Enterprise risk management: how do firms integrate cyber risk?

Sasha Romanosky and Elizabeth L. Petrun Sayers
RAND Corporation, Arlington, Virginia, USA

Received 30 October 2021
Revised 29 April 2022
17 August 2022
3 February 2023
Accepted 24 February 2023

Abstract

Purpose – The purpose of this study is to examine how companies integrate cyber risk into their enterprise risk management practices. Data breaches have become commonplace, with thousands occurring each year, and some costing hundreds of millions of dollars. Consequently, cyber risk has become one of the gravest risks facing organizations, and has attracted boardroom-level attention. On the other hand, companies already manage many kinds of difficult and growing risks, and that firms lose less than 1% of annual revenues as a result of cyber incidents. Therefore, how should firms appropriately address cyber risk? Is it indeed a materially different kind of risk area, or is it simply just one more risk that can seamlessly be integrated into existing enterprise risk management (ERM) practices?

Design/methodology/approach – The authors performed thematic analysis based on semi-structured interviews, with non-probabilistic, purposive sampling, to answer two main questions. First, how do firms manage enterprise risks, generally? And second, how are they integrating cyber risk into these existing processes?

Findings – The authors find that there is considerable variation in the approach and sophistication in ERM practices, such as whether they are driven more like an auditing function, or as a risk champion. The authors also find that despite the novelty of cyber risk, it can be integrated like other enterprise risks, and that cyber risk is most often seen as an operational risk (similar to workplace accidents or fraud), rather than a strategic risk, emerging from, for example, technology innovation and R&D.

Research limitations/implications – The generalization of the results is limited by the sample size and variation of firms interviewed. While the authors attempted to interview enterprise risk managers across a wide variation of firms, there were clear limitations in the scope. That being said, the authors were fortunate to be able to examine ERM and cyber risk practices across small and large, private and publicly traded companies, from a variety of business sectors.

Practical implications – The authors believe these finding are important because they present evidence that while cyber risk may be new, it does not require specialized handling or processes to track it at the enterprise level. While some firms may choose to provide special accommodations or attention because of their data collection or business practices, this approach is neither necessary nor required of all firms in all situations.

Originality/value – This research is one of the only papers that, to the best of the authors' knowledge, examines how cyber risk is integrated at an enterprise level.

Keywords Enterprise risk management, General management, Operational risk, Data breaches

Paper type Research paper

Is there a disconnect with cyber risk?

Data breaches and security incidents have become commonplace, with thousands occurring each year, and some costing hundreds of millions of dollars (Cyentia Institute, 2020). While

This work was supported by the Institute for Civil Justice at the RAND Corporation.

the rate of attacks has been increasing, so have the opportunities for compromising personal and corporate information. For example, phishing attacks, wire fraud, big data theft, social engineering, ransomware attacks, attacks on critical infrastructure and nation-state threats are all different kinds of attack vectors that firms must defend against. Consequently, cyber is ranked as one of the gravest risks facing organizations [1]. Understandably, this has attracted boardroom attention, forcing firms and their enterprise risk management (ERM) functions to address potentially massive disruptions caused by this new and evolving risk.

On the other hand, research has shown that most firms lose less than 1% of annual revenues as a result of cyber incidents (Romanosky, 2016), and that customer responses to data breach notifications are generally positive (Ablon *et al.*, 2016). Moreover, firms already deal with other kinds of strategic, operational and financial risks, and have established a corporate risk apparatus to address enterprise risks such as legal, regulatory, financial, workforce and supply chain risks.

And so, is this boardroom-level attention on cyber risks truly warranted? Are cyber risks captured in a manner that allows boards to meaningfully compare against other risks to make informed decisions, or is there a disconnect between the hype and reality of cyber risks, leading executives to make uninformed, inefficient investments in data security, potentially even overinvesting?

This research is not meant to be a study of cyber risk management, *per se*, but rather seeks to understand how cyber risk is being viewed and integrated into enterprise risk functions across firms. We believe that this is an important managerial question that is relevant to organizations across all sectors. If cyber risk is, indeed, fundamentally different from other risks, this suggests that firms need to build new strategies for assessing, tracking and communicating the risk at an enterprise level. And, perhaps most importantly, they would need fundamentally new ways to compare cyber with non-cyber risk areas. In effect, they would need to construct an entirely new risk framework. On the other hand, if cyber is not materially different, but instead just new and uncomfortable, then there should be a clear path for capturing, processing and communicating cyber risk to enterprise leadership.

In this qualitative research, we seek to answer two main questions. First, how do firms manage enterprise risks, *generally* – that is, what ERM processes do they use? And second, how are firms integrating cyber risk into these existing processes? Specifically, we examine how enterprise risks are collected and communicated to boards and executives, and we examine how cyber risks are understood relative to other risks that an organization faces. We posit that there exists a strong disconnect between the hype of cyber impacts and the reality of the actual costs imposed by these events. And because of this, cyber risks may not be as well formulated or developed as more traditional risks, leading to inefficient investments and prioritization. We also explore the role of data and seek to understand whether the obsession with data is driving a false sense of precision.

Related literature

Our research is influenced by a number of disciplines. First, there is a large body of literature discussing ERM and best practices (COSO, 2004; ISO 31000, IRGC, 2006), which all generally speak to the same principle of taking a holistic, company-wide approach to identifying and assessing the impact and likelihood of adverse events. This ERM process also helps executives define their risk appetite, and align risk mitigation steps with business strategies and goals. Ideally, the process also helps firms recognize and account for correlated risks – something that a siloed risk approach cannot do (Nocco and Stulz, 2006).

Other research examines ERM strategies intended to help establish a set of guiding principles driving relationship styles between the ERM function and the rest of the firm. For

example, Kaplan and Mikes (2016) define archetypes for how ERM functions should operate within firms: as an independent overseer, a business partner or an independent facilitator. Agarwal and Ansell (2016) present their own taxonomy of ERM strategies characterizing the ERM process as rudimentary, anticipatory, resilient or transformation.

More critically, Aven (2015) and Walker (2015) address what they perceive as limitations of ERM practices. Walker (2015) argues that current approaches only capture the *consequences* of risks, but not the *opportunities* that may be enjoyed from risky behavior. Nor do they capture the *change* in risk by applying appropriate mitigation efforts. And so, rather than building a risk register to simply enumerate negative outcomes, Aven (2015) and Walker (2015) suggest that risks should instead be framed as *impacts* to business strategies, which requires moving beyond capturing risks as probability of loss to instead capture the effect of uncertainty on business objectives.

Our research is also informed by literature regarding cyber security risk management frameworks (e.g. NIST 800–53, and ISO 270001), and research related to identifying and patching software vulnerabilities, understanding and anticipating attacker (threat) motives and overall applying better risk management practices (Paté-Cornell *et al.*, 2018; Oughton *et al.*, 2019; Ganin, 2017; Rios Insua, 2019; Allodi and Massacci, 2017). In addition, there is a separate but related body of work that seeks to understand and manage cyber risks as an enterprise risk (Stoll, 2015; Kosub, 2015; Lanz, 2018; NACD, 2020). For example, Moore *et al.*, (2015) interviewed Chief Information Security Officers (CISOs) to understand how executives make security-related investments and how they justify investments to senior leadership . The research describes how compliance, recent shocks (e.g. cyber attacks), peer effects and the desire to comply with best practices and industry frameworks are key motivators used to develop cyber security strategies.

Finally, from a methodological perspective, we leverage qualitative research methods that have been rigorously developed, specifically, the snowball (chain) sampling approach to identifying subject matter experts (Guest *et al.*, 2006) and thematic analysis, which are commonly used techniques when looking to identify and group relevant topic areas (Braun and Clarke, 2006; Glaser and Strauss, 1967).

Theoretical framework

One may consider that the objective of the rational, cost-minimizing (profit maximizing) firm is to minimize the sum of costs across all business activities to generate value for its stakeholders. One key way that business leaders accomplish this is by "quantif[ing] and manag[ing] the risk-return tradeoff that faces the entire firm" (Nocco and Stulz, 2006). Properly implemented risk management activities can add value by reducing redundant risk efforts (Hoyt and Liebenberg, 2015), increasing profitability (Sax and Andersen, 2019), improving overall efficiency (Grace *et al.*, 2015) and better aligning the firm's risk appetite with strategic goals (Tripp *et al.*, 2008). By first identifying potential losses across a portfolio of risks (be they operational, financial or strategic), firms can apply risk-mitigating activities to reduce the expected loss (costs). With these objectives in mind, firms turn to industry frameworks, largely captured as what has been called ERM.

Since the 1990s, ERM gained popularity as a "holistic approach for assessing and evaluating the risks that an organization faces" (Arena *et al.*, 2010, p. 659). It matured into a formal process in 2004 with the publication by the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004), which called into action the need for businesses to evolve from a compartmentalized ("siloed") approach, to managing risks as a single, consolidated effort championed by senior management. Specifically, COSO defined ERM as:

> A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (p. 2).

The COSO ERM framework, as with other enterprise-focused frameworks, such as Casualty Actuarial Society (CAS) [2], RIMS [3], and ISO 31000 [4], are meant to be proactive, holistic and intimately tied to the firm's strategy and business goals (Walker, 2015; COSO, 2017). That is, they describe how uncertainty of business opportunities presents both risks and rewards, and in its charge to provide stakeholder value, an effective ERM program seeks to help management identify and minimize that uncertainty.

Enterprise risk management process

The ERM process can be decomposed into a series of iterative and basic steps. First, the ERM team develops the risk register – an unordered list of risks or adverse events that the organization faces. Risk information is collected in many ways: top-down, where upper management is first polled to articulate their risks; bottom-up, where employees and management are surveyed to identify their risk; through benchmarking with peer companies; or by soliciting expert advice from consulting companies (Carroll, 2016).

The second step is risk assessment where information about each risk is collected, to include (at a minimum) the estimated impact (severity) and likelihood (frequency of occurring). Firms may also collect information related to the speed at which a loss event would be realized (*velocity*), as well as some categorization of loss type, such financial, health/safety or reputational loss.

Once identified, the ERM team vets, sorts, standardizes and prioritizes the risks. Mitigation plans may also be assigned to the individual risk (or risk owner), at which point, diagrams are often used to visualize the relative severity of risks, often according to the familiar impact/likelihood heat map as shown in Figure 1.

Next, the risks are presented to the organization's senior leadership, and conveyed in a series of presentations and documents that prioritize the most serious risks, any mitigation plans and the perceived residual risk. The risks are then monitored, and the cycle of risk identification is repeated. Certainly, there is more complexity and nuances to the entire ERM process and structure, but these steps reflect a minimum strategy relevant for this article.

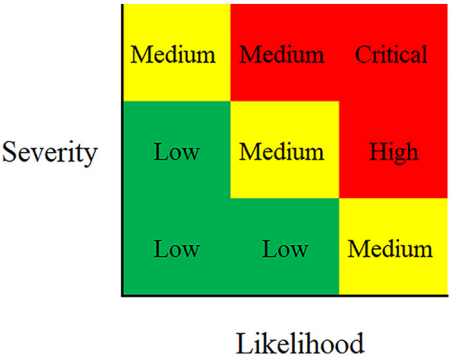

Figure 1.
Sample risk heat map

Source: Created by authors

Interview results

With this background, we next describe the results from our qualitative research, wherein we interviewed 20 senior enterprise risk managers to explore three broad topics:

(1) What does the firm's overall ERM structure look like, and what is its self-described purpose?

(2) What methods are used to collect, standardize and communicate enterprise risks across the organization?

(3) How is cyber risk viewed and managed (integrated) relative to other risk areas?

Formally, we performed thematic analysis based on semi-structured interviews to identify the relevant and important themes from the research protocol (Braun and Clarke, 2006; Glaser and Strauss, 1967). Thematic analysis provides a formal methodology for coding, analyzing and presenting these themes in structured way. We also used non-probabilistic, purposive sampling (Guest *et al.*, 2006) using a convenience sample of individuals known to the authors, as well as the chain sampling approach (Goodman, 1961), where we solicited additional candidates from the participants as well as other colleagues. Our selection criteria for participants were based on domain and professional expertise (e.g. general counsel, enterprise risk manager, risk oversight or senior auditor) and stakeholder organization (we sought a variation in size and industry of the participant's company). All participants were senior management or executives at their respective organization.

In total, we interviewed 26 risk experts between March 2019 and May 2020. Six interviews were not included in the formal analysis because they provided background insights and details on ERM and risk functions generally, rather than addressing our research questions specifically. Summary details of the remaining 20 participants are shown in Table 1.

Participant	Industry	Company size	For profit?	Publicly traded?
#1	Research	Medium	N	N
#2	Transportation	Small	Y	N
#3	Food and beverage	Small	Y	N
#4	Research	Small	N	N
#5	Telecommunication	Large	Y	Y
#6	Arts and culture	Medium	N	N
#7	Hospitality	Large	Y	Y
#8	Aerospace	Large	Y	Y
#9	Media	Large	Y	N
#10	Food and beverage	Large	Y	Y
#11	Retail	Large	Y	Y
#12	Education	Small	Y	N
#13	Finance	Small	Y	Y
#14	Utility	Large	Y	Y
#15	Pharmaceutical	Large	Y	Y
#16	Telecommunications	Large	Y	Y
#17	Retail	Large	Y	Y
#18	Food and beverage	Large	Y	Y
#19	Law firm	Medium	Y	N
#20	Energy	Large	Y	Y

Source: Created by authors

Table 1.
Participant industry

The interviews were not recorded, though research notes were taken by both authors during the interviews. As a validation test, summary notes were sent to the participants, providing an opportunity for participants to correct or modify any statements.
Next, we examine responses from the interviews.

Enterprise risk management structure

In regard to the structure of ERM groups, it was unclear what best practices, if any, firms used for managing enterprise risks, and whether any particular strategy provided optimal results. Based on our interviews, we uncovered substantial variation in size and composition at these organizations. For example, a few firms appointed only a single individual (a Chief Risk Officer, CRO) to manage ERM duties, where the individual typically operated autonomously without any direct reports. The fluidity of this structure was such that individuals were free to float between departments, meetings or other relevant committees as needed.

On the other hand, some ERM groups were composed of individuals holding dual-hatted roles, where they assumed ERM functions part-time, while also overseeing other responsibilities. For example, one organization described a collaborative approach, which included three leaders from different business lines who together managed ERM issues [5]. In this case, the firm was small enough that this ad hoc structure was most efficient, though this approach was not limited to just small companies. One large organization described a similar arrangement where, "no single person is dedicated to ERM, but instead they each spend about 10% of their time on it" [6].

Finally, half of the companies employed a dedicated ERM team, with only one exceeding 10 personnel. In these cases, organizations created distinct roles for ERM team members; for example, focusing on risk identification, measurement, data analysis, insurance issues or corporate sustainability, with one staff serving as a manager or director for all ERM activities.

Reporting structure

ERM staff reported up and through several channels. Most respondents reported some gatekeeping between themselves and top-level decision-makers, such as a board or CEO. Lone ERM staff reported some instances of direct contact with boards or senior leaders without other management involvement. Most teams or committees reported separation from top-level decision-makers, such as reporting to a CRO, one or more vice presidents or a Chief Audit Executive. In these cases, analysis from the ERM team would be shared with a gatekeeper, who then decided if further interactions or information from the ERM team were necessary.

Enterprise risk management frameworks

Less than half of respondents discussed using a guiding framework to inform ERM practices. The COSO framework (previously discussed) was the most referenced, although it elicited mixed reactions from respondents (i.e. "it seemed liked gobbledly goop to me!" [7]; "we used the COSO framework until we adopted a better approach" [8]). Organizations that mentioned frameworks tended to be small to medium sized, for-profit organizations. These risk managers were likely working to build their ERM practices and looking for available frameworks to help guide initial implementation. Over time, larger organizations created their own ERM process that deviated from general frameworks such as COSO (2004, 2017).

Other organizations relied on homegrown strategies to facilitate ERM, suggesting that ERM practices at these firms are still evolving. Without convergence of useful theories and

frameworks, risk managers appear to be left to their own discretion to implement frameworks or approaches they consider appropriate for their organizations.

Purpose of enterprise risk management

Next, we observed interesting themes that regarding the overall purpose or approach of the ERM function, which we group below into the following three archtypes: enforcers, reflectors and strategists.

Enforcers are managed by, or maintain the spirit of, the enterprise's auditing function, where risks are identified, followed clearly by risk-mitigation plans that are meticulously tracked. One respondent described their role as, "we remain the verifier, and accountable to the independent audit committee of the board" [9]. In some cases, enforcers are concerned with satisfying insurance or regulatory guidelines. For example, some industries may require certain insurance policies, and therefore interact directly with the ERM group to ensure insurance is renewed.

Reflectors included groups who are largely divorced from business lines, and instead adopt a role of merely reflecting risks to top-level decision-makers. For example, one organization described its ERM approach as "very basic and rudimentary [. . .] let's figure out what are the risks [and] let's get mitigations in place" [10], while another respondent described their ERM function as, "it's about having the right controls in the right place [. . .] we are like a mirror, reflecting what we see from the company, and aggregate it up" [11]. In other cases, the ERM function was only something that would be engaged once an issue emerged, in which case the ERM personnel would prepare and present information as needed for top-level decision-makers.

Finally, *Strategists* believe their role is to help the company grow- often by looking to push innovation and identifying where the greatest business rewards exist. These risk mavens consider what should be the firm's risk appetite to reach a desired state of risk taking. One risk manager described his role as someone to "help and facilitate the company expand with innovation" [12]. While another mentioned how they believed that the business, "should get better at discussing and analyzing how we *take* risks rather than just avoiding them" (emphasis added) [13]. Another non-profit institution similarly felt that the purpose of identifying risks was to more clearly articulate goals and take action to accomplish the firm's strategic plan. In other words, this ERM group helped the firm find new opportunities. Finally, one organization noted that they are not about "playing defense" [14], but rather they work directly with business divisions to support operations.

Enterprise risk management process

Next, we sought to better understand firm-level ERM processes for collecting and analyzing risk information, followed by a more detailed look at cyber risk processes.

Risk collection

As described by our respondents, the process of collecting and building complete risk register is a laborious task, often taking 3–4 months. The typical approach begins with the ERM group issuing surveys to directors and managers across the organization every two years, with a smaller refresh effort occurring in each off-year. Once the risks are collected, the ERM group assembles, validates (i.e. applying any corrections or adjustments), then sorts and prioritize the results in a suitable manner to present to the executives or leadership.

The survey questions are typically framed by asking employees to identify risks that would pose the greatest threat to the firm's business strategy. In some cases the business

strategies were made clear, while in other cases respondents mentioned how employees required training about corporate strategies.

Despite this consistency in the *overall* process, there was wide variation in *actual* practices. The most striking variation was the approach that firms took in how comprehensive they were in identifying risks. The majority of firms solicited information from a relatively small sample of executive leaders across the organization (e.g. typically between 50 and 100). On the other hand, one large retailer surveyed over 600 individuals, and one large health care company asked *all* employees to submit issues that they thought could pose a concern for the company. Perhaps not a coincidence, both of these companies had recently suffered major cyber incidents.

The size of the risk register (i.e. the number of risks) also varied across organizations, though size does not appear to be strongly correlated with the number of employees surveyed. Some companies appeared quite relaxed about the exercise, recognizing that the list of most critical risks did not fluctuate much (if at all) year over year, and so were typically only concerned with the top 5–10 risks. Another firm, on the other hand, produced risk registers of over 1,000 entries. Ultimately, of course, hundreds of risks are prioritized and winnowed down into around 30–40 risks. Even still, one firm conceded that of the large number of risks collected, only 20 may be critical, and of those, only 3–5 may be the most urgent, on which they spent 80% of their time.

While surveys were the most common method of collecting risk information, peer benchmarking was also frequently used. In these cases, benchmark information came from large consulting companies, while in other cases, the insights came from insurance companies or directly from 10k financial filings of other public companies. One large health care company conducted workshops of teams of 30–40 people at a time, and another large consumer food and beverage company was concerned enough with its international supply chain that it paid particular attention to geopolitical and global economic threats. A couple of respondents also used back-casting methods for risk identification. That method involved conceiving of a particularly harmful event, and tracing back necessary conditions that would need to exist in order for the event to be realized (a process that similarly known as prospective hindsight, pre-mortems or the bow-tie practice [Poole College of Management, 2016]).

Characterizing risk

At a minimum, most firms in our sample collected information about the impact and likelihood of risks using some version of a Likert scale (Likert, 1932) ranging from as few as a three-point (high, med, low) up to as much as a ten-point Likert scale. Impact measures were collected along at least one dimension: an aggregated estimate of financial loss (we discuss more of the challenges of quantifying impacts below). However, in many cases, additional outcome metrics and information were also captured, including reputation, health/safety, velocity [15] as well as mitigating controls that could help reduce the risk.

Reputation captured the public perception of a realized risk, for example, whether the risk would attract heightened (negative) media attention, while *health/safety* provided a measure of physical impact to employees or customers of the firm. *Velocity* captured the speed at which the incident (losses) was expected to propagate through the firm, and the media. Finally, *mitigations* reflected the extent to which the firm had mitigating controls to reduce the impact, or, in another case, how resilient the firm might be against the risk [16].

In a few cases, firms also collected information about how a risk affected *culpability*, *strategy*, *status* and *duration*. One international food and beverage firm was particularly concerned that consumers may blame them for avoidable incidents (*culpability*), or for incidents which they would be perceived as being negligent. This sentiment is not entirely without merit. For example, some research has examined whether shareholders punish

firms more for an avoidable incident, relative to one that was not considered avoidable (Coombs, 2007). *Status* reflected perceptions about whether the risk was a current (active) concern or whether it was merely an emerging threat, to be realized within the next —three to five years [17]. And finally, *duration* was meant to express notions of how resilient (i.e. able to withstand normal business operations) the firm might be from the risk.

Once these characteristics of impact were collected, firms needed to combine these outcome measures into a single metric (value) order to effectively prioritize and compare with other risks. One firm set the risk impact to be the *highest* of all measures, while another firm *averaged* the values. Another firm from an energy industry was particularly methodical because of its use of a very quantitative risk scoring equation, no doubt driven by the high degree of regulation and oversight from state and federal regulators.

Nevertheless, firms conceded that each of their methods for assessing risk was approximate and unscientific, and while they would each prefer to use a more defensible approach, they suggested that this form of low resolution information (i.e. an approximation) may actually be more appropriate for executives (we discuss this more below).

Executive communication

ERM reporting to executives occurred through scheduled, periodic updates or on an as-needed basis. Some boards required updates every 3, 4, 6, 12 or 24 months. In cases where reports happened as-needed, respondents reported no updates in the previous year, whereas for periodic reporting, ERM personnel used predetermined mechanisms such as annual reports or presentations to update top-level decision-makers.

Most respondents preferred to communicate risk information using PowerPoint slides and presented in a matrix or some form of heat map (as previously mentioned). Once a risk is communicated to top-level decision-makers, it was typically accompanied by risk mitigation progress; for example, the group (or individual) will assume responsibility for the risk and provide periodic updates. As described, mitigations for high risks had a time horizons of around 30 days or less, while mitigation for lower risks were queued to be addressed in months or years. The risks will remain on the board's agenda until the ERM personnel choose to remove it, based on their risk identification and prioritization process.

While not common, we found several instances of leadership intervention between ERM personnel and top-level decision-makers. For example, one risk manager noted that once a final list of risks is produced and shared with leadership, "they may review and reallocate priorities and potentially the risks they find compelling" [18]. Another risk manager similarly reported that executive leadership can "overrule us" [19] (i.e. the ERM group). A third respondent shared an instance where a CEO disagreed with the ranking of a risk and noted that it became a collaborative process to agree on its final ranking. In this sense, respondents shared examples of two different types of board/leadership: those that track organizational ERM progress and timelines, and those that actively contribute to the ERM process and push-back on results and subsequent organizational responses to identified risks.

Overall, communicating with top-level decision-makers was limited. Respondents consistently implied that it was unreasonable to expect board members to read a detailed ERM report. One respondent said that "the board does not want the whole report" [20], and added that they tend to be most interested in graphs. In some instances, risks were included on back-up slides (i.e. only shown if needed) or on "one-pager" documents [21]. There was also the strong belief that the "goal was to create a document that was digestible by board" [22]. Exposure to such distilled risks, however, was no secret. Respondents agreed that board members have limited time and thus need efficient ways of consuming risk

information. One respondent noted that, "the board cannot be responsible for saying what the risks are" [23], but rather their job is to ensure the risks are being managed. However, their ability to judge the capacity of the organization to respond to risks, and ensure that the organization can fulfill its mission, is largely tied to the presentation of risk information. In the future, greater scrutiny of risk communication might provide additional insight to the satisfaction of board members with current communication practices.

Managing cyber risks

Next we address the matter of how cyber risk is treated by organizations, and specifically whether it is viewed as a fundamentally differently kind of risk compared with other enterprise risks.

Operational versus strategic risk

The first area where cyber risk may present a more complicated understanding is regarding its classification. In most organizations, cyber risk is thought of as, and therefore falls under the broad risk category of, an *operational risk* (Kaffenberger, 2019), which is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" [24]. Other examples of operational risks include theft or fraud (either by employees or external actors), workplace accidents or natural disasters, as well as, of course, cyber security incidents stemming from accidental outages or malicious activity caused by hackers, criminals or nation-states (Romanosky, 2014).

But clearly cyber (i.e. computer and IT) capabilities and their associated technologies present not just liabilities (i.e. operational risks), but they also generate business innovations and opportunities that produce benefits. It is these benefits that can also introduce *strategic cyber* risks. But how these are best managed is unclear. Some argue that the growing threat of cyber and other technology risks warrants a dedicated board-level committee to track and manage *both* the operational *and* strategic risks (Nolan and McFarlan, 2005; Lankton and Price, 2016; Harrast and Swaney, 2019). However, despite this apparent need, only about 10% of one sample of companies had implemented any sort of technology committee (Stewart, 2017). Moreover, based on a survey of 50 corporate technology committee charters, Harrast and Swaney (2019) found that while almost all firms included an oversight role for *strategic* IT risks, only about half of them included an oversight role for *operational* IT risks [25]. This seems unfortunate because some evidence suggests that these committees add value to firms. Higgs *et al.* (2016) find that while firms with technology committees are more likely to initially *report* a breach, as the committee evolves and matures, it also becomes better at *avoiding* breaches.

From interviews conducted for this research, none of the firms identified cyber as a strategic risk, nor did they mention any sort of technology committee. This suggests that for these firms, cyber – at least as considered by the ERM group – was an inevitable cost, waiting to be realized.

Quantification of cyber risk

A particular area that presents an acute challenge for managing cyber risk is regarding quantification and assessment. It has been a longstanding challenge by information security researchers and practitioners of being able to achieve better cyber risk quantification (Muller, 2019). And yet, there may be a legitimate argument to suggest that this is neither possible nor helpful.

Indeed, quantifying risks, costs and harm has become, what some describe as, an obsession [26]. Muller (2019) writes:

> There are things that can be measured. There are things that are worth measuring. But what can be measured is not always what is worth measuring; what gets measured may have no relationship to what we really want to know. The costs of measuring may be greater than the benefits. The things that get measured may draw effort away from the things we really care about. And measurement may provide us with distorted knowledge—knowledge that seems solid but is actually deceptive.

It is also unclear to what extent quantification of cyber risks can even be achieved, or, more importantly, is even necessary. It is a longstanding problem that because cyber risks are relatively new, we lack enough information about them to develop proper actuarial tables necessary for statistical inference [27]. Indeed, Kaplan and Mikes (2016) suggest that quantitative risk modeling "should not be the sole – or even most important – basis for decision making." Quantitative models are best used to describe losses as a statistical distribution, which can then be used to compare and contrast risk areas, and assess correlations among them, but that this "becomes impossible when historical predictive data are unavailable." Kaplan and Mikes (2016) cite the global financial crisis of 2007 as an example of how and when quantitative modeling fails.

These concerns were similarly reflected in our interviews. While some firms sought to become more data-driven, most firms either acknowledged their limitations or actively recoiled on obsessing over data collection, especially when it came to presenting results to senior executives.

But, moreover, even if quantification of losses was possible, it is unclear whether this would be the proper vehicle by which to deliver risk information. In fact, the overall sentiment was that what was most useful in communicating risk was instead less *quantitative* information and more *narrative descriptions*.

For example, one firm mentioned that "quantification is not as critical because at the Board level, they are making decisions based on human judgment (which is fallible), but that's how decisions are made" [28], while another respondent mentioned, "impacts aren't quantified into dollars because it's not clear how this would be done, anyhow. And so what [the Board is] looking for is better story telling" [29]. Another respondent felt strongly how they wanted to be able to tell better narratives of the risks, and that, "trying to communicate specific metrics is incomprehensible for non IT people" [30]. Finally, another respondent described how "for the past 3 years, many people in the firm would say, "OMG cyber is big. Get a consultant in here to show us our metrics!" There was a lot of focus on quantification and metrics, but no one really understood what those meant. All [the Board] wanted and cared about was to see changes from red to green" [31]. Some respondents provided more nuance around this situation, stating that:

> [e]xecutives are better served by presenting more generic information (e.g. fewer details, less math), while more quantitative, data-driven information becomes useful for situations like allocation of funds (for mitigation), or when estimating the level of insurance they would need [32].

There is also the concern that pressing staff for more and more quantified cyber risk information would simply generate false precision based on the results of many layers of assumptions and estimates. For example, one firm mentioned that an important consideration was that because they were working with financial impact ranges of $10–$100m, finding risk mitigation strategies that could realistically change the financial impact of a risk was not easy, thereby reflecting one disadvantage of low resolution groupings. But there is a tradeoff that with too much resolution "that it can lead to inaccurate results, if even you have the data, or an implied level of accuracy that may not be reflective of reality" [33].

And so, is cyber really different?

Finally, based on these and other insights, we next examine whether, overall among these firms, cyber risks are treated differently relative to other risks.

Based on our interviews, just under half (nine) of respondents considered cyber to be fundamentally different in some way. For these firms, it was materially more difficult to manage because of the uncertainty and dynamic nature. One respondent mentioned that:

> [. . .] it's a top, if not the top risk that people report back. It scares the bejesus out of people because 90% of them don't know how to interpret and understand the risks [34].

While another respondents stated how it was different because, "cyber threats are always changing" [35], and, "it's a unique, speculative, unforeseen risk" [36]. In one case, cyber was treated differently because:

> [. . .] it has the highest visibility of all risks, and therefore the highest level of support. This is a function of how management views information security [where] risk managers [. . .] have direct access to leaders of the company [37].

At least three organizations established separate agenda items during audit committee meetings to discuss cyber risk [38]. However, in one particular case, cyber risk was treated differently not because of the difficulty in assessing risk but because of the perceived advanced capability of the information security management team. Here:

> [. . .] the ERM process has the *least* amount of oversight for cyber risks due to the security group's improved capability at assessing and tracking risks [and therefore] this "light touch" makes cyber different [39].

On the other hand, for the remaining 11 firms in our sample, cyber risks appeared to be integrated and managed organically as with other risks. While these firms recognized how cyber represented a newer risk, it was not special enough to drive firms to adjust their existing ERM practices. For example, one firm stated that they "purposely didn't create a separate committee to manage cyber risk, but instead the [existing] audit committee handles this and gets quarterly readouts" [40], and another respondent seemed unphased by the difficulties of cyber risk, stating that:

> [i]nformation system risks have been around since the 80s and so in that sense, they are not new or different. Risk management is still about people, process, and tools, and cyber still uses this paradigm – so in this way it is the same as any other risk [41].

For these firms, while they recognized and appreciated that there were genuine concerns with cyber risks, it did not cause them to materially change their processes. For example, firms stated:

> [a] few years ago it was cyber, cyber, cyber. But now, people "get it". It's everywhere, but people get it, and the panic is gone. They know there is lots to do, but there is a better sense that the company has a handle on things [42].

while another firm mentioned, "[c]yber is on the thoughts and minds of everyone, [and that overall] cyber is being managed the same as other risks" [43].

Discussion

Our research has shown that ERM practices across firms is an evolving process, with much variation in maturity and style, and not just in regard to cyber risk. For example, while some companies search diligently to find and make data-driven risk decisions, other firms were content with qualitative inputs used to characterize risk, even generally. There are

situations where collecting more data can be useful. But on the other hand, much of this effort spent may be done without purpose or direction.

We found that organizations use several types of staffing models for ERM tasks, including a single autonomous individual, dual-hatted structures, or fully dedicated teams. Based on our sample of respondents, we are reluctant to draw inferences about which approach may be more effective than another. However, what we may infer is some sense of the importance placed on the ERM function, or even the degree of impact that risk managers are expected to make within the organization. For example, a lone ERM staff member would likely have limited influence and ability to conduct far-reaching risk analysis or find novel opportunities for risk taking. Comparatively, dual-hatted staffing models permit the ability to rotate staff and diffuse the duties overtime. Dedicated staffing models, though, can collect and validate more detailed information that can then ostensibly be used to better inform decision-makers.

In regard to process, some firms approached ERM as a conventional audit exercise, while others took a much more proactive and risk-seeking approach. While some firms spent a great deal of time soliciting risk information from each employee to build up their risk register, other firms perform less rigorous inquiries with senior management. That being said, benchmarking with peer companies, consulting companies and even insurance carriers was commonly done.

One emergent theme entails the impacts of leadership interventions during the risk prioritization process. For example, risk managers shared several instances of top-level decision-makers reprioritizing risks (i.e. changing one risk from a "high" likelihood to a "medium" designation). We find this result surprising – while decision-makers must decide how to respond to risks, such interventions during the prioritization process invites additional subjectively (bias) into ERM results. Now, it is also possible that this kind of intervention and resulting discussion could actually be beneficial in identifying, or at least clarifying, problems or mitigations already in place.

Overall, our research sought to explore an underlying question of whether or not cyber is different from other risks and examine how firms integrate and accommodate cyber risk. The vast majority of firms from our interviews agreed that cyber incidents present a new and growing threat that has the potential to cause large financial loss, as well as reputational harm. However, despite this common concern, there was no common approach that firms took to accommodating it.

Cyber risk, as it is currently expressed and captured by firms, was about operational risk – similar to capturing risks related to workplace accidents, as opposed to thinking about it as a strategic risk, that arises from investing in new opportunities and innovation. And while slightly fewer than half of the firms considered cyber risk to be a very special kind of risk, the remaining firms did not, and were therefore quite content with managing it as with other (perhaps equally uncertain) risk areas.

We found that firms have responded to the threat of cyber attacks in two fundamentally differently ways. While cyber risks (e.g. threat of malicious cyber attack or business interruption caused by a cyber attack) are challenging to all firms, how they integrate it has been quite varied, with some firms reacting by establishing dedicated audit committees while other firms have seen very little material change.

We believe these findings are important because they present evidence that while cyber risk may be new, it does not require specialized handling or processes to track it at the enterprise level. While some firms may choose to provide special accommodations or attention because of their data collection or business practices, this approach is neither necessary nor required of all firms in all situations.

Finally, it is no surprise that increasingly firms are relying more and more on data collected about consumers, business processes and the environment around them. However,

with this data collection also comes a growing responsibility to protect it from accidental disclosure, ransomware attacks or malicious theft. We believe that as ERM practices become more informed and efficient, firms will be better able to identify and manage cybersecurity and privacy risks, thereby minimizing harms, while still being able to innovate and provide value to customers and shareholders.

Notes

1. In a survey conducted by Risk.net, cyber risk was ranked as the top operational risk in 2017 (www.risk.net/risk-management/operational-risk/2480528/top-10-operational-risks-for-2017); the World Economic Forum's 2018 report cited cyber risks as the second most critical risk (http://reports.weforum.org/global-risks-2018/executive-summary/); and Travelers Risk index 2018 cited cyber as the second gravest overall risk (www.travelers.com/resources/risk-index/2018-cyber-infographic).
2. See www.casact.org/area/erm/overview.pdf.
3. See www.rims.org/resources/strategic-enterprise-risk-center/risk-maturity-model.
4. See www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.
5. Respondent #3.
6. Respondent #16.
7. Respondent #13.
8. Respondent #7.
9. Respondent #20.
10. Respondent #6.
11. Respondent #16.
12. Respondent #2.
13. Respondent #10.
14. Respondent #17.
15. Respondents #16, #17.
16. Respondents # 2, #17.
17. Respondent #15.
18. Respondent #5.
19. Respondent #10.
20. Respondent #12.
21. Respondent #7.
22. Respondents #5 and #7.
23. Respondent #20.
24. As defined by Basel II, www.bis.org/publ/bcbs195.pdf.
25. Very often, IT and cyber are used synonymously.
26. See https://twitter.com/cobun/status/1094646489220071426, where Paul Ohm described some efforts as "measurement fetishism".

27. See, for example, "A lack of available relevant data adds to the challenge of quantifying and managing [cyber] risk", Cyber Risk Insurance, A Resource Guide for Actuaries, available at www.actuary.org/sites/default/files/2019-06/cyber-risk-insurance.pdf.
28. Respondent #5.
29. Respondent #6.
30. Respondent #7.
31. Respondent #10.
32. Respondent #9.
33. Respondent #14.
34. Respondent #13.
35. Respondent #12.
36. Respondent #19.
37. Respondent #9.
38. Respondents #4, #7 and #13.
39. Respondent #7.
40. Respondent #16.
41. Respondent #8.
42. Respondent #!0.
43. Respondent #14.

References

Ablon, L., Heaton, P., Lavery, D. and Romanosky, S. (2016), "Consumer attitudes toward data breach notifications and loss of personal information", RAND Corporation, RR-1187-ICJ.

Agarwal, R. and Ansell, J. (2016), "Strategic change in enterprise risk management ", *Strategic Change*, Vol. 25 No. 4, pp. 427-439, doi: 10.1002/jsc.2072.

Allodi, L. and Massacci, F. (2017), "Security events and vulnerability data for cybersecurity risk estimation", *Risk Analysis*, Vol. 37 No. 8, pp. 1606-1627, doi: 10.1111/risa.12864.

Arena, M., Arnaboldi, M. and Azzone, G. (2010), "The organizational dynamics of enterprise risk management", *Accounting, Organizations and Society*, Vol. 35 No. 7, pp. 659-675.

Aven, E.T.A. (2015), "On the need for rethinking current practice that highlights goal achievement risk in an enterprise context", *Risk Analysis*, Vol. 35 No. 9, available at: https://onlinelibrary.wiley.com/doi/pdf/10.1111/risa.12375

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101.

Carroll, R. (2016), "Identifying risks in the realm of enterprise risk management", *Journal of Healthcare Risk Management*, Vol. 35 No. 3, pp. 24-30, doi: 10.1002/jhrm.21206.

Coombs, W. (2007), "Protecting organization reputations during a crisis: the development and application of situational crisis communication theory", *Corporate Reputation Review*, Vol. 10 No. 3, pp. 163-176, doi: 10.1057/palgrave.crr.1550049.

COSO (2004), "Enterprise risk management–integrated framework".

COSO (2017), "Enterprise risk management integrating with strategy and performance, committee of sponsoring organizations of the treadway commission".

Cyentia Institute (2020), "2020 Information risk insights study", available at: www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf

Ganin, A., Quach, P., Panwar, M., Collier, Z., Keisler, J., Marchese, D. and Linkov, I. (2017), "Multicriteria decision framework for cybersecurity risk assessment and management", *Risk Analysis*, Vol. 40 No. 1, doi: 10.1111/risa.12891.

Glaser, B.G. and Strauss, A.L. (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine, Hawthorne, New York, NY.

Goodman, L.A. (1961), "Snowball sampling", *Annals of Mathematical Statistics*, Vol. 32, pp. 148-170, doi: 10.1214/aoms/1177705148.

Grace, M.F., Leverty, J.T., Phillips, R.D. and Shimpi, P. (2015), "The value of investing in enterprise risk management", *Journal of Risk and Insurance*, Vol. 82 No. 2, pp. 289-316, doi: 10.1111/jori.12022.

Guest, G., Bunce, A. and Johnson, L. (2006), "How many interviews are enough? An experiment with data saturation and variability", *Field Methods*, Vol. 18 No. 1, pp. 59-82.

Harrast, S.A. and Swaney, A.M. (2019), "What is the role of the board-level technology committee?", *Journal of Corporate Accounting and Finance*, Vol. 30 No. 4, pp. 43-47, doi: 10.1002/jcaf.22414.

Hoyt, R.E. and Liebenberg, A.P. (2015), "Evidence of the value of enterprise risk management", *Journal of Applied Corporate Finance*, Vol. 27, pp. 41-47, doi: 10.1111/jacf.12103.

Higgs, J.L., Pinsker, R.E., Smith, T.J. and Young, G.R. (2016), "The relationship between board-level technology committees and reported security breaches", *Journal of Information Systems*, Vol. 30 No. 3, pp. 79-98, doi: 10.2308/isys-51402.

Kaffenberger, L. and Kopp, E. (2019), "Cyber risk scenarios, the financial system, and systemic risk assessment", Carnegie Endowment For International Peace, available at: https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911

Kaplan, R.S. and Mikes, A. (2016), "Risk management—the revealing hand", *Journal of Applied Corporate Finance*, Vol. 28 No. 1, pp. 8-18, doi: 10.1111/jacf.12155.

Kosub, T. (2015), "Components and challenges of integrated cyber risk management", *Zeitschrift Für Die Gesamte Versicherungswissenschaft*, Vol. 104 No. 5, pp. 615-634, doi: 10.1007/s12297-015-0316-8.

Lankton, N. and Price, J. (2016), "Board-level information technology committees", available at: www.isaca.org/resources/isaca-journal/issues/2016/volume-2/board-level-information-technology-committees

Lanz, J. (2018), "Enterprise technology risk in a new COSO ERM World – The CPA journal", *The CPA Journal*, available at: www.cpajournal.com/2018/06/19/enterprise-technology-risk-in-a-new-coso-erm-world/

Likert, R. (1932), "A technique for the measurement of attitudes", *Archives of Psychology*, Vol. 140, pp. 1-55.

Moore, T.W., Tandy, Dynes, S.B.C. and Chang, F. (2015), "Identifying how firms manage cybersecurity investment.".

Muller, J.Z. (2019), *The Tyranny of Metrics Paperback*, Princeton University Press, Princeton, NJ.

National Association of Corporate Directors (2020), "Handbook on cyber-risk oversight", *National Association of Corporate Directors (NACD)*, available at: www.nacdonline.org/insights/publications.cfm?ItemNumber=67298

Nocco, B.W. and Stulz, R.M. (2006), "Enterprise risk management: theory and practice", *Journal of Applied Corporate Finance*, Vol. 18 No. 4, pp. 8-20, doi: 10.1111/j.1745-6622.2006.00106.x.

Nolan, R. and McFarlan, F.W. (2005), "Information technology and the board of directors", *Harvard Business Review*, available at: https://hbr.org/2005/10/information-technology-and-the-board-of-directors/ar/1

Oughton, E.J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., Dada, R., Ruffle, S., Tuveson, M. and Hall, J.W. (2019), "Stochastic counterfactual risk analysis for the vulnerability assessment of cyber-physical attacks on electricity distribution infrastructure networks", *Risk Analysis*, Vol. 39 No. 9, pp. 2012-2031, doi: 10.1111/risa.13291.

Paté-Cornell, M.E., Kuypers, M., Smith, M. and Keller, P. (2018), "Cyber risk management for critical infrastructure: a risk analysis model and three case studies", *Risk Analysis*, Vol. 38 No. 2, pp. 226-241, doi: 10.1111/risa.12844.

Poole College of Management (2016), "The Bow-Tie analysis: a multipurpose ERM tool, North Carolina state poole college of management", available at: https://erm.ncsu.edu/library/article/the-bow-tie-analysis-a-multipurpose-erm-tool

Renn, O. and Walker, K.D. (2008), *Global Risk Governance: Concept and Practice Using The IRGC Framework*, Springer, Dordrecht, available at: http://site.ebrary.com/id/10275002.

Rios Insua, D., Couce-Vieira, A., Rubio, J.A., Pieters, W., Labunets, K.G. and Rasines, D. (2019), "An adversarial risk analysis framework for cybersecurity", *Risk Analysis*, Vol. 41 No. 1, doi: 10.1111/risa.13331.

Romanosky, S. (2016), "Cost and consequences of cyber incidents", *Journal of Cybersecurity*, Vol. 2 No. 2, pp. 121-135.

Romanosky, S., Hoffman, D. and Acquisti, A. (2014), "Empirical analysis of data breach litigation", *Journal of Empirical Legal Studies*, Vol. 11 No. 1, pp. 74-104.

Sax, J. and Andersen, T.J. (2019), "Making risk management strategic: integrating enterprise risk management with strategic planning", *European Management Review*, Vol. 16 No. 3, pp. 719-740.

Stewart, S. (2017), 2017 Spencer Stuart U.S. Board Index, available at: www.spencerstuart.com/☒/media/ssbi2017/ssbi_2017_final.pdf?la=en

Stoll, M. (2015), "From information security management to enterprise risk management", in Sobh T., Elleithy K. (Eds), *Innovations and Advances in Computing, Informatics, Systems Sciences, Networking and Engineering. Lecture Notes in Electrical Engineering*, Vol. 313 Springer, Cham.

Tripp, M.H., Chan, C., Haria, S., Hilary, N., Morgan, K., Orros, G.C., Perry, G.R. and Tahir-Thomson, K. (2008), "Enterprise risk management from the general insurance actuarial perspective", [Presented to the Institute of Actuaries, 28 April 2008].

Walker, R. (2015), "Increasing importance of operational risk in ERM", *Journal of Enterprise Risk Management*, Vol. 1 No. 1, available at: http://thegrcbluebook.com/wp-content/uploads/2015/03/Journal-of-Enterprise-Risk-Management.pdf#page=86

Further reading

van Asselt, M.B. and Renn, O. (2011), "Risk governance", *Journal of Risk Research*, Vol. 14 No. 4, pp. 431-449, doi: 10.1080/13669877.2011.553730.

Corresponding author

Sasha Romanosky can be contacted at: sromanos@rand.org