CYBER-RISK OVERSIGHT HANDBOOK FOR CORPORATE BOARDS

ORGANIZATION OF AMERICAN STATES
OAS
More rights for more people

INTERNET SECURITY ALLIANCE

CYBER-RISK OVERSIGHT HANDBOOK FOR CORPORATE BOARDS

ORGANIZATION OF AMERICAN STATES

OAS

More rights for more people

INTERNET
SECURITY
ALLIANCE

WHY A CYBER-RISK OVERSIGHT HANDBOOK FOR CORPORATE BOARDS?

Cyber-attacks are the fastest growing, and perhaps most dangerous, threat facing organizations today. Several reports have shown that the digital revolution is impacting Latin America more than perhaps any region in the world. While this revolution offers hope for dramatic economic and social improvements for Latin America, it also comes with substantial risk. According to a SWIFT Institute study, "broadband internet and 3G and 4G mobile networks have spread across Latin America, allowing entrepreneurs to take advantage of technology to bring new customers into the global financial system. However, it has also resulted in rapid growth of cybercrime, as hackers take advantage of weak cyber defenses, poor cyber hygiene practices, limited law enforcement capabilities, and poor cybersecurity governance."[1]

Boards of Directors must take a leading role in oversight of the safety of their company's cyber systems. However, a recent study from the Organization of American States and the Inter-American Development Bank found corporate boards in Latin America generally have low or medium levels of maturity related to cybersecurity, with most boards having only a "formative" knowledge on cybersecurity.[2]Consequently, they may lack awareness of how cyber threats might specifically affect their organizations. However, due to the ever-changing nature of the threat, boards are seeking a coherent approach to deal with the issue at the board level. In response, the Internet Security Alliance (ISA) and the National Association of Corporate Directors (NACD) created the first Cyber-Risk Oversight Handbook for Corporate Boards in 2014. The handbook proved an immediate success in helping Boards address cyber risk on a global scale. Indeed, PricewaterhouseCoopers, in their Global Information Security Survey, referenced the handbook by name and reported that:

"Guidelines from the National Association for Corporate Directors (NACD) advise that Boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. They should discuss cybersecurity risks and preparedness with management and consider cyber threats in the context of the organization's overall tolerance for risk."

Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending."

"Other notable outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals. More than anything, board participation has opened the lines of communication between executives and directors treating cybersecurity as an economic issue."

While many elements of corporate governance in general, and cyber risk oversight in particular, are generalized, there also are unique characteristics that apply to specific countries and regions. The Organization of American States (OAS) and the ISA are working to build on the proven success of the original cyber-risk handbook and adapt it to the unique needs of the Latin American region. This publication is the result of a multi-staged process OAS and ISA engaged in with hundreds of stakeholders from corporate boards, government, academia and senior management throughout the region in an effort aid to organizations in protecting themselves from cyber threats.

CYBER-RISK OVERSIGHT HANDBOOK FOR CORPORATE BOARDS

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The following professionals are acknowledged for their contributions to the development of this Handbook through participation in project meetings, workshops, tele-conferences, and content creation.

The Handbook was revised from the 2017 U.S.-version based on their collective inputs, following a consensus process, and does not necessarily reflect the views of the companies and organizations listed.

Organization of American States (OAS)

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Miguel Ángel Cañada

Internet Security Alliance Board of Directors

INTERNET SECURITY ALLIANCE - Larry Clinton
INTERNET SECURITY ALLIANCE - Josh Higgins
USAA - Gary McAlum
LEIDOS - JR Williamson
AIG - Tracie Grella
RAYTHEON - Jeff Brown
BNY MELLON - Adrian Peters
LOCKHEED MARTIN CORPORATION - Jim Connelly
UNISYS CORPORATION - Jonathan Goldberger
VODAFONE - Richard Spearman
ERNST AND YOUNG - Andrew Cotton CARNEGIE
MELLON UNIVERSITY - Tim McNulty SECURE
SYSTEMS INNOVATION CORPORATION - John Frazzini
NORTHROP GRUMMAN - Mike Papay
CENTENE - Lou DeSorbo
SYNCHRONY FINANCIAL - Matt Fleming
DIRECT COMPUTER RESOURCES - Joe Buonomo
NATIONAL ASSOCIATION OF MANUFACTURERS - Robyn Boerstling
BUNGE LIMITED - Robert Zandoli
FIS - Greg Montana
SAP - Tim McKnight
RSA - Shawn Edwards
MUFG UNION BANK, N.A. - Lisa Humbert GENERAL
ELECTRIC - Nasrin Rezai
STARBUCKS - Dave Estlick
CENTER FOR AUDIT QUALITY - Catherine Ide
THOMSON REUTERS - Richard Puckett

Contributors

DELOITTE - Santiago Gutierrez
PINKERTON - Edith Flores
SECRETARIA DE RELACIONES EXTERIORES - Valeria Solis
CISCO - Gilberto Vicente
AIG - Ricardo Millan
BANBAJIO - Barbara Mair
HUAWEI TECHNOLOGIES - Francisco Cabrera
CENAGAS - Luis Lopez
HONEYWELL - Nahim Dias S.
CENTRO MEDICO ABC - Mary O'Keefe
GRUPO INDUSTRIAL SALTILLO - Lorena Cardenas HP - Aiza Romero Maza
ESTUDIOS Y ASESORIAS SCASOCIADOS LTDA - Cecilia Gutierrez
MINISTERIO DEL INTERIOR - Catherine Narvaez
SUBSECRETARIA DE TELECOMUNICACIONES (SUBTEL) - Jozsef Markovitz
DERECHOS DIGITALES - Pablo Viollier
CIBERSEGURIDAD HUMANA - Cristian Bravo Lillo
BANCO DE CREDITO E INVERSIONES, BCI - Lionel Olavarria Leyton
TRICOT - Susana Carey
MICROSOFT CHILE - Alex Pesso
DREAMLAB TECHNOLOGIES - Gabriel Bergel
CLEVERIT - Diego Stevens
ENTEL - Antonio Moreno Cano
MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA - Hernan Espinoza
SUBSECRETARIA DEL INTERIOR - Juan Pablo Gonzalez Gutierrez
SONDA - Juan Ernesto Landaeta
UNIVERSIDAD DE LOS ANDES - Pedro Anguita Ramirez
EY - Marcelo Zanotti
TECHNOLOGICAL UNIVERSITY OF CHILE - Karin Quiroga
ACTI - Jaime Pacheco
UNIVERSIDAD DE CHILE - Alejandro Hevia
REDBANC S.A. - Carolina Flisfisch
GLOBALSECURE - Manuel Moreno
FISCALIA PRIVADA - Gonzalo Errazuriz
SOLUCIONES ORION - Andres Cargill
RETAIL FINANCIERO AG - Claudio Ortiz T.
VINSON CONSULTING - TRANSBANK, REDBANK,

NEXUS - Alvaro Alliende
GACOF CONSULTING - Orlando Garces
CANCILLERIA - Diana Carolina Kecan Cervantes
CCIT - Juan Alcazar
ITM COLOMBIA - Armando Cuervo Vanegas
PRESIDENCIA - Martha Sanchez
HEINSOHN - Adriana Lucia Rios Sanchez
CORREO POLICIA - Alex Duran
ASO BANCARIA - Sandra Galvis
MINSAIT - Hernando Diaz Bello
ASO BANCARIA - Daniel Absalon Tocaria Diaz
CORREO POLICIA - Alvaro Rios
MINMINAS - Oscar Sanchez Sanchez
OPENLINK - Leonardo Rincon Romero
MINTRABAJO - Nidia Nayibe Gonzalez Pinzon
FONCEP - Hector Pedraza
MIN JUSTICIA - Adriana Aranguren
DAVIVIENDA - Fabian Ramirez
ESDEGUE - Jairo Becerra
MINTIC - Fabiana Garcia
ESDEGUE - Gladys Elena Medina Ochoa
TIGOUNE - Laura Botero
O4IT -Diana Carolina Echeverria Rojas
MGM INGENIERIA - Julian E. Morales Ortega
FIDUCOLDEX - Mabel Leonor Orjuela G.
SONDA - Carlos Bastidas
TIGOUNE - Alejandra Otalora
UROSARIO - Valerie Gauthier
CRCOM - Leidy Diana Rojas Garzon
COLCERT - Wilson Arturo Prieto H.
FOGAFIN - Edgar Yesid Garay Medin
COINTERNET - Gonzalo Romero
METRAIT - Juan Delgado
CRCOM - Felipe Sarmiento
DNP - Sandra Fernanda Poveda Avila
CCB - Jaime Gonzalez
TELEFONICA - Angela Maria Pava Orozco
GEC RISK ADVISORY - Andrea Bonime-Blanc
Graciela Braga
NYU and NJIT - Arnold Felberbaum
Passworld Technical College -Jeffrey Davis Jusino
Sonda - Marcos Gutierrez
Banco Central de Chile - Atilio Mashii
Banco del Austro - Fernando Aguilar Ochoa
Claro Colombia - Juan David Valderrama Silva
Instituto Federal de Telecomunicaciones - Cynthia Daniela Alvarez
Gerente TI - Giovanni Pachon
Ing.- Miguel Gaspar
Langtech - Luis Alfonso Nunez Gutierrez
Superintendencia de Bancos - Daniel Monzon
Lic. En Sistemas - Carin Molina
TTCSIRT - Angus Smith

INTRODUCTION

Internet use is increasing in Latin America at one of the highest rates worldwide[3]. There has been a corresponding digitalization of corporate risk. In the last few years the value of corporate assets has changed dramatically so that now nearly 90% of corporate assets are digital.

As a result, policy makers, regulators, shareholders, and the public are more aware of corporate cybersecurity risks than ever before. Organizations are at risk from the loss of intellectual property and trading plans, destroyed or altered data, declining public and internal stakeholder confidence, disruption to critical infrastructure, and evolving regulatory sanctions. Each of these risks can adversely affect competitive positions, stock price, and shareholder value.

Leading companies view cyber risks in the same way they do other critical risks – in terms of a risk-reward trade-off. This is especially challenging in the cyber domain for two reasons. First, the complexity and persistence of cyber threats has grown dramatically. Corporations, even comparatively small firms, now face increasingly sophisticated events that outstrip traditional defenses. As the complexity of these attacks increases, so does the risk they pose to organizations. The potential effects of a data breach are expanding well beyond information loss, modification, or disruption. Cyber-attacks can have a severe impact on an organization's reputation and brand. Companies and directors may also incur legal and financial risk resulting from cyber-attacks.[4]

Despite these risks, the motivation to deploy new and emerging technologies to drive economic development, lower costs, improve customer service, and drive innovation is stronger than ever. As cybersecurity threats grow, corporate boards can be proactive on cybersecurity by conducting risk assessments and having regular dialogue with senior management across the organization. Failure to address these vulnerabilities could result in cybercriminals blackmailing organizations by threatening to release information about the organization's vulnerabilities, risk, and competitive secrets. There are numerous other benefits to organizations for implementing stronger cybersecurity measures beyond simply protecting against attacks as well, including:

- Competitive advantage against companies that have less robust security;
- Improving cost-effectiveness through effective risk-management protocols;
- Preservation of company reputation;
- Contribution to maintaining the integrity of overall infrastructure and protecting consumer and internal stakeholder confidence;
- Direct demonstration of corporate responsibility toward all potentially affected stakeholders beyond customers – employees, shareholders, suppliers, and the community.

The World Economic Forum reports that the rapid pace of innovation and network connectivity will continue to increase in the coming years, making it even more critical that board-level action on cybersecurity be taken.[5]

These competing pressures mean that conscientious and comprehensive oversight at the board level is essential. It is critical for boards to recognize that managing and mitigating the impact of cyber risk requires strategic thinking that goes beyond the IT department. A study from the Organization of American States and the Inter-American Development Bank recommends at minimum boards understand the cyber risks their companies face, the primary methods of attack that could be employed against them, and how their company deals with and evaluates cyber issues.[6]

A rapidly evolving cyber-threat landscape :
What is the board's responsibility?

As recently as a few years ago, cyber-attacks were largely the province of hackers and a few highly sophisticated individuals. While problematic, many corporations could chalk up these events as simply a frustrating cost of doing business.

Today, corporations are subject to attackers who are part of ultra-sophisticated teams that deploy increasingly targeted malware against systems and individuals in multi-staged, stealthy attacks. These attacks, sometimes referred to as APTs (advanced persistent threats), were first deployed against government entities and defense contractors. More recently, they have migrated throughout the economy, meaning that virtually any organization is at risk.

One of the defining characteristics of these attacks is that they can penetrate virtually all of a company's perimeter defense systems, such as firewalls or intrusion-detection systems. These attacks are meticulously calculated to attack one specific target, and intruders look at multiple avenues to exploit vulnerabilities at all layers of security until they achieve their goals. The reality is that if a sophisticated attacker targets a company's systems, they almost certainly will breach them. This doesn't mean that security is impossible, it just means that cybersecurity needs to be more than simply IT-based perimeter security. As attacks have become more sophisticated, defenses must become more sophisticated. **It is not the responsibility of the board to become IT experts, but the board must know what questions to ask the IT departments. In addition, boards must provide the leadership and the commitment necessary – by proactively overseeing and holding management and the c-suite responsible - to make protecting the organization from cyber-attack a priority.**[7]

It is not just the IT systems that need to be secured, employees, contract workers and employees, whether disgruntled or merely poorly trained, present at least as big an exposure for companies as attacks from the outside. This highlights the need for a strong and adaptable security program, equally balanced between external and internal cyber threats. Management needs to assure the board that IT systems receive basic protection and that the entire cyber eco-system is secured. Organizations cannot deal with advanced threats if they are unable to stop low-end attacks and they must do so on an ongoing, persistent basis as the cyber threat never goes away.[8]

Greater connectivity, greater risk

The growing interconnected nature of traditional information systems and non-traditional systems such as mobile devices, security cameras, copiers, video-gaming platforms and cars (the so-called Internet of Things, or IoT) has resulted in a vast increase in the number of potential points of entry for cyber-attackers; and thus, the need for organizations to expand their thinking about cyber-risk,

Cyber-attackers routinely attempt to steal all types of data, including personal information from customers and employees, financial data, business plans, trade secrets, and IP. For example, in February 2019, Blind Eagle, an advanced persistent threat hacking group, has been posing as Colombia's cyber police in an effort to steal business secrets from target organizations.[9] Increasingly, cyber-attackers are employing tactics that encrypt an organization's data, effectively holding it hostage until they receive a payment – so-called "ransomware."

An Example: WannaCry

What was WannaCry?

WannaCry was a worldwide cyber-attack, which targeted computers running Microsoft Windows by encrypting data and demanding payments in Bitcoin cryptocurrency. WannaCry was a form of ransomware attack. The attack took place on May 12, 2017, beginning in Asia and spreading across more than 230,000 computers in over 150 countries. Mexico was the fifth most-impacted country by the cyber-attack.[1]

What impact did WannaCry have?

One of the largest organizations impacted by the WannaCry attack was the National Health Service (NHS) in the United Kingdom. The malware infected roughly 70,000 devices, including computers, MRI scanners, and blood storage refrigerators, resulting in significant disruption of NHS services.[1] Additionally Nissan Motor Manufacturing halted production at one of their facilities as a result of WannaCry infections, and major organizations such as FedEx were also impacted.[1] Economic losses from the attack worldwide have been estimated at $4 billion.[1]

Due to the immense number of connections to outside data systems, it is no longer adequate that organizations secure only "their" network. Vendors, suppliers, partners, customers, or any entity connected with the company electronically can become a potential point of vulnerability. For example, a major oil company's systems were breached when a sophisticated attacker who was unable to penetrate the network instead inserted malware into the online menu of a local restaurant popular with employees. When the employees used the online menu, they unintentionally granted access to the corporate system to the criminals. Once inside the company's system, the intruders were able to attack its core business.[10]

Cyber Threats by the Numbers

• Estimating the damage of cyber-attacks is difficult, but some estimates put it at $400-500 billion or more annually, with a significant portion of costs going undetected.[11] Cybercrime costs quintupled between 2013 and 2015 and could top $2 trillion per year by 2019.[12]

•Cybersecurity ranked at the top of risks to Latin American markets, according to a survey of risk and non-risk professionals.[13]

•Brazil, Argentina, and Mexico are 3rd, 8th, and 10th place, respectively, in global rankings of country of origin for cyber-attacks.[14]

•Ransomware attacks in Latin America rose by 131% in the past year.[15]Mexico and Brazil rank seventh and eights in the world for the most ransomware attacks.[16]

•34% of all new account origination fraud comes from South America.[17]

•80 percent of cyber-attacks are affiliated with organized crime.[18]

•The median number of days an organization is compromised before discovering a cyber-breach is 146.[19] 53 percent of cyberattacks are first identified by third parties (e.g. law enforcement or corporate partners), only 47 percent that are discovered internally.[20]

•48 percent of IT security professionals do not inspect the cloud for malware, despite the fact that 49 percent of all business applications are now stored in the cloud. Of those cloud-based applications, less than half are known, sanctioned, or approved by IT.[21]

•38 percent of IT organizations do not have a defined process for reviewing their cyber-breach response plans, and nearly a third have not reviewed or updated their plans since they were initially developedi[22].

Smaller Business, Bigger Risk

Although many smaller and medium-sized companies have historically believed that they were too insignificant to be targets, that perception is wrong. In fact, the majority of small and medium-sized businesses have been victims of cyber-attacks. An OAS-Symantec study revealed that small and medium sized enterprises (SMEs) are becoming a significant threat area, with the number of incidents among SMEs rising rapidly.[23] The study identified Cryptolocker ransomware as a threat increasingly targeting SMEs, while more generally, malware utilizing complex security encryption are being deployed against SMEs.[.24] In addition to being targets, smaller firms are often an attack pathway into larger organizations via customer, supplier, or joint-venture relationships, making vendor and partner management a critical function for all interconnected entities.

There is general consensus in the cybersecurity field that cyber-attackers are well ahead of the corporations that must defend against them.

This does not mean that defense is impossible, but it does mean that board members need to ensure that management is fully engaged in making the organization's systems as resilient as economically feasible. This includes developing defense and response plans that are capable of addressing sophisticated attack methods. While complex cybersecurity programs might be difficult to implement within smaller organizations that are constrained by availability of resources, all organizations should be able to implement the five core principles presented in this handbook.

Why Would They Attack Us?

Some organizations believe they are unlikely to be the victims of a cyberattack because they are relatively small in size, are not a well-known brand name, and/or don't hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information.

In fact, adversaries target organizations of all sizes and from every industry, seeking anything that might be of value, including the following assets:

- Business plans, including mergers or acquisition strategies, bids, etc.;
- Trading algorithms;
- Contracts or proposed agreements with customers, suppliers, distributors, joint venture partners, etc.;
- Employee log-in credentials and other useful information;
- Facility information, including plant and equipment designs, building maps, and future plans;
- R&D information, including new products or services in development;
- Information about key business processes;
- Source code;
- Lists of employees, customers, contractors, and suppliers;
- Client, donor, or trustee data.

Source: *Internet Security Alliance*

Balancing cybersecurity with profitability

Luis Alberto Moreno, president of the Inter-American Development Bank, highlighted the core linkage between security and successful economic development in the OAS-IADB report: “If we are to make the most of the so called Fourth Industrial Revolution, we need to create not only a modern and robust digital infrastructure but also a secure one. Protecting our citizens from cybercrime is not a mere option; it is a key element for our development.”[25]

Like other critical risks organizations face, cybersecurity cannot be considered in isolation. Members of management and the Board must strike the appropriate balance between protecting the security of an organization and mitigating losses, while continuing to ensure profitability and growth in a competitive environment.

Many technical innovations and business practices that enhance profitability can also undermine security. For example, many technologies, such as mobile technology, cloud computing, and “smart” devices, can yield significant cost savings and business efficiencies, but they also can create major security concerns if implemented incorrectly. Properly deployed, they could increase security.

Similarly, trends such as BYOD (bring your own device), 24/7 access to information, the growth of sophisticated “big data” analytics, and the use of long international supply chains may be so cost-effective that they are essential elements for a business to remain competitive. However, these practices can also dramatically weaken the security of the organization.

It is possible for organizations to defend themselves while staying competitive and maintaining profitability. However, successful cybersecurity methods cannot simply be “bolted on” at the end of business processes. Cybersecurity needs to be woven into an organization’s key systems and processes from end to end; and when done successfully, it can help build competitive advantage. One study found that four basic security controls were effective in preventing 85 percent of cyber intrusions:

- Restricting user installation of applications (“whitelisting”).
- Ensuring that the operating system is “patched” with current updates.
- Ensuring that software applications are regularly updated.
- Restricting administrative privileges (i.e., the ability to install software or change a computer’s configuration settings)[26].

The study showed that not only were these core security practices effective, they also improved business efficiency and created an immediate positive return on investment, even before considering the positive economic impact of reducing cyber-breaches.[27]

To be effective, however, cyber strategy must be more than reactive. Leading organizations also employ a proactive, forward-looking posture that includes generating intelligence about the cyber-risk environment and anticipating where potential attackers might strike. This includes subjecting their own systems and processes to regular and rigorous testing to detect vulnerabilities.

The five principles for effective cyber-risk oversight detailed in this handbook are presented in a relatively generalized form in order to encourage discussion and reflection by boards of directors. Naturally, directors will adapt these recommendations based on their organization’s unique characteristics; including size, life-cycle stage, strategy, business plans, industry sector, geographic footprint, culture, family business ties and controlling stakeholder concerns, and so forth.

PRINCIPLE 1

Boards need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Historically, corporations have categorized information security as a technical or operational issue to be handled by the information technology (IT) department. In a survey of Latin American companies, 42% said their cybersecurity efforts are led by the IT department.[28] This situation is worsened by corporate structures that leave functions and business units within the organization feeling disconnected from responsibility for the security of their own data. Instead, this critical responsibility is left to IT, a department that in most organizations is working with restricted resources and budget authority. Furthermore, deferring responsibility to IT inhibits critical analysis and communication about security issues and hampers the implementation of effective security strategies.

In an increasingly inter-connected ecosystem, every business is a technology business where IT creates and adds value and – if not properly resourced or deployed – can detract value. Most companies invest heavily in IT innovation and make technology infrastructures increasingly central to overall business strategy and operations. Depending on their sector and the services they provide, some companies rely more inherently on IT than others.

Cyber risks should be evaluated in the same way an organization assesses the physical security of its human and physical assets and the risks associated with their potential compromise. In other words, cybersecurity is an enterprise-wide risk management issue that needs to be addressed from a strategic, cross-departmental, cross-divisional and economic perspective.[29] It is not just an IT (or technology) issue, but also about business processes, people, data or information, and value. For example, cybersecurity should be incorporated into processes and human resources programs through a whole-of-organization approach. Additionally, since boards in Latin America are often completely or partially staffed by family members, it is important that the owning families in companies are adequately educated about and aware of cybersecurity concerns. OAS and IADB identify that mature corporate governance on cybersecurity would require regular engagement from the board and quick and appropriate cybersecurity strategy adjustments based on threats and risk, as well as effective allocation of funding and attention across the organization to address known (and unknown) threats. The World Economic Forum also stresses the need for boards to ensure management integrates cyber resilience and risk assessment into overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.

Cyber risk and the business ecosystem

Some of the highest-profile data breaches to date have had little to do with traditional hacking. For example, spear phishing (a common e-mail attack that targets specific individuals) is a leading cause of system compromise. Product or production strategies that use complex supply chains that span multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions requiring the integration of complicated systems, often on accelerated timelines and without sufficient due diligence, can increase cyber risk.

Another obstacle companies face in creating a secure system is how to manage the degree of connectivity that the corporate network has with partners, suppliers, affiliates, and customers. Several significant and well-known cyber-breaches did not actually start within the target's IT systems, but instead resulted from vulnerabilities in one of their vendors or suppliers. Examples of this are provided below in the section, "Greater connectivity, greater risk," on page 5 t. In Latin America specifically, a large amount of sensitive data is culturally embedded, as many organizations have developed familial relationships with their service providers and often share vast amounts of consumer information across suppliers. Furthermore, an increasing number of organizations have data residing on external networks or in public "clouds," which they neither own nor operate and have little inherent ability to secure. It is a mistake to assume that a cloud provider is automatically going to adequately secure an organizations data. Many organizations are also connected with elements of the national critical infrastructure, raising the prospect of cybersecurity at one company or institution becoming a matter of public security, or even affecting national security.

Boards of directors should ensure that management is assessing cybersecurity not only as it relates to the organization's own networks, but also regarding the larger ecosystem in which it operates. Progressive boards will engage management in a discussion of the varying levels of risk that exist in the company's ecosystem and account for them as they calculate the appropriate cyber-risk posture and tolerance for their own corporation.[30]They should pay special attention to the organizations "crown jewels" – the highly sensitive data the company needs to protect most. Management should assure the board it has a protection strategy that builds from those high-value targets outward. The Board should instruct management to consider not only the highest-probability attacks, but also low-probability, high impact attacks that would be catastrophic.[31] Appendix "A" provides more detailed guidance on questions the board may ask management on these issues.

Cyber-risk oversight responsibility at the board level

How to organize the board to manage the oversight of cyber risk, and enterprise-level risk more broadly, is a matter of considerable debate. Cyber risk can be mitigated and minimized significantly if approached as an enterprise-wide risk management issue. However, as with traditional risks, cyber risks cannot be eliminated entirely, and boards need to understand the nature of their company's threat environment. The NACD Blue Ribbon Commission on Risk Governance recommended that risk oversight should be a function of the full board.[32] NACD research finds this to be true at most US public-company boards with so-called "big picture risks" (i.e., risks with broad implications for strategic direction, or discussions of the interplay among various risks). Yet just over half of boards assign the majority of cybersecurity-related risk-oversight responsibilities to the already usually overburdened audit committee (Figure 2), which also assumes significant responsibility for oversight of financial reporting and compliance risks.

There is no single approach that will fit every board: some choose to conduct all cyber-risk-related discussions at the full-board level; others assign specific cybersecurity-related oversight responsibilities to one or more committees (audit, risk, technology, international, etc.); and still others use a combination of these methods.

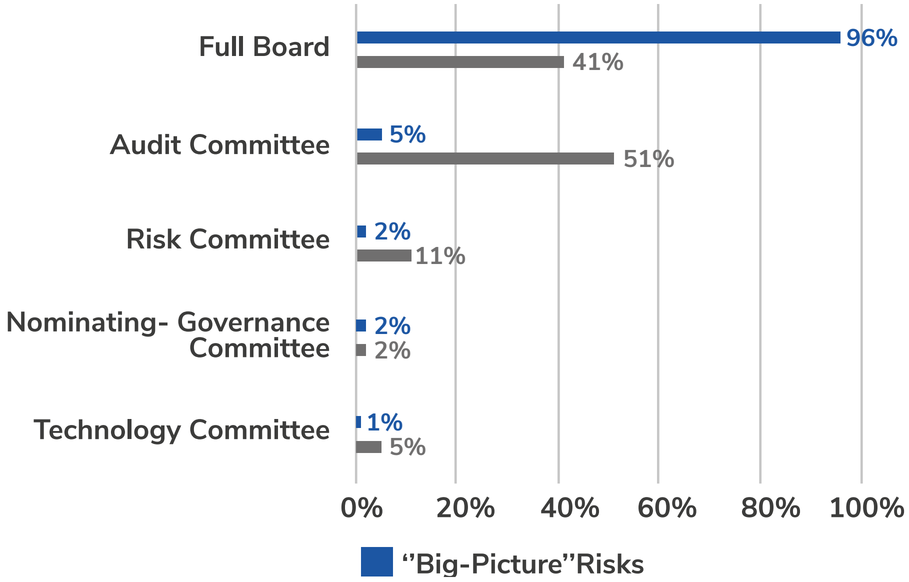
The nominating and governance committee should ensure the board's chosen approach is clearly defined in committee charters to avoid confusion or duplication of effort. Virtually all significant business decisions including mergers/acquisitions, new product development – especially those involving digital transformation issues and opportunities - and strategic partnerships have important cyber security implications and thus cyber security ought to be woven into business discussions similar to how legal and financial issues are woven into virtually all significant business discussions. The full board should be briefed on overall cybersecurity matters at least semi-annually and as specific incidents or business issues (e.g. a merger, a new strategic partnership, launching a new product and its supply chain) warrant. Committees with designated responsibility for risk oversight (and for oversight of cyber-related risks in particular) should receive overall cyber security briefings on at least a quarterly basis and as specific incidents or situations arise.

See Appendix A for suggested questions to help directors assess their Board's level of understanding of cybersecurity issues or cyber literacy.

In order to encourage knowledge-sharing and dialogue, some boards invite all directors to attend committee-level discussions on cyber-risk issues or make use of cross-committee membership. For example, one global company's board-level technology committee includes directors who are experts on privacy and security from a customer perspective. The audit and technology committee chairs are members of each other's committees, and the two committees meet together once a year for a discussion that includes a "deep dive" on cybersecurity.[33] Some boards are even establishing a cybersecurity committee to better address these issues.

Figure 2

To which group has the Board allocated the majority of tasks connected with the following areas of risk oversight? (Partial list of response choices' multiple selections permitted)



Source: *(2016-2017 NACD Public Company Governance Survey)*

PRINCIPLE 2

Boards should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

The legal and regulatory landscape with respect to cybersecurity, including required disclosures, privacy and data protection, information-sharing, infrastructure protection, and more, is complex and constantly evolving. Boards should stay aware of current liability issues faced by their organizations – and, potentially, by directors and family owners and controlling shareholders on an individual basis. For example, high-profile attacks may spawn lawsuits, including shareholder and customer class-actions, and could lead to regulatory enforcement actions. Claimants also may allege that the organization's board of directors neglected its fiduciary duty by failing to take sufficient steps to confirm the adequacy of the company's protections against data breaches and their consequences. Exposures can vary considerably depending on the organization's sector and operating locations. Regardless of the legal merits or ultimate outcome of any challenge, reputational damage to a business from a cyber-breach can be severe and long-lasting. It is not only important that the board take the following steps, but it is equally important that they document their due diligence.

Boards should consider how they:

- Maintain records of discussions about cybersecurity and cyber risks;
- Stay informed about industry-, region-, and sector-specific requirements that apply to the organization, including any laws and requirements that might be established at the regional, state, and local level;
- Analyze evolving risks in relation to business resilience and response plans;
- Determine in advance what to disclose in the wake of a cyberattack.

The culture of a company tends to flow from the top down and so boards should take a vigorous approach to cybersecurity, holding management tightly accountable, to show employees that cyber risk must always be an important consideration. Effective governance structures should then be implemented to underpin that culture and ensure the company is properly focused on managing these risks. It also is advisable for directors to participate in cyber-breach simulations to gain exposure to the company's response procedures in the case of a serious incident to mitigate against its potential impact, and to practice for a potential scenario that requires the board to make an important decision.

Among the topics boards should be mindful of are:

Board Discussion and Minutes

Board minutes should reflect the occasions when cybersecurity was present on the agenda at meetings of the full board and/or of key board committees, as well as when cyber issues were woven into specific business issues before the board such as employee training or strategic partnerships. Discussions at these meetings might include updates about specific risks and mitigation strategies, as well as reports about the company's overall cybersecurity program and the integration of technology with the organization's strategy, policies, and business activities.

Legal Landscape

As in much of the world, Latin American governments are considering a wave of new regulations regarding cyber security and privacy. While it is important that boards demand their management comply with cyber and privacy regulation, it is **critical** for boards to also understand that being in compliance with government standards and regulations is not equivalent to being secure. Many government regulations provide for only minimum security measures that may well be insufficient to secure valuable data from ever increasingly sophisticated cyber-attack methods.

Many organizations will need to manage overlapping and even conflicting rules and requirements stemming from lack of coordination among rulemaking and legislative authorities, and different priorities driving the development of new regulations. While directors do not need to have deep knowledge about this increasingly complex area of law, they should be briefed by internal or external counsel on a regular basis about requirements that apply to the company. Reports from management should enable the board to assess whether or not the organization is adequately addressing both their security and potential legal risks.

A company's disclosure and reporting requirements depend on the type of business it runs and the sector in which it operates. However, all board members should keep in mind their overriding duty as directors to exercise reasonable care, skill and diligence.[34]

A report prepared by the OAS Cybersecurity Program[35] recommended defining and enforcing sound privacy and data protection regulatory frameworks, creating national, sustainable multi-stakeholder platforms, and strengthening international cooperation. In recent years, policymakers' interest in cybersecurity and privacy has grown, and while many cybersecurity laws and regulations remain in their nascent stage, there are several trends emerging across the legal landscape in Latin America:[36]

1. Development of privacy and data protection-focused regulations aligned with European Union requirements;
2. Integration of cybersecurity regulation into financial technology laws;
3. Introduction of requirements to notify regulatory authorities of data breaches.

Another legal matter that must be taken into account is criminal activity related to the underground economy, as laundering of assets such as cryptocurrency poses a major threat and can have significant impact on the cybersecurity of an organization.

Privacy and data protection regulations[37]

Many policymakers in Latin America are looking to the European Union's approach to cybersecurity as a model as they develop their own regulations. While most of these regulations are in their infancy, development and implementation of privacy-focused cybersecurity regulations has become a priority for Latin American governments. Countries in Latin America are beginning to integrate the EU's General Data Protection Regulation (GDPR) and other EU cybersecurity directives into their own comprehensive data protection regimes. The region also is using the Budapest Convention (Argentina, Chile, Costa Rica, the Dominican Republic, Panama and Paraguay were parties to the Budapest Convention, and Colombia, Mexico, and Peru were observers) on cybercrime as a model, and enforcement of EU cybersecurity directives is already in effect. With it appearing more likely that the region will adopt an EU-based model, it is likely businesses will need to adhere to cybersecurity requirements that necessitate implementation of "appropriate" technical and organizational measures to ensure a level of security appropriate to risk.

Financial technology ”fintech” requirements

Latin America has emerged at the forefront of developing new technology within the financial sector. Countries in Central and South America have preserved an innovation-driven financial sector, but new requirements are emerging via cybersecurity policies and requirements for data processing and storage. Many of these regulations are still in development but are expected to bring more certainty to industry on what cybersecurity measures need to be in place. However, financial institutions likely will face more heavy cybersecurity obligations due to the focus on cybersecurity of fintech devices and services.

“Notification to Authority” requirements

Latin American countries traditionally have required reporting data breaches to affected parties but not regulatory authorities. However, that is beginning to change as Latin American organizations begin to comply with GDPR and other European regulatory obligations. Due to implementation of the EU rules, many Latin American countries are beginning to create national data protection authorities and adopt “notification to the authority” rules similar to those included in the GDPR, establishing requirements for not only notifying affected consumers but also relevant regulatory authorities.

Role of legal counsel

In-house legal and compliance teams, together with external counsel play a critical role in the fight against cyber-attacks, especially as regulators in the region grow stronger and more active in areas like cybersecurity and corporate governance.[38] Directors should ask management to solicit legal counsel’s views on:

- Implementing a framework to mitigate against legal and regulatory risks;
- The organization’s cyber incident response plan, including interaction with regulators and document management;
- Potential disclosure considerations related to forward-looking risk factors in general.

As disclosure standards, regulatory guidance, formal requirements, and company circumstances all continue to evolve, management and directors should expect to be updated on a regular basis by legal counsel.

Litigation

Boards may face litigation, for example, if action is taken against the company by customers or employees affected by a data breach, or by shareholders alleging that the board failed to take appropriate steps to protect assets, or that it mismanaged the response to a breach.

Organizations also may be required to bring litigation, for example, in the form of injunctions freezing money or information stolen by cyber criminals or in claims against responsible third-party suppliers. In each case, the board will be required to make strategic decisions based on a variety of factors such as costs, publicity, prospects of success and duties owed to shareholders.

PRINCIPLE 3

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

In a recent survey, only about 14 percent of directors believe their Board has a “high” level of knowledge of cybersecurity risks.[39] An OAS study revealed that most corporate boards in Latin America have a “startup” or “formative” understanding of cybersecurity, meaning they have minimal or no understanding of cybersecurity and related fiduciary duties, or have some awareness of cyber issues but not on how risks might affect their organizations. Even among the corporate boards in Latin America that have more advanced cybersecurity knowledge, management of cyber issues has tended to be perimeter oriented and reactive rather than proactive. As the World Economic Forum has pointed out “Being resilient requires those at the highest levels of a company, organization, or government to recognize the importance of avoiding and proactively mitigating risks.”

Unless there have been discovered cyber incidents, boards have not been aware of where to go to address cybersecurity within their companies. The OAS study stresses the criticality of using cybersecurity best practices within their governance structure, calling on boards to understand the risks they face, primary attack methods, and company protocols for dealing with cyber threats.

Receiving one-time or only periodic briefings may also be inadequate. One director observed: “[Cybersecurity] is very much a moving target. The threats and vulnerabilities are changing almost daily, and the standards for how to manage and oversee cyber risk are only beginning to take shape.”[40] At a different peer-exchange session, another director suggested this useful analogy: “Cyber literacy can be considered similar to financial literacy. Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business.”[41] (See appendix A for more on cyber literacy)

Improving access to cybersecurity expertise

As the cyber threat has grown, the responsibility (and expectations) of board members has grown. Directors need to do more than simply understand that threats exist and receive reports from management. They need to employ the same principles of inquiry and constructive challenge that are standard features of board-management discussions about strategy and company performance.

As a result, some companies are considering whether to add cybersecurity and/or IT security expertise directly to the board via the recruitment of new directors. While this may be appropriate for some companies or organizations, there is no one-size-fits-all approach that will apply everywhere.

Nominating and governance committees must balance many factors in filling board vacancies, including the need for industry expertise, financial knowledge, global experience, owning family and controlling stakeholders’ desires, and other desired skill sets, depending on the company’s strategic needs and circumstances. In Latin America often time family business owners and controlling shareholders hold significant influence over corporate board decision-making and membership, and thus play a significant role in determining whether to add cyber expertise to the board. Whether or not they choose to add a board member with specific expertise in the cyber arena, boards can take advantage of other ways to bring knowledgeable perspectives on cybersecurity matters into the boardroom, including:

- Scheduling deep-dive briefings or examinations from independent and objective third-party experts validating whether the cybersecurity program is meeting its intended objectives;
- Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multi-client and industry-wide perspective on cyber-risk trends;
- Participating in relevant director-education programs, whether provided in-house or externally.
- Providing opportunities for directors to share takeaways from outside programs on cybersecurity with fellow board members
- Creating education opportunities on cybersecurity to board members, company owning families, and/or controlling stakeholders that have major influence in board decisions.

Gaining Access to Adequate Cybersecurity Expertise

Most directors are specialists in particular fields or areas of expertise. While they may have certain subject matter expertise derived from their previous careers, directors should bring a broader view of enterprise-wide risk management and response.

An organization does not necessarily need to add a cyber-expert to its board. That is a decision best left to each business. However, boards should be clear as to where cyber responsibility may lie such as a board committee, specified management or the full board. This refers to the responsibility of the oversight, not execution, of cybersecurity and the risk management issues that accompany it and convey the importance of cybersecurity to controlling stakeholders and family owners

Moreover, cyber risks have some important differences from traditional risks. For example, organizations cannot fully protect themselves in an interconnected and rapidly evolving world. Cyber adversaries, including nation states, may have more resources than even the biggest corporations, and the practical difficulties associated with catching and tracing cyber-criminals are often greater than those associated with more conventional criminals, something the cyber oversight board member(s) should understand.

There are several ways boards can consider increasing their access to security expertise. Boards can create a check-and-balance system by seeking advice from multiple sources. For example, some sophisticated organizations have developed reporting structures from three independent (not necessarily external) sources, which could include the perspective of the person accountable for cyber risk, the perspective of the person assessing cyber risk, and the perspective of the operational manager. This enables an organization to challenge the functions and approaches and see cyber risk from varied perspectives. Principle 4, below, offers an outline of an organizational structure that may over time enhance the overall knowledge base regarding cyber security within an enterprise.

Enhancing management's reports to the board

When asked to assess the quality of information provided to the board by senior management, information about cybersecurity was rated lowest. Nearly a quarter of US public-company directors reported that they were dissatisfied or very dissatisfied with the quality of information provided by management about cybersecurity. Less than 15 percent said they were very satisfied with the quality of the information they received, as compared with an approximately 64 percent high-satisfaction rating for information about financial performance.[42]

Survey respondents identified several reasons for their dissatisfaction with management's cybersecurity reporting, including:

- Difficulty in using the information to benchmark performance, both internally (among business units within the organization) and externally (with industry peers);
- Insufficient transparency about performance; and
- Difficulty in interpreting the information.[43]

Cybersecurity and cyber-risk analysis are relatively new disciplines (certainly, less mature than financial analysis) and it will take time for reporting practices to mature. Nonetheless, board members should set clear expectations with management about the format, frequency, and level of detail of the cybersecurity-related information and key performance indicators they wish to receive, and reports should be written in business terms. In reviewing reports from management, directors should also be mindful that there might be an inherent bias on the part of management to downplay the true state of the risk environment. One study found that 60 percent of IT staff do not report cybersecurity risks until they are urgent (and more difficult to mitigate) – and acknowledged that they try to filter out negative results.[44] Boards' should seek to create a culture of open, straightforward and transparent communication on cyber-risk management and reporting.

See Appendix D for details regarding what sorts cyber-risk reporting metrics boards can and should expect to receive from management.

Source: *2016-2017 NACD Public Company Governance Survey*

PRINCIPLE 4

Board directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

Technology integrates modern organizations, whether workers are across the corridor or halfway around the world. But, as noted earlier, the reporting structures and decision-making processes at many companies are legacies of the past, where each department and business unit make decisions relatively independently, and without fully taking into account the digital interdependency that is a fact of modern business. Directors should seek assurances that management is taking an appropriate enterprise-wide approach to cybersecurity. The World Economic Forum (WEF) notes that boards' governance function is vital regarding cybersecurity.

Appendix J contains considerations for building a relationship with the CISO and the security team.

Creating an Overall Approach to Cyber-Risk Management

An organization should start with an assessment of its unique risk profile and threat environment. Perhaps the greatest risk to a modern organization is to operate under a poorly constructed risk assessment mechanism. The ability of an organization to implement an effective cybersecurity framework starts with a clear understanding of the risk environment, its unique risk appetite, and the availability of resources needed to mitigate the potential cyber risks. It truly begins with an appropriately developed and relevant enterprise risk management (ERM) system in place where a company's principal strategic risks and other risks are properly collected, assessed, prioritized, mitigated, and reported.

Technical Controls Framework for Risk Management

It is essential that management be able to articulate clearly to the board the existence and implementation of a thoughtful and coherent technical framework to manage and secure the organizations data. In the United States the NIST Cybersecurity Framework is used to outline a set of standards, methodologies, procedures, and processes that aligns policy, business, and technological issues to address cyber risks. The NIST framework seeks to provide a common language for senior corporate management to use within the organization in developing an enterprise-wide approach to cyber-risk management.

Several Latin American governments have begun moving forward with their own cybersecurity standards frameworks. For example, the Government of Peru has in recent years requested technical assistance from the OAS in developing its own national cybersecurity framework. Peru has also implemented the ISO 27001:2013 standard, which is also being increasingly utilized throughout Latin America.

On a broader scale, the Red Iberoamericana has published Standards for Data Protection for the Organization of Ibero-American States in June 2017. These standards are largely based upon the EU's GDPR's security standards.

It should be noted that there also may be industry specific cybersecurity framework(s) relevant to organizations. For example, fintech regulatory regimes – such as those being developed by the Comisión Nactional Bancaria y de Valores, Mexico's banking and securities regulator –may designate specific requirements for data security and privacy for financial sector entities.

Many organizations will adapt one or more of these frameworks to their unique sector, culture and business plans. What is important from the board's perspective is not to understand the technical details of the framework, but that management has a coherent plan for assuring technical cyber security and be able to clearly articulate this to the board.

While the existence of a coherent technical framework – driven by business goals – is critical, and possibly necessary for various compliance requirements, boards must be aware that compliance with technical frameworks does not necessarily equate with an organization's data being adequately secured. Indeed, the operational checklists of requirements typically based on these frameworks have been widely criticized for not providing a true picture of an organization's security. Fortunately, the field of cyber risk management is evolving and new cyber risk assessment methods are now available which provide a more contextualized, empirical and economics-based way for an organization to understand its relative cyber security. See the appendix on metrics for examples of these newer methods of risk assessment.

A Management Framework for Cyber Security

Directors also should set the expectation that management consider if traditional corporate structures, which often isolate various departments, are appropriate for a much more integrated system consistent with the digital age. At least with respect to cybersecurity, leading organizations worldwide are adopting management frameworks that create an enterprise-wide cyber risk management team – not dominated by IT but under the supervision of an executive with enterprise wide perspective such as a Chief Operating Officer, Chief Financial Officer or a Chief Risk Officer. The cyber risk management team also should operate with a separate, and adequate budget to assess and manage cyber risk. One such framework developed by ISA in conjunction with the American National Standards Institute (ANSI) is outlined below.

An Integrated Approach to Cyber Risk Governance

1. Establish ownership of cyber risk on a cross-departmental basis. A senior manager with cross-departmental authority, such as the Chief Information Security Officer, Chief Financial Officer, Chief Risk Officer, or Chief Operating Officer (not the Chief Information Officer), should lead the team.

2. Appoint a cross-organizations cyber-risk management team. All substantial stakeholder departments must be represented, including business unit leaders, legal, internal audit and compliance, finance, HR, IT, and risk management. (See "Roles and Responsibilities of Key Management" excerpt below). A key objective of such a cross-organizational effort is to ensure that there is no cybersecurity weak link or exception within the organization.

3. The cyber-risk team needs to perform a forward-looking, enterprise-wide risk assessment, using a systematic framework that accounts for the complexity of cyber risk; including, but not limited to,

regulatory compliance. This would include assessing the organization's current threat landscape and risk picture. Then, clearly establishing its risk appetite. Identifying potential risk to the organization, as well as its risk threshold, will help the cyber-risk team assess which systematic framework aligns most appropriately with its mission and goals.

4. Be aware that cybersecurity laws and regulations differ significantly across jurisdictions and sectors. As noted in Principle 2, management should dedicate resources to tracking the standards and requirements that apply to the organization, especially as some countries aggressively expand the scope of government involvement in the cybersecurity arena.

5. Take a collaborative approach to developing reports to the board. Executives should be expected to track and report metrics that quantify the business impact of cyber threats and associated risk-management efforts. Evaluation of cyber-risk management effectiveness and the company's cyber-resiliency should be conducted as part of quarterly internal audits and other performance reviews. These reports should strike the right balance between too much detail and what is strategically important to report to the Supervisory Board.

6. Develop and adopt an organization-wide cyber-risk management plan including internal communications strategy across all departments and business units and internal audit and assurance plans. While cybersecurity obviously has a substantial IT (information technology) component, all stakeholders need to be involved in developing the corporate plan and should feel "bought in" to it, including the legal, audit, risk and compliance functions. Testing of the plan should be done on a routine basis.

7. Develop and adopt a total cyber-risk budget with sufficient resources to meet the organization's needs and risk appetite. Resource decisions should take into account the severe shortage of experienced cybersecurity talent and identify what needs can be met in-house versus what can or should be outsourced to third parties. Because cybersecurity is more than IT (or information technology) security, the budget for cybersecurity should not be exclusively tied to one department: examples include allocations in areas such as employee training, tracking legal regulations, public relations, product development, and vendor management. The budget could also include a talent review and succession plan for critical management, such as COO, CTO, CISO, etc. Assessing the readiness of successors and determining if additional training for current employees is needed in order to fulfil these roles in the future or whether outside recruitment of talent is necessary increases the organization's cyber preparedness. By conducting a talent review, an organization can minimize the disruption caused by employee turnover.

Source: *Internet Security Alliance*[1]

[1] *Adapted from Internet Security Alliance and American National Standards Institute, The Financial Management of Cyber Risk: An Implementation Framework for CFOs (Washington, DC: ANSI, 2010). See also Internet Security Alliance, Sophisticated Management of Cyber Risk (Arlington, VA: ISA, 2013).*

PRINCIPLE 5

Board-management discussion about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Total cybersecurity is an unrealistic goal. Cybersecurity is a continuum, not an end state, and security is not the equivalent of compliance. Management teams need to determine where, on a spectrum of risk, they believe the firm's operations and controls can be optimized, in other words, what is the organizations cyber risk appetite (and it cannot be zero – that is unrealistic)

Defining Risk Appetite

"Risk appetite is the amount of risk an organization is willing to accept in pursuit of strategic objectives or what the organization is not willing to accept at all. Risk appetite needs to be high on any board's agenda and is a core consideration of an enterprise-wide risk management approach. Thus, it should define the level of risk at which appropriate actions are needed to reduce risk to an acceptable level. When properly defined and communicated, it drives behavior by setting the boundaries for running the business and capitalizing on opportunities.

"A discussion of risk appetite should address the following questions:

- Corporate values – What risks will we not accept?
- Strategy – What are the risks we need to take?
- Stakeholders – What risks are they willing to bear, and to what level?
- Capacity – What resources are required to manage those risks?

"Risk appetite is a matter of judgement based on each company's specific circumstances and objectives. There is no one-size-fits-all solution."

Source: *PwC, Board oversight of risk: Defining risk appetite in plain English (New York, NY: PwC, 2014), p. 3.*

As with other areas of risk, an organization's cyber-risk tolerance must be consistent with its business strategy and objectives. When an organization analyzes its cyber risk, it ought to do so as part of its overall risk assessment, properly placing cyber in the context of other risks. Security resource allocation is a function of balancing business goals with the inherent risks in digital systems (see "Defining Risk Appetite," page 19). There are multiple cyber risks and multiple methods to address them. Management needs to present the board with a clear picture of the risk landscape and a plan for addressing it. To accomplish this, directors and management teams will need to grapple with the following questions:

- **What data, systems and business operations are we willing to lose or have compromised?** Discussions of risk tolerance will help to identify the level of cyber risk the organization is willing to accept as a practical business consideration. In this context, distinguishing between mission-critical or highly sensitive data (see "Identifying the Company's 'Crown Jewels,' and highly sensitive categories of data" page 9) and other data or systems that are as important, but less essential or sensitive, is a key first step. However, data compromise is not the only component of cyber risk. Legal implications, including regulatory sanctions for data breaches, could exist that far exceed the actual value of the data, and reputational risk from bad publicity may correspond more to external factors than the actual value of the systems compromised.

- **How should cyber-risk mitigation investments be allocated among basic and advanced defenses?** When considering how to address more sophisticated threats, management should place the greatest focus on sophisticated defenses designed to protect the company's most critical data and systems. While most organizations would agree with this in principle, in reality, many organizations apply security measures equally to all data and functions. Boards should encourage management to frame the company's cybersecurity investments in economic terms of ROI, and to reassess ROI regularly. New analytical tools have recently come on the market that can assist management in better defining cyber risk in economic terms and management should consider if these tools are appropriate for their cyber risk calculations. (See Appendix ___ on Economics of Cyber Metrics)

- **What options are available to assist us in mitigating certain cyber risks?** Organizations of all industries and sizes have access to end-to-end solutions that can assist in reducing some portion of cyber risk. They include a battery of preventative measures such as reviews of cybersecurity frameworks and governance practices, employee training, IT security, expert response services and managed security services. Beyond coverage for financial loss, these tools can help to mitigate an organization's risk of suffering property damage and personal injury resulting from a cyber-breach. Some solutions also include access to proactive tools, employee training, IT security, and expert response services, to add another layer of protection and expertise. The inclusion of these value-added services proves even further the importance of moving cybersecurity outside of the IT department into enterprise-wide risk and strategy discussions at both the management and Board levels. However, management needs to keep the board informed of the rapidly changing cyber risk landscape and be agile enough to adjust to quickly changing technologies and cyber-attack scenarios such as data theft, data corruption, and even the use of security mechanisms (e.g. encryption) as attack methods (e.g., ransomware).

- **What options are available to assist us in transferring certain cyber risks?** Cyber insurance exists to provide financial reimbursement for unexpected losses related to cybersecurity incidents. This may include accidental disclosure of data, such as losing an unencrypted laptop, or malicious external attacks, such as phishing schemes, malware infections, or denial-of-service attacks. When choosing a cyber-insurance partner, it is important for an organization to choose a carrier with the breadth of global innovation that best fits the organization's needs. Insurers frequently conduct in-depth reviews of company cybersecurity frameworks during the underwriting process and policy pricing can be a strong signal that helps companies understand their cybersecurity strengths and weaknesses. Many insurers, in partnership with technology companies, law firms, public relations companies and others, also offer access to the preventative measures discussed above. It is important to note, however, that not all Latin American countries have mature insurance markets that will allow transfer of cyber risk through insurance, so organizations should weigh whether cybersecurity insurance is a feasible option in transferring cyber risk.

- **How should we assess the impact of cybersecurity incidents?** Conducting a proper impact assessment can be challenging given the number of factors involved. In an interconnected world, there may be cyber risks to the organization that exist outside the organization's ability to directly mitigate them effectively. For example, publicity about data breaches can substantially complicate the risk evaluation process. Stakeholders (including employees, customers, suppliers, investors, the press, the public, and government agencies) may see little difference between a comparatively small breach and a large and dangerous one. As a result, reputational damage and associated impact (including reactions from the media, investors, and other key stakeholders) may not correspond directly to the size or severity of the event. Indeed, in this age of hyper-transparency, social media, and inaccurate news, the impact of reputation risk resulting from a cyber incident can be sever and disproportionate, and it is incumbent on the board and the c-suite to think about and be prepared for the possible reputation risk associated with a cyber incident.[45] The board should seek assurances that management has carefully thought through these implications in devising organizational strategies for cyber-risk management that include operational IT management, but also include strategies such as legal agreements with partners and vendors helping to ensure appropriate security and a public relations or communication plan to address reputational risk when an event occurs.

APPENDIX A

Assessing the Board's Cybersecurity Culture

A Report from the NACD Blue Ribbon Commission on Board Evaluation defined boardroom culture as "the shared values that underlie and drive board communications, interactions, and decision making. It is the essence of how things really get done."[46]

In the words of one participant:

> *Boards need to change their mindsets. We must move from asking, "What's the likelihood we'll be attacked?" to saying, "It's probable that we've been attacked"; from viewing cybersecurity as a cost to viewing it as an investment that helps us stay competitive; from expecting management to prevent or defend against cyber threats to asking how quickly they can detect and respond to them.*[47] *Additionally, boards need to consider what vulnerabilities exist within their organization that an attacker could exploit, identifying the assets of value and what benefit would be gained from attacking those assets.*

Directors wishing to incorporate a cybersecurity component into their board's self-assessments can use the questions in the table below as a starting point. A rating of 1 is low, a rating of 5 is excellent.

Use the numerical scale to indicate where the Board's culture generally falls on the spectrum shown below. <---------------------------->			Action Item
Our Board mostly thinks of cybersecurity primarily as an IT/Technology issue.	1 2 3 4 5 □ □ □ □ □	Our Board understands cybersecurity as an enterprise wide risk management issue.	
Our Board relies on the legal environment for cybersecurity as largely stable and generally applicable to most companies in the same way.	1 2 3 4 5 □ □ □ □ □	Our Board appreciates the need to regularly seek legal counsel as to an emerging cyber legal landscape tailored to our evolving business plans and environments.	
Our Board does not need regular updating on cybersecurity from industry experts in the field.	1 2 3 4 5 □ □ □ □ □	Our Board regularly seeks cyber expertise relative to our emerging cyber needs and threat picture.	
Our Board does not feel the need for management to provide a specific plan for managing cyber risk.	1 2 3 4 5 □ □ □ □ □	Our Board expects management to provide us with an operational and a management framework that reflects the modern impact of digital technology, and how we are to manage that technology, consistent with our business needs and risks.	
Our Board does not expect management to uniquely assess and manage cyber risks.	1 2 3 4 5 □ □ □ □ □	Our Board expects management to provide us with a clear analysis of what our cyber risks are, which to accept, what we can mitigate, and what we can transfer consistent with our business goals.	

APPENDIX B

Fundamental Questions Directors Should Ask Themselves About Cybersecurity

Even prior to a board meeting, directors may do well to self-assess if they have considered various aspects of cybersecurity beyond the technical and operational aspects. In particular, boards should be thinking of cybersecurity in business terms, and considering if they are preparing their organization on a strategic level. Among the questions directors may want to ask are the following:

1. Does the CEO encourage open dialogue between and among the board, external sources, and management about emerging cyber threats?

2. Are there mechanisms in place to adequately inform family business owners and controlling shareholders who have decision-making powers on the board about the organization's cybersecurity?

3. Who is managing our cybersecurity? Do we have the right talent and clear lines of communication/accountability/responsibility for cybersecurity? Is cyber included in our risk register? [48] What do we consider our most valuable business assets? How does our IT system interact with those assets?

4. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?

5. Do we think there is adequate protection in place if someone wanted to get at or damage our corporate "crown jewels" or other highly sensitive data? What would it take to feel confident that those assets/data were protected?

6. Are we spending wisely on cybersecurity tools and training? Do we know if our spending is cost effective? Are we actually improving security or just completing compliance requirements? What mechanisms are being put in place to train employees on basic cybersecurity topics across the entire enterprise?

7. Have we considered how we would manage our communications in the case of an event, including communicating with the public, our shareholders, our regulators, our rating agencies? Do we have segmented strategies for each of these audiences?

8. Does our organization participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organizations? Should we?

9. Is the organization adequately monitoring current and potential cybersecurity-related legislation and regulation and development of national cybersecurity policies and frameworks?? [49]

10. Is the organization leveraging resources from national CSIRTs to analyze risk and prevent attacks?

11. Is the organization working with peers to share information on cybersecurity threats?

12. Does the company have adequate insurance, including Directors and Officers, that covers cyber events? What exactly is covered?[50] Are there benefits beyond risk transfer to carrying cyber insurance?[51]

APPENDIX C

Questions for the Board to Ask Management About Cybersecurity on Situational Awareness

Principles 4 & 5 in this handbook relate to the board's responsibility to have management provide adequate information to manage cyber risk at the strategic level. In implementing these principles, Board members may choose to ask some of the following questions of management. Cybersecurity questions should not only be raised in the context of an existing breach, but at various points in the business development process. For ease of use, the Handbook breaks down the questions into relevant topics that have cybersecurity implications.

1. What are our critical business services? How do they map to legal entities, regulators' perspectives, IT departments, and suppliers?

2. How are we using IT operations to advance our business goals, and what are the weaknesses in our approach?

3. What are the company's cybersecurity risks, and how is the company managing these risks?[52]

a. Do we have an inventory of IT systems and list of most critical IT systems?
b. Where is the highest risk? Where are we in the replacement of outdated programs?
c. What is our board map to approve these in order to understand age of the systems and when it is time to replace/update?

4. Were we told of cyber-attacks that have already occurred and how severe they were?

5. What is important to protect, and how many times have we seen these assets compromised?

6. Who are our likely adversaries? Are they private hackers or nation-states?

7. In management's opinion, what is the most serious vulnerability related to cybersecurity (including within out IT (and technology) systems, personnel, or processes)?

8. If an adversary wanted to inflict the most damage on our company, how would they go about it?

9. When was the last time we conducted a penetration test or an independent external assessment of our cyber defenses? What were the key findings, and how are we addressing them? What is our maturity level?

10. Do we answer to regulators or external auditors? When would an audit likely occur? What would an audit mean for compliance and risk management?

1**1.** Does our external auditor indicate we have cybersecurity-related deficiencies in the company's internal controls over financial reporting? If so, what are they, and what are we doing to remedy these deficiencies?

12. Have we considered obtaining an independent, third-party assessment of our cybersecurity risk management program?

13. Are we members of information sharing communities? If so, what are the lessons learned from our peers who have experienced breaches?

APPENDIX D

Questions for the Board to Ask Management on Strategy and Operations

1. What are the frameworks we align to, and have you done a gap analysis?

2. Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?

3. Do we have an enterprise-wide, independently budgeted cyber-risk management team? Is the budget adequate? How is it integrated with the overall enterprise risk management process? What kind of strategy decisions have an impact on cyber risk?

4. Do we have a systematic framework, such as the NIST Cybersecurity Framework, the Standards for Data Protection guidelines in place to address cybersecurity and to assure adequate cybersecurity hygiene?

5. Where do management and our IT/Technology teams disagree on cybersecurity?

6. Do the company's outsourced providers and contractors have cybersecurity controls and policies in place? Are those controls monitored? Do those policies align with our company's expectations?

7. What is our insurance coverage for cyber? Is it adequate and what kind do we have? Why do we have that sort of insurance?

8. Is there an ongoing, company-wide awareness and training program established around cybersecurity?

9. What is our strategy to address cloud, BYOD, and supply-chain threats?[53]

10. How are we addressing the security vulnerabilities presented by an increasingly mobile workforce?

11. Are we growing organically or buying companies? Are they mature companies or start-ups? Where are we geographically?

12. How should the board be structured to oversee cybersecurity on an enterprise-wide basis?

APPENDIX E

Questions for the Board to Ask Management About Cybersecurity on Insider Threats

1. How do our operational controls, including access restrictions, encryption, data backups, monitoring of network traffic, etc., help protect against insider threats?

2. How have we adapted our personnel policies, such as background checks, new employee orientation, training related to department/role changes, employee exits, and the like, to incorporate cybersecurity?

3. Do we have an insider-incident activity plan that spells out how and when to contact counsel, law enforcement and/or other authorities, and explore legal remedies?

4. Do we have forensic investigation capabilities?

5. What are the leading practices for combating insider threats, and how do ours differ?

6. How do key functions (IT, HR, Legal, and Compliance) work together and with business units to establish a culture of cyber-risk awareness and personal responsibility for cybersecurity? Considerations include the following:

a. Written policies which cover data, systems, and mobile devices should be required and should cover all employees.
b. Establishment of a safe environment for reporting cyber incidents (including self-reporting of accidental issues).
c. Regular training on how to implement company cybersecurity policies and recognize threats.

7. What are we trying to prevent by protecting against insider threats?

8. What conflicts of interest may exist within organizations that could contribute to a cybersecurity-related insider threat?

APPENDIX F

Questions for the Board to Ask Management About Cybersecurity on Supply Chain

1. What do we currently do and what will need to be done to fully include cybersecurity in our current supply-chain risk management?

2. How much do we know about our supply chain regarding cyber-risk exposure and controls? What due diligence processes do we use to evaluate the adequacy of our suppliers' cybersecurity practices (both during the on-boarding process and during the lifetime of each contract)? Which departments/business units are involved? Are there appropriate contingency arrangements in place in the event of a major problem with critical third-party suppliers?

3. Does the business carry out appropriate strategic monitoring of third-party suppliers?

4. What providers do we use for the Cloud? Which critical business functions have we outsourced to third parties, such as Cloud security?

5. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?

6. How are cybersecurity requirements built into vendor agreements? How are they monitored, and are we doing our due diligence to enforce contracts? Contracts can be written to include minimum cybersecurity requirements, including for example:

a. Written cybersecurity policies.
b. Personnel policies, such as background checks, training, etc.
c. Access controls.
d. Encryption, backup, and recovery policies.
e. Detailed requirements regarding data held by the third party.
    i. Retention and deletion requirements for data held.
    ii. Clear inventories of types of data held.
    iii. Clarity on what is stored, moved, processed, etc.
f. Secondary access to data.
g. Countries where data will be stored.
h. Notification of data breaches or other cyber incidents.
i. Communication plans for incident reporting and response.
j. Incident-response plans.
k. Audits of cybersecurity practices and/or regular certifications of compliance.

7. Do we allow our suppliers to subcontract the delivery of any part of the contract? If so, what level of control/scrutiny do we exercise over the subcontracting arrangements? How do we monitor changes to subcontracting arrangements through the lifetime of the contract?

8. Do we have technology in place to profile suppliers and partners from the cybersecurity point of view to identify potential vulnerabilities and actively manage third party risk?

9. Are we indemnified against security incidents in our supply chain? What is the financial strength of the indemnification?

10. How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?

11. How difficult/costly will it be to enhance monitoring of access points in the supplier networks?

12. Do our vendor agreements bring incremental legal risks or generate additional compliance requirements (e.g., GDPR, FCA, etc.)?

APPENDIX G

Questions for the Board to Ask Management on Planning for a Potential Incident, Crisis Management and Response

1. What is our ability to protect, detect and respond to incidents? How does it compare with others in our sector?

2. In the context of our business, what constitutes a material cybersecurity breach? How does this compare to the definition (if any) included in relevant laws and regulations applicable to our business?

3. At what point is the board informed of an incident? What are the criteria for reporting?

4. What is known about the intent and capability of the attacker? What do we know about how the attacker might use the data?

5. Are we clear as to who must be notified and when? Does law require a notification to regulatory bodies or just affected parties? If so, what are the timetables and strategy considerations for reporting incidents to customers? Regulators/relevant government entities? Law Enforcement? Vendors/partners? Internally? Peers? Investors? What timetables are mandated by laws and regulations and what is at the company's discretion?

6. How will management respond to a cyberattack?[54] Does the company have a validated incident-response plan?[55]Are we adequately exercising our cyber-preparedness and response plan?

7. Do we have a crisis management plan in place? For significant breaches, how good is our communication plan (both internally and externally) as information is obtained regarding the nature and type of breach, the data impacted, and the ramifications to the company and the response plan?[56]

8. What are we doing to avoid making the problem worse for our organization? How do we ensure we have appropriate legal advice in the incident and crisis management teams? Are the legal teams integrated in the incident and crisis plans?

After a Cybersecurity Incident

1. How did we learn about the incident? Were we notified by a third party, or was the incident discovered internally?

2. What do we believe was the motive for the incident? What was the impact, and how do we measure it? Have any of our operations been compromised?

3. Is our cyber-incident/crisis response plan in action, and is it working as planned?

4. What is the response team doing to ensure that the incident is under control and that the attacker no longer has access to our internal network?

5. Is the response team coordinating with national CSIRTs to manage the incident? What mechanisms are in place to collaborate and share information with trusted peers in the private sector and/or government?

6. What were the weaknesses in our system that allowed the incident to occur and why had they not been identified or remediated?

7. Has the security team checked for associated vulnerabilities across all company systems/networks, not just the affected systems or services? Have they checked what happened against the controls framework and made the necessary changes to both security controls and business controls?

8. What steps can we take to make sure this type of event does not happen again? How do we ensure that lessons are learned and remediation actions tracked?

9. What can we do to mitigate any losses caused by the incident?

10. Does the incident alter the risk tolerance of the business? Has this been discussed and have any changes been captured?

Source: *NACD, et al., Cybersecurity: Boardroom Implications (Washington, DC: NACD, 2014) (an NACD white paper).*

APPENDIX H

Cybersecurity Considerations During M&A Phases

Companies involved in transactions are often prime targets for hackers and cybercriminals, because the value of confidential deal-related information is high, and the short timelines, high-pressure environment, and significant workloads associated with transactions can cause key players to act carelessly and potentially make mistakes. Cybersecurity vulnerabilities exploited during a transaction can pose risks to the deal's value and return on investment:

Short-term risks

- Paralyzed operations as a result of ransomware or malware.
- Transaction period might be used by threat actors to gain entry and conduct reconnaissance, an event which often is not detected until well after the deal closes.
- Theft of inside information, including valuations, bids, etc.
- Warranty claims, a change of deal terms, or a reduction in the deal's value.
- Forensic investigations related to a data breach.

Long-term risks

- Exposure to risk from regulatory and other lawsuits.
- Regulatory investigation and penalties.
- Loss of customers, and associated impacts on sales and profit.
- Reputational damage.
- Loss of market share to competitors without a known data breach.

Directors should ask management to conduct a cyber-risk assessment for each phase of the transaction's lifecycle to confirm that systems and processes are secure, and to quantify the risks that may impact the company after the deal closes, including revenues, profits, market value, market share, and brand reputation.

Strategy and Target Identification Phase

The risk of attack starts even before an official offer or merger announcement is made. Law firms, financial advisors, consultants and other associated firms are attractive to hackers because they hold trade secrets and other sensitive information about corporate clients, including details about early-stage deal exploration that could be stolen to inform insider trading or to gain a competitive advantage in deal negotiations. Cyber-attacks on law firms are increasing globally, leading attorneys to label cyber as an "existential threat" to firms.[57] A company therefore needs to have an understanding of the controls and security in place at all of the third parties assisting it during the M&A process and a thorough understanding of how sensitive data is to be shared between parties.

Attackers look for hints that a company is considering a merger, acquisition, or divestiture. They may be tipped off by industry gossip, a slowdown in a company's release cycle, staff reductions, or data leakage through social media channels. There are four primary ways that information is at risk:

- A hacker enters the network through gaps in its defenses, starting with a company's Internet-facing computers.
- A hacker launches a social engineering attack against a company employee.
- Company insiders (employees, contractors, vendors) release sensitive data and information, either intentionally or as a result of negligence. The risk of insider threats heightens significantly in an M&A.
- Information is exposed through vulnerabilities in third-party vendors or service providers.

During this phase, management should gain an understanding of cyber risks associated with the target company and model the impact of those risks to compliance posture, financial forecasts, and potential valuations. Management can perform the following analysis even before direct engagement with the target company begins:

- Conducting "dark web"[58](difficult-to-access websites favored by hackers) searches about the target, their systems, data, and intellectual property. This helps identify whether the company is already on hackers' radar, if systems or credentials are already compromised, and if there is sensitive data for sale or being solicited. Management will need to consider the lawfulness of such searches with reference to the information being accessed.
- Profiling the target company from the cybersecurity point of view, while implementing relevant technology.
- Researching malware infections in the target company and gaps in their defenses visible from the outside. This information is publicly available and can be used to compare one company to another, allowing management to save time and energy by not pursuing companies whose risk profile is unacceptably high.
- Modelling the financial impact of identified cyber risks. These risks may not only impact a company's return on invested capital, but also result in loss of competitive advantages, costly remediation, fines, and possibly years of litigation, depending on what was stolen. An initial estimate of the impact may be material enough to encourage strategy teams to alter a deal trajectory. The estimate can be refined as the transaction process continues and as risks are mitigated.

Due Diligence and Deal Execution Phases

During these phases, the company should perform confirmatory cybersecurity due diligence. Significant problems would call for negotiation of a reduction in purchase price to cover costs of necessary remediation. Depending on the risks identified, the Board may want to defer approving the transaction until remediation is complete or decide to back out of a transaction if the risks that are identified warrant such action. Identification of cybersecurity risks during the diligence phase can be accomplished by performing cybersecurity diligence that is tailored to discover these risks:

- Identify insufficient investments in cybersecurity infrastructure, as well as deficiencies in staff resources, policies, etc.
- Identify lax cultural attitudes toward cyber risk.
- Determine cybersecurity-related terms and conditions (or, the lack thereof) in customer and supplier contracts that have a potential financial impact or result in litigation for noncompliance.
- Discover noncompliance with cyber-related data privacy laws or other applicable regulations and requirements.
- Identify recent data breaches or other cybersecurity incidents.

Effective due diligence on cybersecurity issues demonstrates to investors, regulators, and other stakeholders that management is actively seeking to protect the value and strategic drivers of the transaction, and that they are aiming to lower the risk of a cyber-attack before integration. These risks and upsides can then be factored into the initial price paid and into performance improvement investments that will raise the transaction value, enabling a robust transaction proposal to be presented to shareholders for approval.

Integration Phase

Post-deal integration poses a range of challenges related to people, processes, systems, and culture. Cyber risks add another dimension of complexity and risk to this phase of the transaction. Hackers take advantage of the inconsistencies that exist between the platforms and technology operations of the company and the newly-merged or acquired entity at this phase.

Integration teams need to have the expertise to explore and delve into the smallest of details to identify and mitigate cyber risks such as the following:

- Security gaps identified during preceding phases.
- Prioritization of remediation activities based on potential impact of identified gaps.
- Prioritization of integration activities.
- Employee training on newly integrated systems.

Post-Transaction Value Creation Phase

After a transaction is completed, continued monitoring of cyber risks by management will create numerous opportunities for portfolio improvement and growth.

Management should continue to evaluate the cyber maturity of the merged or acquired entity by benchmarking it against industry standards and competition, just as they do with the core business. Low maturity could impact growth projections and brand reputation due to cyber incidents and possible fines. A breach or compliance issue could cause regulators to investigate, leading to a financial loss or stalling of post-transaction exit plans. Cyber issues can also lead to legal action by customers and suppliers causing value loss and lower returns.

A View from the Sell Side

Many of the same risks impacting the acquiring company that are described herein will of course equally apply to the seller side. In the post transaction valuation creation phase, the seller is particularly exposed to breach disclosures that may impact the deal price / timing and even the ongoing operations of the selling entity if the transaction falls through. Accordingly, a thorough understanding of existing risk vectors prior to deal execution will better inform the nature of warranties made by the selling corporation and reduce exposure.

Information flow to directors of selling companies may be more limited in its nature and frequency as time passes after deal announcement and directors should establish the thresholds and nature for any breach communications in the post announcement period.

Conclusion

Cybersecurity diligence during M&A calls for a two-pronged approach. Companies must conduct rigorous due diligence on the target company's cyber risks and assess their related business impact throughout the deal cycle to protect the transaction's return on investment and the entity's value post-transaction. In addition, all parties involved in the deal process need to be aware of the increased potential for a cyber-attack during the transaction process itself and should diligently maintain their cybersecurity efforts. Applying this two-pronged approach during M&A will serve to ultimately protect stakeholder value.

APPENDIX I

Board-Level Cybersecurity Metrics

Which cybersecurity metrics should be included in a board-level briefing? This question is deceptively simple. Similar to virtually every other division and function within the organization, the cybersecurity function collects and analyses a tremendous volume of data and there is little consensus on which are the critical few pieces of data that should be shared with a board audience. Adding to the challenge is the fact that cybersecurity is a relatively new domain, with standards and benchmarks that are still developing or evolving.

Ultimately, directors will need to work with members of management to define the cybersecurity information, metrics, and other data that is most relevant to them given the organization's operating environment – including industry or sector, regulatory requirements, geographic footprint, and so on. More often than not, Boards see a high volume of operational metrics which provide very little strategic insight on the state of the organization's cybersecurity program. Metrics that are typically presented include statistics such as "number of blocked attacks," "number of unpatched vulnerabilities," and other stand-alone, compliance-oriented measures, that provide little strategic context about the organization's performance and risk position.

As a starting point, directors can apply the same general principles used for other types of Board-level metrics to cybersecurity-related reporting (see Sidebar, "Guiding Principles for Board-Level Metrics").

In addition, the following recommendations provide a starting point for the types of cybersecurity metrics that Board members should consider requesting from management.

1. What is our cyber-risk appetite? This is a fundamental question and one that the Chief Information Security Officer (CISO) should work with the Chief Risk Officer (CRO) function to address. This type of collaboration can produce qualitative and quantitative data points for presentation to the Board that provide context around cyber-risk appetite.

2. What metrics do we have that indicate risk to the company? One organization has implemented a cybersecurity risk "index" which incorporates several individual metrics covering enterprise, supply chain, and consumer-facing risk.

3. How much of our IT/technology budget is being spent on cybersecurity-related activities? How does this compare to our competitors/peers, and/or to other outside benchmarks? These metrics will support conversations about how management determines "how much spending is enough," and whether increasing investments will drive down the organization's residual risk. Additional follow-on questions include these:

- What initiatives were not funded in this year's budget? Why?
- What trade-offs were made?
- Do we have the right resources, including staff and systems, and are they being deployed effectively?

4. How do we measure the effectiveness of our organization's cybersecurity program and how it compares to those of other companies? Board-level metrics should highlight changes, trends and patterns over time, show relative performance, and indicate impact. External penetration-test companies and third-party experts may be able to provide an apples-to-apples comparison within industry sectors.

5. How many data incidents (e.g., exposed sensitive data) has the organization experienced in the last reporting period? These metrics will inform conversations about trends, patterns, and root causes.

6. Value chain relationships typically pose increased risk for companies given the degree of system interconnectivity and data-sharing that is now part of everyday business operations. How do we assess the cyber-risk position of our suppliers, vendors, JV partners, and customers? How do we conduct ongoing monitoring of their risk posture? How many external vendors connect to our network or receive sensitive data from us? This is a borderline operational metric, but it can help support discussions with management about residual risk from third parties. There are service providers within the cybersecurity market place that provide passive and continuous monitoring of companies' cybersecurity postures. A growing number of firms use these services to assess their high-risk third-party relationships as well as their own state of cybersecurity.

7. What operational metrics are routinely tracked and monitored by our security ream? While operational metrics are the domain of the IT/Security team, it would be beneficial for directors to understand the breadth and depth of the company's cybersecurity monitoring activities for the purposes of situational awareness.

8. What metrics do we use to evaluate cybersecurity awareness across the organization? Data about policy compliance, the implementation and completion of training programs, and the like will help to inform conversations about insider risks at various seniority levels and in various regions and divisions.

9. How do we track the individuals or groups that are exempt from major security policies, activity monitoring, etc.? These measures will indicate areas where the company is exposed to additional risk, opening the way for discussions about risk/return trade-offs in this area.

Developing Cyber Economic Metrics

Cyber risk is now accepted as a Board-level conversation. The challenge, however, is how to effectively and precisely communicate the financial impact of cyber incidents to the Board. Before Boards can make informed decisions on how to manage cyber risk, they must first have the ability to translate cybersecurity data into financial metrics. Board directors will need to work with management to outline the most relevant cybersecurity information given the organization's operating environment, including industry or sector, regulatory requirements, geographic footprint, and so on. To get started, the following board-level cyber risk recommendations provide a starting point that Boards should consider requesting from management:

- What are our quarterly expected loss ration metrics related to our cyber-risk condition across our various business units and operating environments?
- What is the financial impact related to our cyber risk worst-case scenario?
- What processes have we established related to making cyber-risk acceptance, cyber-risk remediation, and cyber-risk transfer decisions? How do we measure how these decisions reduce our financial exposure to cyber risk?
- How are we measuring and prioritizing our control-implementation activities and cybersecurity budgets against our financial exposure to cyber risk? Have we connected our control implementation strategy and cybersecurity programs, including budgets, with our cyber-risk transfer strategy?
- Based on our financial performance targets, how can cyber risk impact our financial performance? What is our annual cyber risk expected loss value?
- What is our cyber risk remediation plan to achieve our target expected loss tolerance level? Is our plan producing a net positive financial return?
- How does our cybersecurity program align cyber risk based expected loss ratio analysis and expected loss tolerance targets? How are we measuring, tracking, and demonstrating how our cybersecurity investments are reducing our financial exposure to cyber incidents and delivering cybersecurity return on investment?
- How are we measuring and aligning our cyber risk based expected loss ration analysis and cybersecurity planning with our cyber insurance risk-transfer plan?
- How do we measure the effectiveness of our organization's cybersecurity program and how it compares to those of other companies?

Source: *Secure Systems Innovation Corporation (SSIC) and X-Analytics*

APPENDIX J

Building a relationship with cybersecurity management and the security team

Until recently, the notion of a senior executive whose efforts were dedicated to ensuring the company's cybersecurity was an alien concept to businesses outside of the technology arena. Times have changed; dedicated C-suite managers responsible for controlling digital risk are on the rise in medium- and large-sized companies in many different industries, a consequence of conducting business in today's always-connected world.

According to one study, 54 percent of companies world-wide employ a Chief Information Security Officer (CISO).[59] Another survey found that organizations with CISOs in place were more likely to have dedicated incident-response teams and plans and were more confident about the strength of their company's defenses against threats such as malware.[60] In Latin America, organizations are just beginning to establish CISOs within their organizations. Where there is no CISO, however, there will be a security team that carries the responsibilities for cybersecurity. The key is that the board develops the relationship with those leading on cybersecurity within the organization. It is important to clarify that the role of a CISO and the security team are traditionally not the same. CISO's are usually associated with the information security function as a second line of defense in managing and evaluating information risks, while cybersecurity teams often are the first line of defense in managing IT systems directly.

Building the right relationships between the CISO or equivalent and the board is essential. As corporate information security functions become more mature, a new question has arisen: How does the Board effectively communicate with the security function? The CISO or equivalent is responsible for managing significant operational, reputational, and monetary risk, so a relationship of trust with the Board is essential. Many board members now seek to establish an ongoing relationship with the CISO and include the security executive in discussion about cybersecurity matters at full-board and/or key-committee-level meetings. During these briefings between the CISO and board, it is important that the cyber-risk management team be fully represented before the board to mitigate fears of individual punishment for cybersecurity vulnerabilities.

The questions and guidelines below are designed to assist directors in establishing or enhancing a relationship with the CISO or equivalent. They can also help board members improve their communications with the security team and help boards to gain a better understanding of the company's overall approach to cybersecurity. Because not every question will have relevance for every company, directors should select those that are most appropriate to the issues and circumstances at hand.

1. Understand the Security Team's role and mandate.

- What is the security team's charter and scope of authority in terms of resources, decisions rights, budget, staffing, and access to information? How does this compare to leading practice in our industry and generally?[61]

- How is the organization's cybersecurity budget determined? Comparing this figure with industry spending trends is probably the best way to gain context over the adequacy of funding. What is its size (e.g., percentage of total IT/Technology spending), and how does this figure compare with leading practice in our industry and generally? What role does the security team play in cybersecurity budget allocation and investment decisions? Which security tools or other investments were below the "cut" line in the budget?

- What is the security team's administrative reporting relationship (e.g., CIO, CTO, COO, Head of Corporate Security, other)? Does it differ from the functional reporting relationship? What protocols are in place to ensure that the security team has an independent channel to escalate issues and to provide prompt and full disclosure of cybersecurity deficiencies?[62]

- What role does the security team play in the organization's enterprise risk management (ERM) structure and in the implementation of ERM processes?

- What role, if any, does the security team play beyond setting and enforcing cybersecurity policies and related control systems?

    - For example, does the security team provide input on the development process for new products, services, and systems or on the design of partnership and alliance agreements, etc., such that cybersecurity is "built in" rather than "added on" after the fact?

- Does the security team have the necessary skills, and is the company able to attract and retain the level necessary to be effective?

- How is the division of risk decided? How is company's security posture determined, how is it signed off and how often is it reviewed?

- What are the arrangements in place to be able to scale up the security team in case of a crisis? Do we have the right relationships with suitable third parties?

2.Spending time with the security team before an incident reaps dividends.

- A crisis is the wrong time for directors to get acquainted with the security team and key staff. Board members can arrange to visit the security team and receive orientations first-hand from personnel situated on the front lines of cybersecurity, perhaps scheduled in conjunction with a regular board meeting or site visit. These sessions will provide valuable insights and learning opportunities for board members. The security team will appreciate it, too, since visits like this can increase its visibility, raise morale, and reinforce the need to focus on this area.

- Directors can also ask the security executive for an assessment of their personal cybersecurity situation, including the security of their devices, home networks, etc. These discussions are not only informative for individual directors, but also will help safeguard confidential information Board members receive in the course of their service.

- Many security teams routinely produce internal reports for management and senior leadership on cyber-attack trends and incidents. Directors can discuss with the security team, corporate secretary, and Board leaders whether this information might be relevant and useful to include in Board materials.

- Boards can suggest a quarterly or monthly meeting with the key security personnel to access the current state of security and risk exposure. Boards should understand that security is continuously evolving and changing and, therefore, regular meetings to assess the current state of an organization's risk profile provides insight into what resources are needed and where attention needs to be turned. Boards should also request that a simulation or "table-top exercise" of incident response plans be conducted at least annually.

3. Gain insight into the Security Team's relationship network.

Inside the organization

- How does the information-security team collaborate with other departments and corporate functions on cybersecurity-related matters? For example, does the security team coordinate with:

  - Business development regarding due diligence on acquisition targets and partnership agreements;
  - Internal audit regarding the evaluation and testing of control systems and policies;
  - Human resources on employee training and access protocols;
  - Purchasing and supply chain regarding cybersecurity protocols with vendors, customers, and suppliers; and/or
  - Legal regarding compliance with regulatory and reporting standards related to cybersecurity as well as data privacy?

The security team should be able to articulate how cybersecurity isn't just a technology problem; it's about enabling the company to implement its strategy as securely as possible.

- What support does the security team receive from the CEO, CIO, and senior management team?

- How does the information security team develop and maintain knowledge of the organization's strategic objectives, business model, and operating activities?

  - For example, in companies that are actively pursuing a "big-data" strategy to improve customer and product analytics, to what extent does the security team understand the strategy and contribute to its secure execution?

- What continuing education activities are undertaken by the information security team in order to remain current in cybersecurity matters?

Outside the organization

- Does the information security team participate in cybersecurity information-sharing initiatives (e.g., industry-focused, IT/Technology-community-focused, or public-private partnerships)? How is the information that is gathered from participation in such initiatives used and shared within the organization?

- Does the information security team have relationships with public-sector stakeholders such as law enforcement agencies and regulatory agencies' cybersecurity divisions?

4. Assess performance.

- How is the security team's performance evaluated? How is the information security team's performance evaluated? Who performs these evaluations, and what metrics are used?

- What cybersecurity performance measures and milestones have been established for the organization as a whole? Do we use a risk-based approach that provides a higher level of protection for the organization's most valuable and critical assets?

- To what extent are cyber-risk assessment and management activities integrated into the organization's enterprise-wide risk-management processes? Are we using appropriate cybersecurity to assess cybersecurity hygiene from an organization-wide perspective?

5. Engage the Security Infrastructure in discussion about the "state of the organization."

- What was the organization's most significant cybersecurity incident during the past quarter? How was it discovered? What was our response? How did the speed of detection and recovery compare with that of previous incidents? What lessons did we learn, and how are these factored into the organization's continuous improvement efforts?

- What was our most significant "near miss" on cybersecurity in the past quarter? How was it discovered? What was our response? What lessons did we learn, and how are these factored into the organization's continuous improvement efforts?

- Where have we made the most progress on cybersecurity in the past six months, and to what factor(s) is that progress attributable? Where do our most significant gaps remain, and what is our plan to close those gaps?

Guiding Principles for Presenting to the Board on Cybersecurity

As management works with boards of directors on cybersecurity, it is critical that cybersecurity is properly communicated to the board. To effectively utilize the following appendices, management should keep these characteristics in mind when presenting on cybersecurity to the board:

- Relevant to the audience (full-board; key committee);

- Reader-friendly: Use summaries, callouts, graphics, and other visuals; avoid technical jargon;

- Convey meaning: Communicate insights, not just information;

    - Highlight changes, trends, patterns over time;
    - Show relative performance against peers, against industry averages, against other relevant external indicators, etc. (e.g., maturity assessments);
    - Indicate impact on business operations, costs, market share, etc.;

- Concise: Avoid information overload.

Above all, enable discussion and dialogue.

About the Contributors

The Internet Security Alliance

The Internet Security Alliance (ISA) is an international trade association, founded in 2000, that is focused exclusively on cybersecurity. The ISA Board consists of the primary cybersecurity personnel from international enterprises, representing virtually every sector of the economy. ISA's mission is to integrate economics with advanced technology and government policy to create sustainably secure cyber systems. In 2014, ISA produced the first Cyber-Risk Oversight Handbook, specifically addressing the unique role corporate Boards play in managing cyber risk. In their annual Global Information Security Survey, PricewaterhouseCoopers (PwC) reported that the handbook was being widely adopted by corporate Boards and that its use resulted in better cybersecurity budgeting, better cyber risk management, closer alignment of cybersecurity with overall business goals, and helping to create a culture of security in organizations that use it. For more information about ISA, visit www.isalliance.org.

Endnotes

1. https://www.swiftinstitute.org/wp-content/uploads/2017/10/SIWP-2016-004-Cyber-Threat-Landscape-Carter-Final.pdf
2. https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean
3. https://www.sites.oas.org/cyber/Certs_Web/OAS-Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf
4. https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf?UWqJEbDm.dBKSLEIFTyYs1IxJaExh9Y7
5. World Economic Forum, **"Advancing Cyber Resilience Principles and Tools for Boards"**
6. https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean
7. https://www.oas.org/es/sms/cicte/cipreport.pdf
8. Verizon RISK Team, et al., **2013 Data Breach Investigations Report,** March 2013.
9. https://www.cyberscoop.com/apt-c-36-blind-eagle-colombia/
10. Nicole Perlroth, **"Hackers Lurking in Vents and Soda Machines,"** *the New York Times*, Apr. 7, 2014.
11. Steve Morgan, **"Cyber Crime Costs Projected to Reach $2 Trillion by 2019,"** *Forbes*, Jan. 17, 2016.
12. Ibid.
13. http://aldianews.com/articles/culture/unknown-consequence-latin-americas-tech-boom/55104
14. http://www.seguridadinternacional.es/?q=es/content/cybersecurity-challenges-latin-america
15. https://www.trendmicro.com/en_ae/about/newsroom/press-releases/2015/trend-micro-partners-with-rmeducation-to-bring-worry-free-secur21221111111212.html
16. https://www.symantec.com/security-center/threat-report
17. https://www.threatmetrix.com/info/q1-2018-cybercrime-report/
18. Limor Kessem, **"2016 Cybercrime Reloaded: Our Predictions for the Year Ahead,"** Jan. 15, 2016.
19. FireEye Inc, **Mandiant M-Trends 2016**, p. 4.
20. Kessem, **"2016 Cybercrime Reloaded."**
21. Jeff Goldman, **"48 Percent of Companies Don't Inspect the Cloud for Malware,"** *eSecurity Planet (blog)*, Oct. 12, 2016.
22. Thor Olavsrud, **"Companies complacent about data breach preparedness,"** *CIO*, Oct. 28, 2016.
Eset, Latin American Security Report (2017)
23. http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf
24. Mark Smith, **"Huge rise in hack attacks as cyber-criminals target small business,"** *The Guardian*, Feb. 8, 2016.
25. Estudio del BID
26. AFCEA Cyber Committee, **The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment,** 27. October 2013. See also: Internet Security Alliance, **Sophisticated Management of Cyber Risk** (Arlington, VA: Internet 28. Security Alliance, 2013).
27. AFCEA Cyber Committee, **The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment,** October 2013.
28. https://www.oas.org/es/sms/cicte/cipreport.pdf
29. Internet Security Alliance and American National Standards Institute, The Financial Management of Cyber Risk: An Implementation Framework for CFOs, 2010.
30. NACD, et al., **Cybersecurity: Boardroom Implication** (Washington, DC: NACD, 2014) (an NACD white paper).
31. Ibid. See also: KPMG Audit Committee Institute, Global Boardroom Insights: The Cyber Security Challenge, Mar. 26, 2014.
32. NACD, **Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward** (Washington, DC: NACD, 2009).
33. Adaptado de Robyn Bew, **"Cyber-Risk Oversight: 3 Questions for Directors,"** Ethical Boardroom, Spring 2015.
34. Section 174 Companies Act 2006
35. https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean
36. https://www.lexology.com/library/detail.aspx?g=c0701531-2665-4e4b-a87b-00434e25d55f

37. Regulation (EU) 2016/679 [NB: *This paragraph has been written as if the GDPR is effective. The effective date is May 2018.]*

38. https://www.atkearney.com/documents/783760/869855/Governance+practices+of+Corporate+Boards+in+Latin+America.pdf/f5ae6de9-86e6-9999-8e9d-2fa4cc8e913d?version=1.0

39. NACD, **2016-2017 NACD Public Company Governance Survey** (Washington, DC: NACD, 2016), p. 26.

40. NACD Audit Committee Chair and Risk Oversight Advisory Councils, **Emerging Trends in Cyber-Risk Oversight**, July 17, 2015, p. 1.

41. NACD, et al., **Cybersecurity: Boardrooms Implications** (Washington, DC: NACD, 2014) (an NACD white paper), p. 3.

42. NACD, **2016-2017 NACD Public Company Governance Survey** (Washington, DC: NACD, 2016), p. 28.

43. Ibid.

44. Sean Martin, **"Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's Serious,"** *International Business Times*, April 16, 2014.

45. Andrea Bonime-Blanc. **"Cyber-Reputation: Risk Turbocharged"**. *Ethical Corporation Magazine*. March 2016.

46. Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness (Washington, DC: NACD, 2010), p. 7.

47. Italicized quotations are from participants in the Global Cyber Summit, held Apr. 15-16, 2015, in Washington, DC. Discussions were conducted under the Chatham House Rule.

48. Lexology.com, Ed Batts, DLA Piper LLP, **"Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members,"** Jan. 23, 2014.

49. Ibid.

50. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, **"Board Oversight."**

51. Ibid.

52. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "**Board Oversight."**

53. Lexology.com, Ed Batts, DLA Piper LLP, **"Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members,"** Jan. 23, 2014.

54. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, **"Board Oversight."**

55. Ibid.

56. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, **"Board Oversight."**

57. https://www.law.com/international/2018/04/27/cyberattacks-geopolitical-shocks-and-global-competition-what-keeps-law-firm-leaders-up-at-night-396-2954/?slreturn=20180728162144

58. "The Dark Web" é um termo geral que descreve sites da Internet ocultos que os usuários não podem acessar sem usar um software especial como o TOR ("The Onion Router"). Embora o conteúdo desses sites possa ser acessado, os editores desses sites são ocultados. Os usuários acessam a "Dark Web" com a expectativa de poder compartilhar informações e / ou arquivos com pouco risco de detecção.

59. PwC, **Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016** (New York, NY: PwC, 2015), p. 26, and see Paul Solman, **"Chief information security officers come out from the basement,"** Financial Times, Apr. 29, 2014.

60. Kris Monroe, **"Why are CISOs in such high demand?"** Cyber Experts Blog, Feb. 8, 2016.

61. See, for example, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment (Armonk, NY: IBM Center for Applied Insights, 2014).

62. A 2014 study of global information security issues found that organizations with CISOs reporting outside the CIO's office have less downtime and lower financial losses related to cybersecurity incidents as compared with those who report directly to the CIO. See Bob Bragdon, "Maybe it really does matter who the CISO reports to," The Business Side of Security (blog), June 20, 2014.

ORGANIZATION OF AMERICAN STATES

OAS

More rights for more people

INTERNET
SECURITY
ALLIANCE

CYBER-RISK OVERSIGHT HANDBOOK FOR CORPORATE BOARDS

CYBER-RISK OVERSIGHT HANDBOOK FOR CORPORATE BOARDS