figure 6b), Marriott paid out a higher percentage of executive compensation in the form of salary and short-term incentives throughout this period. Salary made up around 13% of the executive compensation at Marriott and only 9-12% at Hilton. Short-term bonuses at Hilton comprised 16-17% of executive compensation but short-term bonuses were 32% of the total at Marriott in 2017, although this falls to around 21% in 2018 and 2019. A major difference between Marriott and Hilton is that deferred pay made up a much larger share of the compensation package at Hilton. Deferred pay was between 70% and 74% at Hilton but only between 54% and 63% at Marriott.

Not only was deferred pay less substantial at Marriott than Hilton, but prior to the cyber event the composition of the pay was more heavily weighted to options at Marriott (15% versus 9%). Options have been linked to increased risk taking, as outlined in Sheedy (2021) Chapter 4. Interestingly, both firms increased the allocation of options in 2018 and 2019 to over 17%. This is contrary to the findings of Kamiya et al. (2021) that a reduction in the granting of options following a major cyber event is typical.

Clawback provisions were in place at Marriott but these related only to serious misconduct, fraud, and tortious conduct that is injurious to the company or if the executive engages in competition with the company.

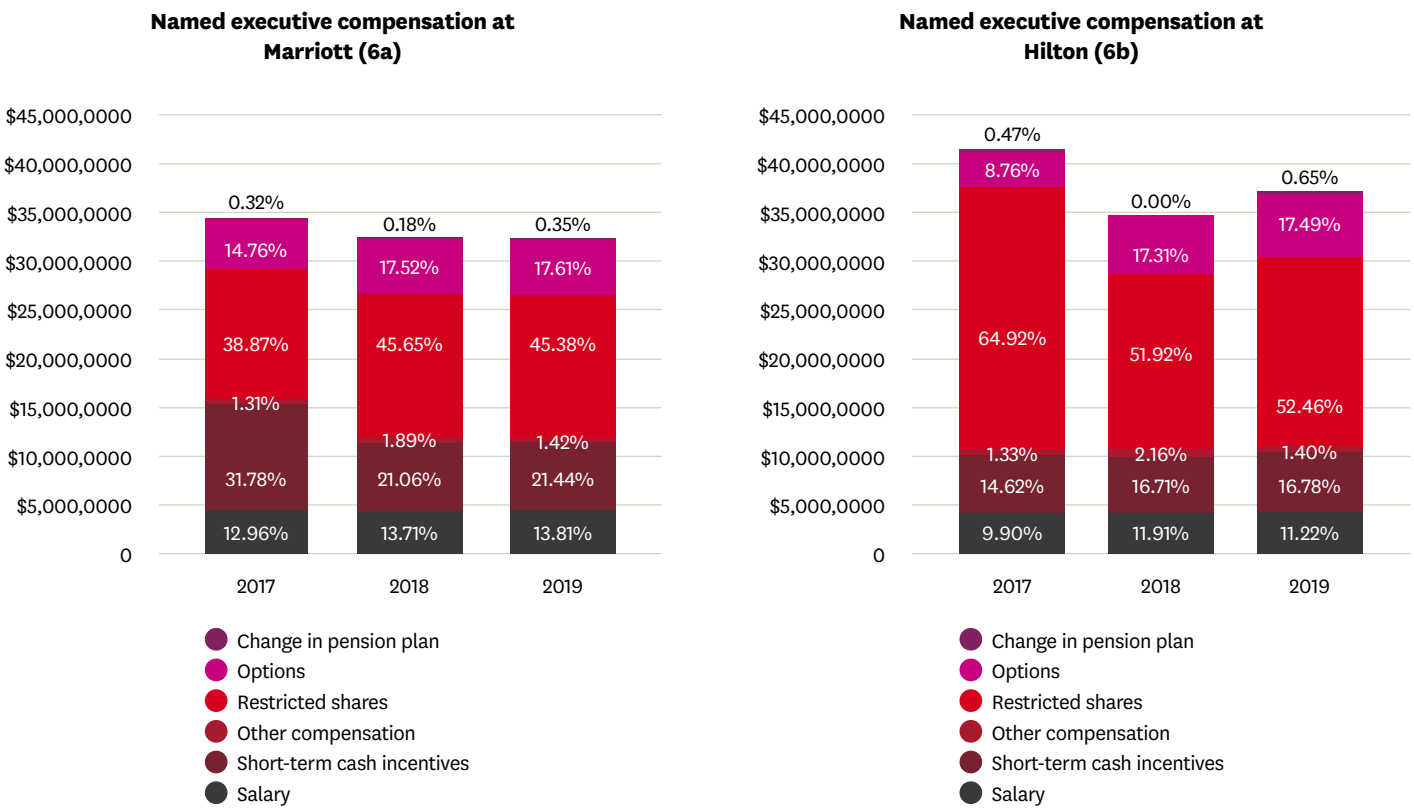


FIGURE 6. NAMED EXECUTIVE COMPENSATION AT MARRIOTT (6A) AND HILTON (6B) FROM 2017-19
Compensation figures are sourced from S&P Capital IQ. Salary refers to base salary earned during the year. Short-term cash incentives refer to any bonuses and other non-equity incentives earned during the year. Other compensation refers to perquisites and benefits. Restricted shares refer to new grants of restricted shares. Options refer to restricted share options awarded during the year. Change in pension plan refers to changes to accumulated pension benefit accruals for the executives or changes in non-qualified deferred comp earnings.[12]

Further research is needed in the area of executive compensation and how it relates to cyber risk management. However, the evidence to date suggests that there are opportunities to improve cyber governance through better executive compensation choices by boards as follows:

- Greater use of certain forms of deferred remuneration (restricted shares and deferred cash) relative to short-term incentives and restricted options;
- Longer vesting periods for restricted shares and deferred cash;
- Greater use of malus and clawback clauses to reflect poor risk management outcomes as opposed to just fraud and serious misconduct; and
- Enhanced executive accountability, that is, more severe consequences for executives after serious cyber events, such as termination with loss of benefits and more significant reductions in variable rewards (cash and share awards).

12 Non-qualified deferred comp earnings refers to compensation that has been earned by an employee but not yet received from the employer. It is therefore not included in taxable income.

## 6. CYBER SECURITY GOVERNANCE SCORES

Environmental, Social, and Governance (ESG) ratings are an increasingly important consideration for investors, with many now seeing ESG issues as material for financial outcomes. A number of organisations provide ESG ratings and within the category of governance more broadly, some providers aim to quantify the quality of a firm's cyber security governance. For the investors who subscribe to these ratings, it's important to consider whether they provide a valid indication of the firm's true cyber security governance status.

In this section, we look at one of these attempts, Standard and Poor's (S&P) cyber security governance metrics. We examine S&P because the scores were available to the research team through an existing subscription. The S&P offering draws on the firm's 2019 purchase of the ESG business of RobecoSAM, including its well-known Corporate Sustainability Assessment (CSA). A 'rate the raters' report by Sustainability (Sustainability, 2020) states that no single provider is favoured by investors, but the RobecoSAM CSA is one of the five most highly regarded.

### 6.1 CYBER SECURITY GOVERNANCE SCORE METHODOLOGY

S&P has included a cyber security governance score in its S&P Capital IQ platform since 2016 for banks and since 2019 for other industries. The methodology as at 2021 is explained in the CSA Companion (S&P, 2021). The cyber security governance score is comprised of four separate dimensions of cyber security governance and an overall score. Starting from 2020, a fifth dimension "IT infrastructure incidents" was added for banks.

The scores are derived from questionnaires completed by the companies being rated, but the company responses are not publicly available. The algorithm for translating the company responses to scores is also not provided. Companies are asked to provide supporting evidence for certain questions. In many cases the evidence can be based on internal, unaudited documents, creating obvious opportunities for impression management. The other problem with the methodology is the possibility that companies may not complete the questionnaire, thus limiting the universe of companies that receive a score. The five dimensions considered in the cyber security governance score are as follows:

#### CYBER SECURITY BREACHES

The cyber security breach dimension has two components. First, the questionnaire asks for details of cyber loss events in each of the past three years, including number of affected customers and fines/penalties paid. Second, the questionnaire asks for information on the firm's use of cyber risk insurance.

#### CYBER SECURITY GOVERNANCE

The cyber security governance dimension assesses the skills and experience of a firm's board members and its executives who have responsibility for the firm's cyber security strategy and review process.

#### PROCESS AND INFRASTRUCTURE

The process and infrastructure dimension assesses the process a firm has in place to prevent and manage potential cyber security events.

#### SECURITY MEASURES

The security measures dimension assesses the policies and procedures a firm has in place to make employees aware of cyber security risks.

#### IT INFRASTRUCTURE INCIDENTS

The IT infrastructure incidents dimension was introduced in 2020 for banks. It assesses whether banks measure the costs associated with IT infrastructure events which they had to pay penalties for or suffered revenue losses from.

Using the banking industry as an example, Table 7 shows the total cyber security governance scores for the twenty largest banks by total assets from the US, UK, Canada, and Australia from 2016 to 2020. The range of scores is striking in what one would expect to be a relatively homogeneous group. In the period 2016-20, only four banks, namely the Royal Bank of Canada, the Bank of Montreal, Toronto-Dominion Bank, and the Bank of America, improved their cyber security governance scores. This is also surprising, as one would have expected an upward trend in cyber security governance through this period. It is possible that the general downtrend could be caused by changes in methodology by the ESG rating provider. This may have occurred in 2019 when S&P purchased the ESG business of RobecomSAM. With the exception of Citi Group, the average cyber security governance scores are higher in Canada and Australia and lower in the US and UK.

TABLE 7: CYBER SECURITY SCORES FOR THE 20 LARGEST BANKS IN THE US, UK, CANADA, AND AUSTRALIA
The table contains the S&P cyber security governance scores for the twenty largest banks by total assets from the US, UK, Canada, and Australia, from 2016 to 2020. The score is the overall S&P cyber security governance score, comprising the individual dimensions outlined in Section 6.1.

| Bank | Total assets (M) | Country | 2016 | 2017 | 2018 | 2019 | 2020 | Average |
|---|---|---|---|---|---|---|---|---|
| Royal Bank of Canada | 1116.31 | Canada | 87 | 87 | 87 | 100 | 97 | 91.6 |
| Westpac Banking Corporation | 611.47 | Australia | 94 | 94 | 99 | 77 | 76 | 88 |
| Citigroup Inc | 1951.16 | US | 94 | 94 | 99 | 62 | 87 | 87.2 |
| Canadian Imperial Bank of Commerce (CIBC) | 495.99 | Canada | 88 | 90 | 93 | 84 | 70 | 85 |
| Bank of Montreal | 665.2 | Canada | 86 | 99 | 75 | 66 | 94 | 84 |
| National Australia Bank | 571.34 | Australia | 87 | 88 | 88 | 89 | 68 | 84 |
| Toronto Dominion Bank | 1102.04 | Canada | 69 | 83 | 84 | 87 | 88 | 82.2 |
| Australian and New Zealand Banking Group (ANZ) | 661.72 | Australia | 87 | 88 | 87 | 57 | 81 | 80 |
| Commonwealth Bank of Australia (CBA) | 688.4 | Australia | 96 | 99 | 87 | 47 | 65 | 78.8 |
| Bank of Nova Scotia | 872.62 | Canada | 74 | 75 | 87 | 75 | 68 | 75.8 |
| Bank of America Corporation | 2818.15 | US | 68 | 89 | 91 | 44 | 73 | 73 |
| Barclays Bank PLC | 1510.14 | UK | 79 | 76 | 76 | 57 | 60 | 69.6 |
| NatWest Group plc | 957.6 | UK | 83 | 76 | 84 | 57 | 4 | 60.8 |
| Standard Chartered | 720.4 | UK | 62 | 74 | 76 | 42 | 39 | 58.6 |
| Goldman Sachs Group, Inc. | 992.97 | US | 57 | 54 | 59 | 16 | 30 | 43.2 |
| Lloyds Banking Group plc | 1104.42 | UK | 57 | 57 | 44 | 6 | 6 | 34 |
| Morgan Stanley | 895.43 | US | 42 | 42 | 40 | 4 | 35 | 32.6 |
| Wells Fargo & Company | 1927.26 | US | 50 | 40 | 40 | 4 | 12 | 29.2 |
| JPMorgan Chase & Co | 3386.07 | US | 25 | 25 | 45 | 17 | 20 | 26.4 |
| HSBC Holdings plc | 2984.16 | UK | 34 | 22 | 22 | 4 | 4 | 17.2 |

### 6.2 THE PREDICTIVE POWER OF CYBER SECURITY GOVERNANCE SCORES

Cyber security governance scores are useful if they can identify cyber governance characteristics that are associated with future cyber security outcomes. Investors can trade based on the scores to earn positive abnormal returns by longing firms with higher scores and shorting firms with lower scores.

Table 8 shows the correlations among the cyber security governance scores of the 20 largest banks in 2016 and future and past cyber events. Future and past cyber events are measured using the number of files affected in the four years following and preceding 2016, respectively.[13] If the cyber security governance scores have predictive power, we would expect to see a significantly negative correlation between the cyber security governance score and future cyber events. On the contrary, we observe a statistically insignificant correlation between the cyber security governance score and future cyber events (8%), suggesting the scores do not have any predictive power. The cyber security governance scores are, however, significantly negatively correlated with past cyber events (-50%), suggesting the scores reflect past cyber security events. Past cyber events and future cyber events are statistically insignificantly correlated (-7%), highlighting the unpredictability of cyber security events.

TABLE 8. CORRELATION BETWEEN S&P'S CYBER SECURITY SCORE IN 2016 AND FUTURE AND PAST CYBER EVENTS
This table reports the correlations among cyber security governance scores, future cyber events, and past cyber events. The cyber security governance scores refer to those of the 20 largest banks in 2016 provided by S&P. Future cyber events are the total files affected between 2017-2020 for all cyber security events. Past cyber events are the total files affected between 2012-2015 for all cyber security events.

| | Cyber security governance score | Future cyber events | Past cyber events |
|---|---|---|---|
| Cyber security governance score | 1.00 | | |
| Future cyber events | 0.08 | 1.00 | |
| Past cyber events | -0.50* | -0.07 | 1.00 |

*Represent statistically significant at 5% level.

13 Total files affected is sourced from Advisen, a data provider for the commercial and casualty insurance market

## REFERENCES


Aebi, V., Sabato, G., & Schmidt, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, 36(12), 3213-3226.

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2021). Hacking Corporate Reputations. Rotman School of Management Working Paper No. 3143740, available at SSRN: https://ssrn.com/abstract=3143740 or http://dx.doi.org/10.2139/ssrn.3143740

Ashraf, M. (2021). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, https://doi.org/10.2308/TAR-2019-1033

Ellul, A., & Yerramilli, V. (2013). Stronger risk controls, lower risk: Evidence from US bank holding companies. *The Journal of Finance*, 68(5), 1757-1803.

Florakis, C., Louca, C., Michaely, R., & Weber, M. (2020). Cybersecurity Risk (No. w28196). *National Bureau of Economic Research*.

Gopalan, R., Milbourn, T., Song, F., & Thakor, A. V. (2014). Duration of executive compensation. *The Journal of Finance, 69*(6), 2777-2817.

Haislip, J. Z., Peters, G. F., & Richardson, V. J. (2016). The effect of auditor IT expertise on internal controls. *International Journal of Accounting Information Systems, 20*, 1-15.

Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. (2019). The economic cost of cybersecurity breaches: A broad-based analysis. *In Workshop on the Economics of Information Security (WEIS)* (pp. 1-37).

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives, 19*(2), 73-100.

Hogan, K. M., Olson, G. T., & Angelina, M. (2020). A Comprehensive Analysis of Cyber Data Breaches and Their Resulting Effects on Shareholder Wealth. Available at SSRN: https://ssrn.com/abstract=3589701 or http://dx.doi.org/10.2139/ssrn.3589701

Institute of Internal Auditors of Australia (2021). *Auditing Risk Culture: A Practical Guide*. Available at https://www.iia.org.au/technical-resources/publications/auditing-risk-culture---a-practical-guide

Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk (No. w28906). *National Bureau of Economic Research*.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719-749.

Klemash, S., Smith, J., & Seets, C. (2020). What companies are disclosing about cybersecurity risk and oversight. Available at https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/

Kolasinski, A. C., & Yang, N. (2018). Managerial myopia and the mortgage meltdown. *Journal of Financial Economics, 128*(3), 466-485.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review, 53*(2), 413-455.

Leonhardt, M. (2019). Equifax to pay $700 million for massive data breach. Here's what you need to know about getting a cut, *CNBC*, 22 July 2019. Available at: What you need to know about the Equifax data breach $700 million settlement (cnbc.com) (Accessed: September 2021)

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory, 39*(1), 151-171.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems, 30*, 40-55.

Magee, S., Schilling, C., & Sheedy, E. (2019). Risk governance in the insurance sector—determinants and consequences in an international sample. *Journal of Risk and Insurance, 86*(2), 381-413.

Radu, C., & Smaili, N. (2021). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. *Journal of Business Ethics*, 1-24.

Sheedy, E. A., & Canestrari-Soh, D. (2020). Regulating Accountability: An Early Look at the Banking Executive Accountability Regime (BEAR). Available at SSRN: https://ssrn.com/abstract=3775275 or http://dx.doi.org/10.2139/ssrn.3775275

Sheedy, E., & Griffin, B. (2018). Risk governance, structures, culture, and behavior: A view from the inside. Corporate Governance: *An International Review, 26*(1), 4-22.

Sheedy, E. (2021). *Risk Governance: Biases, Blind Spots and Bonuses*. Routledge.

Sheneman, A. (2017). Cybersecurity risk and the cost of debt. Available at SSRN: https://ssrn.com/abstract=3406217 or http://dx.doi.org/10.2139/ssrn.3406217

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G., Sofronov, G., & Trueck, S. (2021). Quantification of Cyber Risk – Risk Categories and Business Sectors. Available at SSRN: https://ssrn.com/abstract=3858608 or http://dx.doi.org/10.2139/ssrn.3858608

Sustainability (2020). *Rate the Raters 2020*. Available at https://www.sustainability.com/thinking/rate-the-raters-2020/

S&P (2021). *CSA Companion: Corporate Sustainability Assessment*. Available at: https://www.spglobal.com/esg/csa/methodology/

Xu, H., Guo, S., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems, 33*(3), 267-284.

MACQUARIE University
SYDNEY·AUSTRALIA

# Optus Macquarie University Cyber Security Hub


**CONTACT US**

Elizabeth Sheedy
**E:** elizabeth.sheedy@mq.edu.au
Visit **Elizabeth's profile**

Fan Yu
**E:** fan.yu@mq.edu.au
Visit **Fan's profile**

Vincent McGrath
**E:** vincent.mcgrath@students.mq.edu.au
Visit **Vincent's profile**