ISACA®

Reporting Cybersecurity Risk to the Board of Directors

Risk

CONTENTS

ABSTRACT

Enterprise boards of directors need to understand how cybersecurity risk affects business objectives and board oversight responsibilities. Cybersecurity professionals have the knowledge that boards require but need to learn how to translate that information into business language that is useful to boards. This white paper helps risk and cybersecurity professionals to report cybersecurity risk in ways that their enterprise board of directors can understand, by providing an overview of board responsibilities and structure, a method to decompose high-level board concerns into technologically relevant (and measurable) risk scenarios, and information on cyberrisk economics.

Introduction

Cybersecurity professionals are being asked increasingly to prepare materials for and give presentations to their enterprise board of directors. Communicating priorities to any board member requires understanding the board perspective on the subject that is being considered. This means recognizing that board members have an overall enterprise perspective that subsumes cybersecurity. Therefore, gaining attention (and being relevant to the board) requires placing cybersecurity concerns in the context of business objectives—cybersecurity practitioners need to learn how to speak the language of business.

This white paper will help to lay out the landmarks that can be used to better understand how to adapt cybersecurity matters for consumption by professionals who are less knowledgeable about technology. The goal is to better understand the process of reporting technology risk to the board and provide context for how to tailor their messages. This white paper provides an overview of the role and structure of boards, and information on presenting cybersecurity as a strategic risk, scenario analysis, risk economics, risk appetite, metrics and dashboards. These discussions help technology professionals to communicate cybersecurity risk in ways that businesses can understand.

Role of the Board of Directors

For cybersecurity professionals to better connect their specialized skills and roles to concerns of the board of directors, it is critical that professionals understand the job of a board director. The National Association of Corporate Directors (NACD), in the United States, explains that boards have two primary responsibilities—to oversee management and to advise management.[1] According to the United Kingdom Institute of Directors (IoD), boards have a responsibility to ensure the prosperity of an enterprise.[2]

Boards have limited ability to be involved in day-to-day operations, which is the role of enterprise management. Directors take an overarching and strategic vantage point to ensure the long-term prosperity and survivability of the enterprise. They also have a legal responsibility to provide effective governance oversight, to ensure that the enterprise is well managed and to provide reasonable protections to its customers, employees, shareholders and business partners (i.e., duty of care). This governance oversight extends to ensuring that the enterprise fully understands its cybersecurity risk and is managing that risk adequately and effectively. However, to fulfill these responsibilities, directors need to be appropriately briefed by the enterprise cybersecurity and risk professionals.

Directors understand enterprise operations, such as finance, sales, corporate investment, risk management, legal and audit, and have a depth of experience from which they can draw to give guidance to enterprise operators. When boards make decisions, it is important that they balance short-term and long-term goal; keep operations focused on core business functions, while also encouraging growth and innovation; and generally understand the marketplace in which the enterprise operates. Typical board tasks include establishing/advising on vision, mission, values, strategy, legal/regulatory issues and corporate structure. The board

[1] National Association of Corporate Directors, "The Role of the Board vs. the Role of Management FAQ," 30 September 2016, https://www.nacdonline.org/insights/publications.cfm?ItemNumber=35784

[2] Institute of Directors, "What is the role of the board?," 25 September 2018, www.iod.com/services/information-and-advice/resources-and-factsheets/details/What-is-the-role-of-the-board

delegates specific tasks to management, which operates the business in alignment with board strategy and guidance.

Although cybersecurity was not a typical board task in the past, the proliferation of IT in enterprise objectives prompted the need for individuals with an IT background to appropriately advise management on their technology choices. As boards and shareholders become increasingly concerned about cybersecurity incidents, the need increases for directors that understand what good cybersecurity operations look like and how they can influence them.

Although cybersecurity was not a typical board task in the past, the proliferation of IT in enterprise objectives prompted the need for individuals with an IT background to appropriately advise management on their technology choices.

Research in reputational risk reveals that cybersecurity events can cause enterprises to no longer purchase from an enterprise that experienced an event.[3] Because enterprises rely on their reputations to meet their strategic goals, anything that can negatively affect those reputations has strategic importance. Therefore, insights into how cybersecurity failings can be connected to strategic objectives are key to helping boards better understand cybersecurity risk.

Successfully presenting cybersecurity concerns to the board requires the ability to weave a narrative around what is occurring in the broader cybersecurity industry, how attackers are affecting industry peers, and using metrics, financial impact and enterprise maturity to show how cybersecurity events will affect the enterprise.

Cyberrisk as Strategic Risk

For long time, cybersecurity was not clearly connected to enterprise objectives. This disconnect between cybersecurity and the business only recently began to be repaired. Breaches and ransomware events during the past three years brought into sharp focus how devastating the failure to manage cybersecurity risk can be to enterprise operations. The Wannacry ransomware attack in 2017 is the high-water mark in business interruption, with enterprises around the world impacted—utilities, governments, universities, healthcare, manufacturing, telecommunications, transportation and more. Aggregate losses from this single ransomware event are estimated at between several hundred million US dollars and $4 billion.[4]

Breaches and ransomware events during the past three years brought into sharp focus how devastating the failure to manage cybersecurity risk can be to enterprise operations.

Financial impacts like that of the Wannacry attack spurred senior executives and boards of directors to want to know if their enterprises are at risk and how these events will look if they happen in their enterprises. Although they have keen interest in understanding cybersecurity risk exposure, these executives and boards need a bridge between cybersecurity and business. This bridge function is best filled by risk management professionals who understand the details of technology and can render these technology concerns into operational and strategic matters.

Presenting cybersecurity as a business issue requires some translation. Strategic risk areas are those that affect, or are created by, the enterprise business strategy and objectives. The technology-to-business translation goal is to capture the elements of technological failure and connect them to enterprise objectives, presented as strategic risk. This process typically involves

[3] Moody's Investors Service, Inc., "Cyber Risk – Global: Reputational Risks From Cyberattacks Are Rising As Episodes Become More Publicized," www.moodys.com/research/Cyber-Risk-Global-Reputational-risks-from-cyberattacks-are-rising-as—PBC_1205103

[4] Berr, J.; "'WannaCry' ransomware attack losses could reach $4 billion," 16 May 2017, CBS Interactive Inc., www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

decomposing cybersecurity risk into a series of progressively decomposed loss scenarios.

At the top of the process, the broadest categories are thematic risk; cybersecurity may be one, but credit and market risk are also at this level. At the next level, the categories get more granular. For cybersecurity, this may include categories such as data disclosure, business interruption and fraud. Depending on the industry, this level may also include product security and privacy. Developing a full slate of risk that connects technology to business strategy requires the identification of scenarios that can cause negative outcomes. The section about risk identification and scenario analysis describes how to create this taxonomy.

Structure of Cybersecurity Program Oversight

A board of directors typically organizes itself into several committees—some standing committees and often some *ad hoc* committees. The exact charge of these committees varies among enterprises, but some expectations on how different committees can have an impact on cybersecurity risk reporting are described here.

Standing committees typically include an executive committee to oversee the chief executive, a governance committee that provides oversight to the board, a finance or budget committee that is responsible for revenues and expenses, and an audit committee that oversees financial reporting and disclosure. Some enterprises also have a risk committee that focuses on sources of strategic, financial, compliance and operational (including cybersecurity) risk.

Boards vary in their structures, but governance of cybersecurity operations typically comes from either the risk or audit committee—and sometimes both. It is typically the role of an enterprise risk management (ERM) function to establish a risk governance framework to provide these committees the information they need to provide appropriate oversight. A generic design principle to accomplish this is to use the Three Lines of Defense (3LoD) model.

Boards vary in their structures, but governance of cybersecurity operations typically comes from either the risk or audit committee—and sometimes both.

The 3LoD model provides layers of management controls to protect against risk. The model evolved in the late 1990s and was codified in a 2013 paper by the Institute of Internal Auditors (IIA).[5] Since then, it has become a cornerstone of most risk management frameworks and is referenced in the ISACA *Risk IT Framework*.[6]

A description of the foundation of this framework follows.

First Line of Defense (1L)

These are the control and risk owners who have operational responsibility for managing enterprise risk. Typically, these owners include the personnel in IT that are responsible for the day-to-day operation of technology controls. For example, business process owners set the requirements, and IT professionals develop software and systems to meet those requirements.

Second Line of Defense (2L)

The second line is a relatively new addition to the assurance world and encompasses risk management and

[5] The Institute of Internal Auditors, "The Three Lines of Defense in Effective Risk Management and Control," January 2013, https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

[6] ISACA, *Risk IT Framework, 2nd Edition*, www.isaca.org/bookstore/bookstore-risk-digital/ritf2?cid=pr_2004614&Appeal=pr

compliance functions. The goal of the second line of defense is to provide checks and oversight on the responsibility of the first line of defense. This line sets the standards either explicitly, by publishing internal policies and standards, or implicitly, by its influence in an advisory function and creating issues and findings. In some enterprises, the 2L reports independently of operations and directly to the chief executive officer (CEO) or the chief risk officer (CRO).

Third Line of Defense (3L)

The third line of defense is the internal audit, which provides independent validation of the functions of the first line and second line of defense. The 3L reports independently, outside of operations, and directly to the CEO.

IT risk management can also have a 1.5 line of defense (1.5L). This function sits between the first and second lines of defense and shares roles and responsibilities of both. The 1.5L is typically a function assigned to IT risk management, because it operates inside a security function and, therefore, alongside security control operators. Because information risk management typically has a large scope of work, the amount of technology in use is often too much for a pure second-line-of-defense function to oversee. In enterprises that use a 1.5L, the 2L tends to oversee checks done by the 1.5L instead of doing its own detailed checks of the first line.

These lines of defense connect to the board committees to report on risk. The 3LoD traditionally aligned to the board audit committee, giving them independent oversight of the performance of the enterprise controls. As the second line of defense developed, so too did the board risk committee. Thus, 2L work products are delivered to the risk committee in a way that is similar to the 3L reporting to the audit committee.

Legal Concerns

Some enterprises realize that their strategic goals are tied to technology and place security requirements in contracts with third parties. Governments place similar legal requirements on enterprises to help protect the public, creating economic externalities to shift the marketplace towards more secure and privacy-aware computing practices.

Boards must ensure that their enterprises are meeting these contractual and regulatory obligations to avoid potential legal claims, including any personal liability that board members may have. As a result, connecting cybersecurity to legal and regulatory implications is critical to help ensure that the needs of the board are met and that board members understand potential pitfalls. The following subsections include two major legal frameworks—GDPR and PCI DSS—that can help boards understand their legal and regulatory exposure.

GDPR

The biggest recent cybersecurity regulation to be implemented is the General Data Protection Regulation (GDPR), which passed into law in 2016 with an implementation date in 2018. With this single law, the number of countries that require breach notification jumped from eight in 2015 to 40 in 2016.[7] As of 2020, 64 countries require such disclosure. The more countries that require breach disclosure, the more consumers who will be made aware of security failings and, by extension, the less likely that the reputation of an affected enterprise will be imperiled.

Reporting on GDPR risk for a board does not require a lawyer. The cybersecurity professionals advise enterprises on their legal risk. It is important that cybersecurity professionals align with the legal function in an enterprise (internal and/or external) around the following requirements:

- Data subject consent and access to personal data (right of access)

[7] *Op cit* Moody's Investors Service, Inc.

- Data subjects can request the removal of their information (right of erasure)
- Data subjects can object to having their data processed for sales and marketing or other reasons (right to object to automated decisions)
- Cross-border data transfers have strict requirements

Not having these requirements in place creates legal risk. GDPR fines can be the greater of either €20 million (US$23.8 million) or up to four percent of annual worldwide turnover. Another GDPR requirement is to notify the supervising authority within 72 hours of identifying a reportable breach. The GDPR states that an enterprise should have processes in place to be able to detect security breaches. However, the IBM "Cost of a Data Breach Report 2020" shows that the average time to identify a breach is 207 days (up from 206 days in 2019) and a further 73 days to contain the breach.[8] Therefore, there is a potential gap between how long it takes to identify a breach and the legal requirements of GDPR.

The GDPR states that an enterprise should have processes in place to be able to detect security breaches.

Although the GDPR is an EU law, it impacts enterprises in countries outside the EU if the enterprise operates in an EU country or on behalf of a data controller in the EU that processes (i.e., stores, alters, utilizes, records, etc.) data from an enterprise that is under GDPR jurisdiction.

PCI-DSS

Since 2004, enterprises that issue or process credit cards are subject to the PCI-DSS contractual obligation. Although not a regulation, it exposes enterprises to sometimes significant financial penalties, including a prohibition against accepting credit cards. Key factors in PCI include:

- Limiting a collection of cardholder data
- Maintaining a secure system (end to end) for accepting and processing cardholder data
- Conducting regular security testing

PCI has 12 requirements and numerous subrequirements to ensure a secure cardholder data environment. Penalties or restrictions on how an enterprise can accept payment cards can be a huge limitation in an enterprise executing its strategies to achieve its objectives. Board reporting on PCI noncompliance requires connecting it to revenue goals and reputational harm. If customers do not feel safe using their credit cards at an enterprise, revenue targets suffer.

Private Rights of Action and Class Actions

In some cases, following a cybersecurity event at an enterprise, affected customers, individually or with others, can initiate legal proceedings against the enterprise, under laws established by a jurisdiction. Individual lawsuits focus on the damage incurred by a single aggrieved party; a class action lawsuit combines a series of grievances represented by a single plaintiff. There is often much greater cumulative damage from a combined lawsuit, but potentially less distraction than multiple, simultaneous lawsuits generate. Class action lawsuits are primarily a phenomenon in the United States, but they can also occur in Canada and some EU countries.

For board reporting, it is important to consider legal defense costs, ranges of possible settlements, marketing and public relation efforts to counteract any reputational harm, and costs associated with distracted boards and executives. These costs can be incorporated into risk quantification efforts.

Unfair Business Practices and Other Regulations

If a cybersecurity event impacts products or services offered, there can often be additional regulatory oversight. For example, unfair business practices cover things like deceptive marketing plans (intentional or not), outright

[8] IBM, "Cost of a Data Breach Report 2020," www.ibm.com/security/digital-assets/cost-data-breach-report/#/

fraud and misrepresentation. Attempting to market a product or service as being secure when it is not can result in action against an enterprise by government entities. Enterprises that operate in specific verticals (financial services for instance) have regulations they must follow that prescribe security requirements and limitations around how they represent their products and services to customers.

Threat Intelligence

It is critical that board directors understand the threats that are facing their enterprises. Like all board and executive communications, it is important to make sure that the complex cyberthreats that are managed every day are translated appropriately to the business concerns that are managed by the board.

This translation is of critical importance for technology professionals. Threat intelligence is a critical component of cyberdefense and leverages paid and open-source services to provide technological insight into who is attacking and what tactics, techniques and procedures (TTPs) they are employing. There are many frameworks that can be used to collect, classify and report cyberthreats, such as MITRE ATT&CK® and Lockheed Martin Cyber Kill Chain®.[9]

Threat intelligence is a critical component of cyberdefense and leverages paid and open-source services to provide technological insight into who is attacking and what tactics, techniques and procedures (TTPs) they are employing.

Although these models are useful, they are too complex to be effective for executive and board communication. Instead, categorizing the attackers and the attack types is very useful for giving executives an understanding of who is attacking and what they are using to attack.

Attacker Profiles

Constructing attacker profiles is a critical part of a threat communication plan. Attribution is not the goal—instead, the concept is to develop a series of attacker profiles that can be characterized in terms of access to resources and access to skill sets. Following is a sample set of threat communities:[10, 11]

- Nation states
- Cybercriminals
- Suppliers
- Hacktivists
- Privileged insiders
- Nonprivileged insiders

These categories are not meant to identify specific attackers (e.g., APT28 or Fancy Bear), but, instead, to give executives a range of types of attackers that the enterprise might face. Such attacker groups can be expressed quantitatively using two variables: threat capability and threat event frequency. These variables give executives a vantage point into how often these threats are acting against them and how powerful an attacker is when it does attack.

Industry-based Risk Profiles

Some immutable qualities can contribute to an enterprise threat profile. People intuitively understand that operating in certain industries can have more risk than in others. Sutton's Law states that the reason to rob a bank is that is where the money is located. Cybercrime against financial service enterprises is well known. Nation-state action against government contractors and the intelligence community (IC) at large is also well known.

[9] Lockheed Martin Corporation, "The Cyber Kill Chain®," www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[10] Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Portsmouth, NH, Butterworth-Heinemann, 2014

[11] Freund, J.; S. Fritts; J. Marius; "Using Data Breach Reports to Assess Risk Analysis Quality," *ISSA Journal*, February 2016, vol. 14, issue 2, https://issa-cos.org/wp-content/uploads/2016/02/ISSA_Journal_February_2016.pdf

Two factors that are necessary to communicate to boards and executives regarding their industry risk are target value and probability of attack by various threat communities. Creating an inventory of relevant data types, finances and other information assets that might be of value to attackers is a useful exercise. This list doubles as the enterprise list of crown jewels, which deserve special protection.

The second factor measures how likely threat communities are to take action against the enterprise. Industry classification systems, such as the North American Industry Classification System (NAICS) and Standard Industrial Classification (SIC),[12] can show the board where the enterprise fits alongside peers and how it fares across all other industries.

Risk Identification and Scenario Analysis

Risk identification is more than simply identifying a potentially bad thing. It requires a combination of systematic thinking and creativity to imagine an entire series of failings. To build out these connections between the highest and lowest levels of an enterprise requires the decomposition of high-level board concerns into technologically relevant (and measurable) scenarios.

To accomplish this, many risk professionals use labels to describe the level of decomposition with which they are working. Building an enterprise risk taxonomy can be accelerated by leveraging the BASEL II loss event type classifications.[13] This framework was originally established as a regulatory tool for financial services; however, this breakdown of risk types is very executive-friendly and is often already familiar to them. Risk type categories include fraud, hacking and business disruption.

The first step is to identify a business strategy and then decompose it into the series of cybersecurity failings that can prevent it from succeeding. A typical chain of risk decomposition (i.e., risk taxonomy) using this approach follows.

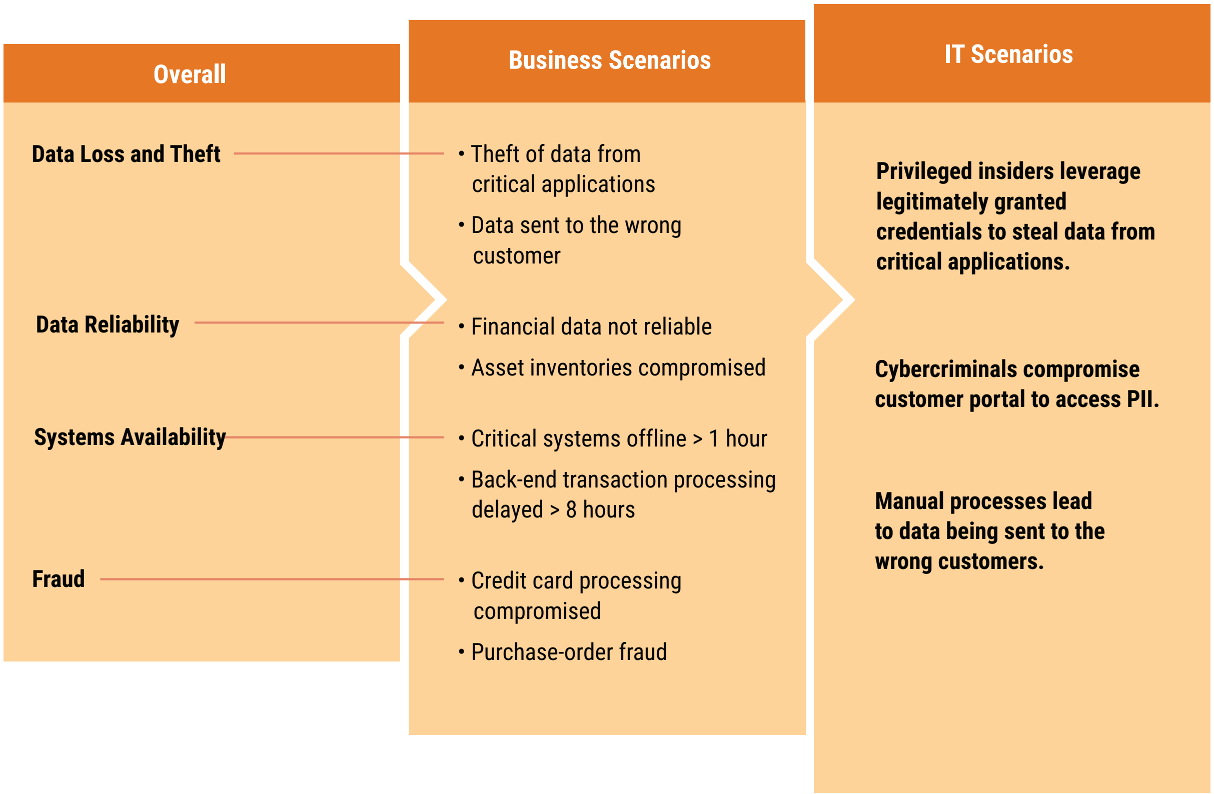
- Strategic Objective 1: Increase percentage of customers that use more than one enterprise product by 40 percent
    - Risk to Objective 1 (filtered for cybersecurity):
        - **Layer 1**—External fraud
        - **Layer 2**—Systems security
        - **Layer 3**—Hacking
        - **Layer 4**—Credential stuffing, privilege escalation, lateral movement, etc.
- Strategic Objective 2: Increase sales in North American market by 15 percent
    - Risk to Objective 2 (filtered for cybersecurity):
        - **Layer 1**—Business disruption
        - **Layer 2**—Systems
        - **Layer 3**—Software
        - **Layer 4**—Ransomware

The upper layers tend to be less technologically specific but are helpful when trying to label and classify risk from all sources in an enterprise. For example, Objective 2 risk may also include things like natural disasters and pandemics at layers 1 and 2 (in BASEL II terms: damage to physical assets and workplace safety, respectively).

Figure 1 shows a simplified example of this decomposition.[14]

[12] NAICS Association, "NAICS & SIC Identification Tools," www.naics.com/search/
[13] BIS, "OPE - Calculation of RWA for operational risk," www.bis.org/basel_framework/chapter/OPE/30.htm
[14] Freund, J.; "Communicating Technology Risk to Nontechnical People: Helping Enterprises Understand Bad Outcomes," *ISACA Journal*, vol. 3, 2020, https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/communicating-technology-risk-to-nontechnical-people

FIGURE 1: Decomposition of Scenario Analysis



Overall

- **Data Loss and Theft**
- **Data Reliability**
- **Systems Availability**
- **Fraud**

Business Scenarios

- Theft of data from critical applications
- Data sent to the wrong customer
- Financial data not reliable
- Asset inventories compromised
- Critical systems offline > 1 hour
- Back-end transaction processing delayed > 8 hours
- Credit card processing compromised
- Purchase-order fraud

IT Scenarios

Privileged insiders leverage legitimately granted credentials to steal data from critical applications.

Cybercriminals compromise customer portal to access PII.

Manual processes lead to data being sent to the wrong customers.

Risk Measurement

After the scenarios are articulated using decomposition, measuring them becomes a straightforward task. Presenting a full slate of risk scenarios to the board is not beneficial until the scenarios are ordered and prioritized using quantitative measurement that is in a familiar format for executives. The members of board committees are adept at managing financial measurements. The more a risk-management measurement resembles the financial statements and income projections that the board typically sees, the easier it is for board members to manage cybersecurity risk.

Measuring each of the risk scenarios that is articulated in the previous taxonomy by using measures of economic impact is the best way to provide prioritization for board directors. Using a cybersecurity value at risk (VaR) methodology, such as the factor analysis of information risk (FAIR), can enable the economic representation of cybersecurity risk that is sorely missing in the boardroom, but can illuminate cybersecurity exposure.[15]

Too many risk presentation methods use ordinal scale measures, which have inherent limitations and can be detrimental to good management. Such scales typically represent risk as a value from 1 to 5, for example. The actions that the board needs to take are difficult to envision with a descriptor like risk factor 3.

Too many risk presentation methods use ordinal scale measures, which have inherent limitations and can be detrimental to good management.

[15] *Op cit* Freund, J.; J. Jones

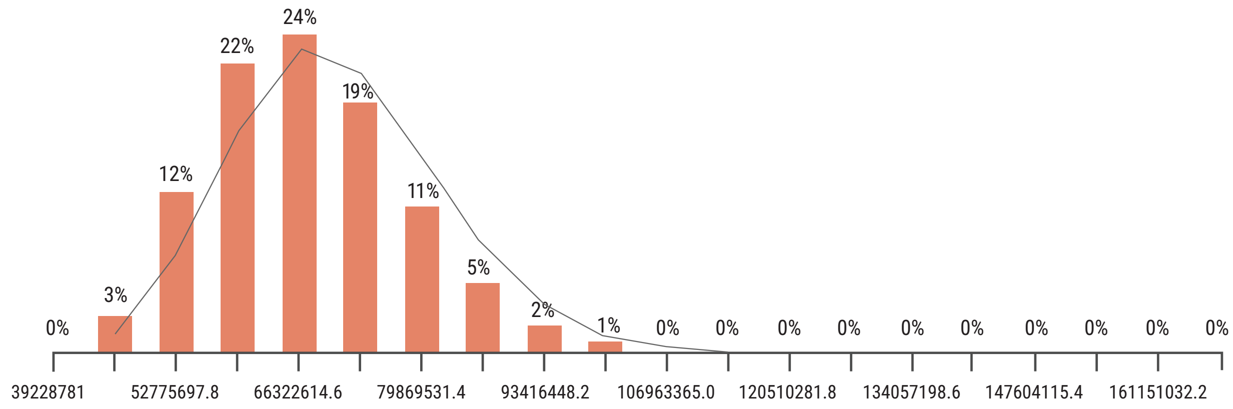
Measuring cybersecurity risk using FAIR requires a fully formed risk scenario that allows for measurement of the following:

- How often threat agents act against an asset
- How much resistance the control environment offers
- How much loss can occur if they are successful.

FAIR asks that each variable be estimated three times, to represent a best case (5th percentile), worst case (95th percentile) and a most likely (mode) value. These three estimates are input to a Monte Carlo function that creates a distribution of possible values for each input variable and then combines them to create an overall loss distribution model. This model shows a range of possible losses if a cybersecurity event materializes. An example of such a loss distribution model is shown in **figure 2**, which represents the money that an enterprise may lose if a particular scenario materializes.

Because there are numerous scenarios at the L4 level, it is not feasible to escalate all of them to the board. Instead, the strategy should be to choose exemplar scenarios to represent each aggregate category. A good way to present these scenarios and metrics to executives is through a dashboard.

FIGURE 2: Monte Carlo Loss Distribution Output from a FAIR Calculation



Dashboards and Metrics

Combining risk quantification into a board-friendly presentation requires some abstraction. Fortunately, decomposing risk scenarios allows for easy representation. **Figure 3** shows a clear and concise report that can represent enterprise risk to a board.

In **figure 3**, there are four high-level scenarios—data loss and theft, data reliability, systems reliability and fraud. An aggregate amount of risk is associated with each scenario. For communication and accessibility purposes, a single loss-event loss value (as opposed to annualized) is easier to understand and does not require probabilistic understanding. The most likely value (mode) from the previous loss distribution is a good representative value to use in this graph. However, a value at the 95th percentile might be helpful for communicating a worst-case scenario.

Each of these categories of cybersecurity risk can be decomposed down to the next level, as illustrated in **figure 4**.

FIGURE 3: High-Level Board Cyber Loss Report

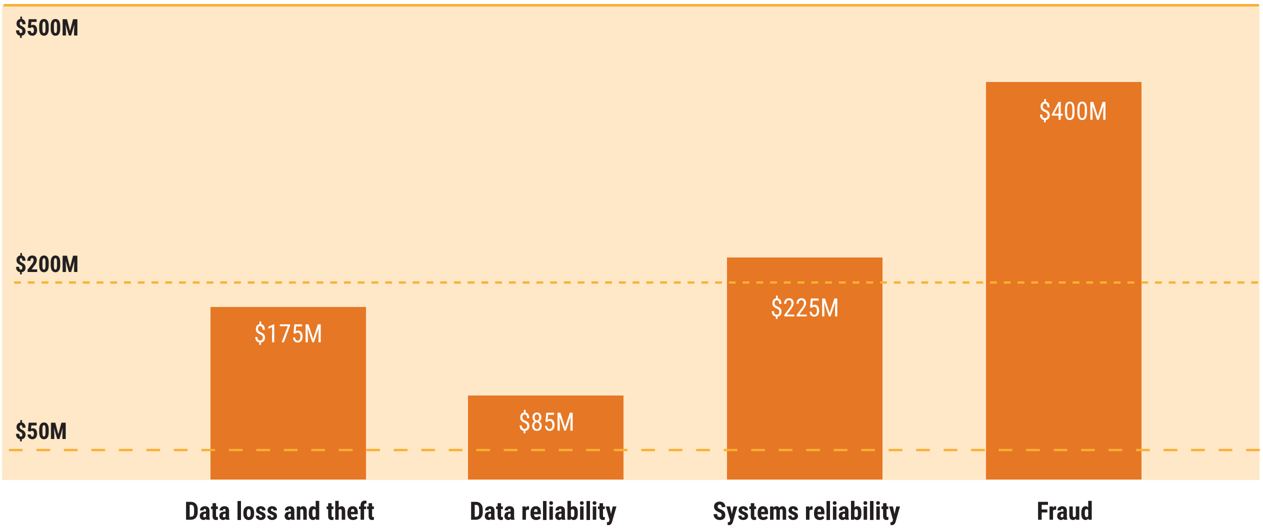
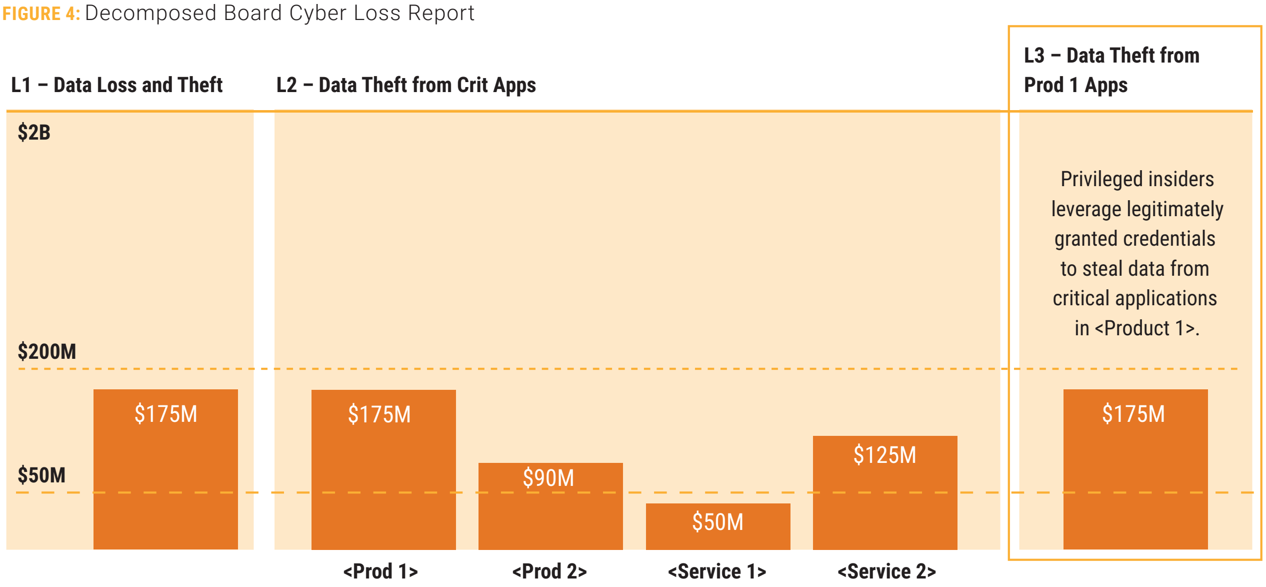


FIGURE 4: Decomposed Board Cyber Loss Report



The L1 – Data Loss and Theft risk category is derived from a measurement of the risk in critical enterprise products and services. The L3 scenario shows the highest-rated risk among these key scenarios. The highest-risk scenario across all the products and services becomes the example that is representative of the risk associated with the L1 risk scenario.

Further decomposing the L3 scenario for that product establishes a series of metrics, as illustrated in **figure 5**.

FIGURE 5: Cybersecurity Risk-Aligned Board Metrics

Metric	Thresholds (G/Y/R)	Value	Trend
KRI: Percent of applications with risk scenarios that exceed limit	10% <= 12% <= 15%	17%	←
KRI: Number of applications with open audit issues	2% <= 5% <= 8%	1%	↓
KPI: Percent of applications that completed annual risk assessment	99% >= 97% >= 95%	97%	↑
KCI: Percent of endpoints with updated DLP agent	99% >= 97% >= 95%	99%	→
KCI: Percent of applications with validated quarterly entitlements	99% >= 97% >= 95%	99%	→

These metrics can help to establish actions that boards and executives can take in response to risk that is unacceptable. For example, in the first metrics (applications that exceed limits), the recommendation is a series of control failures or gaps that can be prioritized for remediation. Generating actions for any of these quantitative risk assessments requires thresholds that drive action.

Capacity, Appetite and Limits

The concept of risk appetite can cause much confusion. Using key risk indicator (KRI) metrics to serve as an appetite is a mismatch of data and purpose. For example, using something like record count as a measure of risk has problems in implementation.[16] What happens when the record limit is reached? Are those records removed from the environment? Or, is it a lagging measure that can only be taken after a negative event has occurred?

Instead, it is advisable to establish three thresholds that each drive different actions and represent a different level of risk to the enterprise. The three categories are capacity, appetite and limits (**figure 6**):[17]

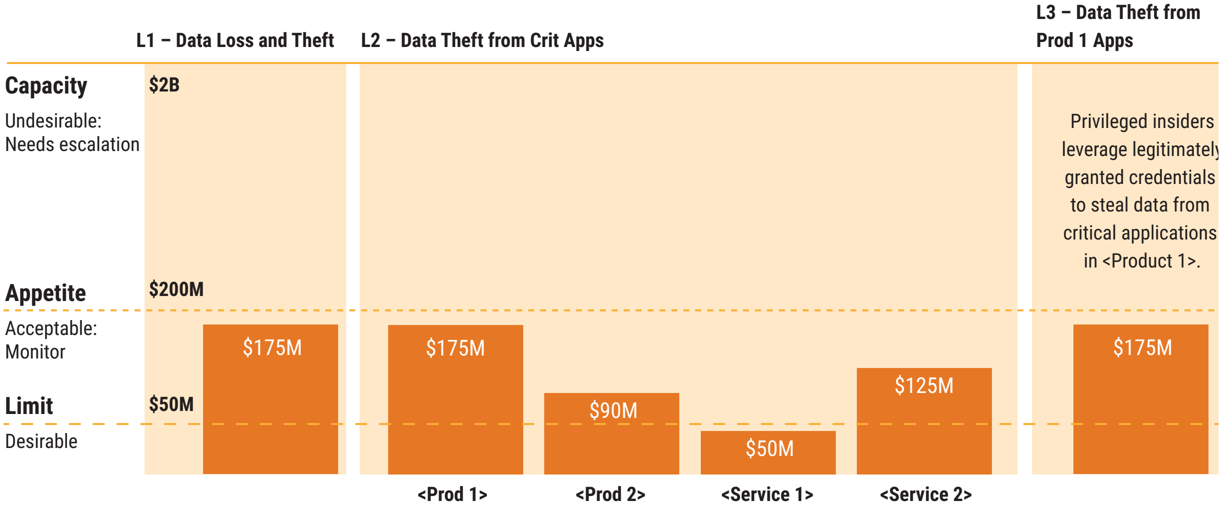
- **Capacity**—Maximum level of risk at which an enterprise can operate, while remaining within constraints implied by capital and funding needs and its obligations to stakeholders (Enterprises should not operate at this level..)
- **Appetite**—Level of risk at which the enterprise is willing to operate, but necessitates immediate escalation and action (Also known as tolerance.)
- **Limits**—Thresholds and triggers

Applying these thresholds determines whether action is necessary for the board and is helpful for making other financial decisions related to cybersecurity.

[16] Freund, J.; "Problems With Using Record Count as a Proxy for Risk," *@ISACA*, vol. 19, 14 September 2020, www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-19/problems-with-using-record-count-as-a-proxy-for-risk

[17] Deloitte, "Risk appetite frameworks: How to spot the genuine article," 2014, www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-financial-services-0614.pdf

FIGURE 6: Capacity, Appetite and Limits on Board Cyberrisk Report



Cyberrisk Economics

Several governance activities can be enabled by measuring and reporting cybersecurity risk in financial terms. Each of these has a role in determining the right risk treatment decision. The board responsibilities for protecting the enterprise depends on the directors understanding whether the enterprise is well-capitalized for regular negative events and worst-case events. Doing this properly includes exercises to measure materiality, insurance and capital allocation.

Materiality

It is important for the board directors to understand how financially material a cyberevent will be to an enterprise. Many measures of materiality tend to be fairly subjective in nature; however, some research suggests that using a value between two percent and 10 percent of gross revenue is a reasonable threshold against which to compare cyberloss estimates.[18] Based on the assessments previously outlined, a comparison can be made between the amount of expected loss and whether such a loss is financially material to the enterprise. In many cases, such a loss is considered significant and may warrant a material disclosure, regardless of whether it is financially so. Further, such a materiality threshold is likely to have a great influence on decisions to set risk appetite and limit thresholds for comparison.

Cyberinsurance

Boards are also interested in knowing if they have the correct amount of cybersecurity risk insurance coverage in place. For these types of assessments, it is helpful to know how much loss the enterprise may face. Cybersecurity risk quantification exercises are extremely helpful in determining loss potential.

For insurance purposes, a tail value can be far more helpful than a most-likely one. For boards, casting an

[18] Freund, J.; "Engineering Economic Externalities: Methods for determining material cybersecurity fines," Society of Information Risk Analysts, 2020, https://societyinforisk.org/SIRACon-2020#Jackfreund20

assessment, like a pseudo-stress test, can be helpful in setting the context. The purpose is not necessarily to insure against all cybersecurity losses, but to limit the extreme values at the tail and their impact on the enterprise balance sheet. Reporting potential risk losses to the board, accounting for insurance reductions, helps board members to understand if they are over-insured, under-insured, or properly managing their risk posture.

Capital Allocation

Certain enterprises have regulatory requirements to ensure that they have money set aside in case there are severely adverse financial impacts to the enterprise. These are called capital reserves and effectively serve as a rainy-day fund. Many of these requirements were established or enhanced after the global financial crisis of 2007 to 2008, and there are formal stress-testing exercises that help financial services enterprises to determine how much capital to set aside. These tests include operational and cybersecurity risk. Even if an enterprise does not have specific capital allocation requirements, it is prudent to consider setting money aside, depending on the enterprise risk culture.

Peer Comparisons

Many boards and executives are curious about how their enterprise compares to their peer enterprises, not only in cybersecurity loss potential, but also the maturity of their control measures. Most concerns focus on where the enterprise performs worse than its peers and what is needed to close the gap.

Most enterprises looking for a peer comparison use a third party to provide such measures. This comparison typically includes an assessment of enterprise maturity, measured on a CMMI scale from 0 to 5.[19] Although these scales are widely used, they have the aforementioned ordinal scale limitations. Further, many of the quantification efforts that are required for effective board communication are not done at the lower maturity levels of the CMMI model.

Further, many of the quantification efforts that are required for effective board communication are not done at the lower maturity levels of the CMMI model, as specific quantitative elements are prescribed at level 4.

Other peer comparisons can be done using global scales, such as the one being developed by Moody's Investor Services, which has been considering global scales in their credit-scoring methodology for several years.[20, 21]

Budgeting

The board often has conversations about funding. Boards may ask introspectively if they are spending enough money on cybersecurity. Often, basic comparisons against peers are done. The ratio of security spending compared to overall technology spending, with a target goal, for example, 10 percent, is a typical comparison to peer enterprises.[22] It is difficult to make absolute comparisons, because enterprises allocate funding for

[19] ISACA, "CMMI Levels of Capability and Performance," CMMI Institute, https://cmmiinstitute.com/learning/appraisals/levels

[20] Williams, R.; "Credit implications of cyberattacks will hinge on long-term business disruptions and reputational impacts," Moody's Investors Service Inc., 28 February 2019, www.moodys.com/research/Moodys-Credit-implications-of-cyberattacks-will-hinge-on-long-term—PBC_1161216

[21] Fazzini, K.; "Moody's is going to start building the risk of a business-ending hack into its credit ratings," CNBC, 12 November 2018, www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html

[22] Bernard, J.; D. Golden; M. Nicholson; "Reshaping the cybersecurity landscape," *Deloitte Insights*, 24 July 2020, www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

security expenses in different ways. For example, some enterprises pay for network device security through their IT budget as opposed to their security budget.

The ratio of security spending compared to overall technology spending, with a target goal, for example, 10 percent, is a typical comparison to peer enterprises.

In general, these ratio comparisons offer a limited argument when trying to justify additional spending. For example, if the enterprise has a real need for an updated logging and monitoring solution, including software, hardware and staffing, the argument that peers spend three percent more is likely to fail to get additional spending.

However, presenting such incremental spending in terms of potential economic cybersecurity losses is helpful in drawing a straight line from loss exposure that has crossed defined thresholds (appetite and limit), to the systems supporting the products and services, and to the compromised technological controls that are causing this excess loss exposure.

It is critical that such straight-line arguments allow for a follow-up to show that loss exposure was reduced. It is important that the loss amount (quantitatively) shows a reduction after the money is allocated, controls are implemented and assessments are updated, in a subsequent board report.

Issues and Findings

Sometimes, enterprises want to escalate missing, failed or broken controls directly to boards. Many enterprises mistakenly designate these issues as risk and place them in their risk register. In most cases, such voluminous lists are not appropriate for inclusion in board reports, which may include a list of top risk concerns. It is important that IT organizations align their top risk concerns reports with risk scenarios and not with missing, failed or broken controls. Identifying cybersecurity as a strategic concern and applying it to patching is a critical activity, but a list of missing patches does not communicate a strategic concern. Instead, those missing patches should be aligned to scenarios that provide a bottom-up view and, when aggregated, support the high-level assessment of organizational risk.

It is important that IT organizations align their top risk concerns reports with risk scenarios and not with missing, failed or broken controls.

Translating these broken and missing controls into strategic risk management requires a risk practitioner to avoid confusing security terminology. Leveraging the nomenclature in the FAIR methodology provides additional clarity to distinctions between risk, threat and vulnerability that are helpful to boards.[23] When asked for top risk concerns, cybersecurity professionals should not provide lists of control vulnerabilities, attack types and other maturity-based gaps. Instead, they should translate those concerns into risk scenarios and tie them to critical functions in the enterprise.

Board Education and Awareness

Another element that is often included in board presentations is general cybersecurity education and security awareness. These can include helping directors understand the particular threat actors, industry profile and risk posture facing the enterprise. However, there is value in selected storytelling to help directors understand

[23] *Op cit* Freund, J.; J. Jones

issues in the broader security industry. Directors read the news and are aware of major cybersecurity incidents. It is helpful to be conversant in these stories and to be able to offer comparisons to the enterprise. A board director is concerned with relatability, and why an event can or cannot happen in the enterprise. Lastly, some enterprises provide their board members with internal security awareness training, such as including them in phishing tests to prepare them for attempts to compromise systems and access sensitive information.

Conclusion

Communicating cybersecurity risk to the board of directors requires an individual to be conversant in technology and business. This ability starts with understanding the concerns of the board and its role in ensuring the longevity of the enterprise. It is imperative to understand how money flows through the enterprise and how technology systems support that money flow.

Articulating cybersecurity risk to the board requires the need to establish a taxonomy of cybersecurity scenarios that are aligned to those financial flows. Those scenarios can be broken down into quantitatively valid and accessible financial assessments that the board can leverage to adjust spending and take advantage of risk transfer devices to manage the enterprise and ensure its longevity. Cybersecurity board reporting is increasing, and more technology professionals will be asked to adjust their skill sets to respond.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Jack Freund, Ph.D.
CISA, CRISC, CISM, CGEIT, CDPSE, CISSP
VisibleRisk, USA

Expert Reviewers

Mike Hughes
CISA, CRISC, CGEIT, MIoD
Prism RA, United Kingdom

Jack Jones
CISA, CRISC, CISM, CISSP
RiskLens, USA

Linda Kostic
CISA, CISSP, Doctor of IT-Cybersecurity & Information Assurance, PRMIA Complete Course in Risk Management, George Washington University
Citi, USA

Katsumi Sakagawa
CISA, CRISC
Japan

Dirk Steuperaert
CISA, CRISC, CGEIT
IT In Balance, Belgium

Alok Tuteja
CRISC, CGEIT, CIA, CISSP
BRS Ventures, United Arab Emirates

Prometheus Yang
CISA, CRISC, CISM, CFE
Standard Chartered Bank, Hong Kong

Lisa Young
CISA, CISM, CISSP
Axio, USA

Board of Directors

Tracey Dedrick, Chair
Former Chief Risk Officer, Hudson City Bancorp, USA

Rolf von Roessing, Vice-Chair
CISA, CISM, CGEIT, CDPSE, CISSP, FBCI
Partner, FORFA Consulting AG, Switzerland

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

Maureen O’Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Gregory Touhill
CISM, CISSP
President, AppGate Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
Chief Executive Officer, introSight Ltd., Israel

Anna Yip
Chief Executive Officer, SmarTone Telecommunications Limited, Hong Kong

Brennan P. Baybeck
CISA, CRISC, CISM, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

Chris K. Dimitriadis, Ph.D.
CISA, CRISC, CISM
ISACA Board Chair, 2015-2017
Group Chief Executive Officer, INTRALOT, Greece

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

DISCLAIMER

ISACA has designed and created *Reporting Cybersecurity Risk to the Board of Directors* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

https://www.isaca.org/reporting-cyberrisk-to-bod

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/