The tradeoff with the segregation of work in a committee is the cost of information asymmetry between committees. This is typically overcome through the mechanism of putting multi-committee directors in place, a practice frequently observed where a technology and cybersecurity committee is present. Commonly, a director working on a technology and cybersecurity committee will share committee assignments with the audit committee, where enterprise risk management oversight responsibilities frequently reside.

It took the Sarbanes-Oxley Act of 2002 to require the creation of an independent audit committee and also mandate that all committee members be financially literate and that at least one be a financial expert. Other committee reforms from SOX introduced a compensation committee and nominating and governance committee. Revisions to the NYSE, NASDAQ listing requirements, and SEC rules followed SOX. These legal reforms introduced a generally accepted committee structure commonly adopted in national codes and adopted by boardrooms around the world. Other committees can also exist on many boards, including risk committees, which are frequently seen on the boards of financial services companies. This practice was driven by regulatory reforms put in place after the financial crisis of 2008.

Charters that define the responsibilities of technology and cybersecurity committees can vary given it is an emerging practice. A model charter has been prepared by reviewing some of the leading practices within U.S. companies that have adopted this committee structure. See Appendix Exhibit 3.

A common existing cyber governance practice is for the audit committee to have responsibility for cyber risk. This is not a recommended practice by U.S. corporate governance leaders Digital Directors Network and the National Association of Corporate Directors for the reasons that it subordinates the cyber risk agenda to the primary financial reporting responsibility of audit committees, and it introduces an inherent competency misalignment between the skills needed to effectively govern cyber risk and the audit and financial expertise that exists on audit committees.

The U.S. SEC's Acting Chief Accountant has also called this practice into question (Munter, 2021):

> Without a doubt, today's audit committees have a lot on their plates. Increasingly, audit committees are being tasked with overseeing a company's cybersecurity policies; environment, social, and governance practices; legal and regulatory compliance; and tax risks. While these are most assuredly important issues, and audit committees may be adept at monitoring these risks, we believe it is important that audit committees assess whether the scope of their responsibilities is appropriate, achievable, and aligned with the experience of its members, and importantly, not lose sight of their core responsibility—oversight of financial reporting, including ICFR, engagement of the independent auditor, and oversight of the external audit process.

Organizational design in the boardroom is a critical tool that directly impacts what corporate directors focus on and how they perform their duties. The leading, albeit emergent, practice of putting a technology and cybersecurity committee on the board reflects the real need for more focused attention to the broad and dynamic agenda that encompasses digital and cybersecurity risk oversight.

3.4 Calculating the Projected Economic Losses From Cyber Risk

The cyber insurance industry and some forward-thinking cyber competent boards and management leaders are starting to understand and project cyber risk in economic terms to govern and manage it like any other financial risk.

With the growing acknowledgment that it is not "if" but "when" a company will experience a data breach or cyber-attack, the issue of whether financial statements should reflect contingent liabilities for cyber losses is also a consideration. At present, international accounting standards and practices do not reflect it in my experience. Under U.S. Generally Accepted Accounting Principles (GAAP), companies are currently required to accrue projected losses if a loss is probable (with a greater than 50% likelihood) and the amount of the loss is estimable. Recognizing contingent losses from uncollectable accounts receivables is

a typical application of this rule. Loan loss reserves, warranties, product liability, litigation, and losses from property damage are others (FASB of the Financial Accounting Foundation, 2010).

The cyber insurance industry is on the front lines of understanding the economic implications of the cyber risks they have underwritten. However, they are struggling with higher-than-expected cyber losses and are raising rates and reducing coverages (Reuters, 2021a). A key regulator of the insurance industry, the New York Department of Financial Services (NY DFS), released their *Cyber Insurance Risk Framework* to address the insurance industry's shortcomings in understanding the cyber risks they are insuring. Their concerns can be seen in the statement, "Many insurers still have work to do to develop a rigorous and data-driven approach to cyber risk, and experts have expressed concerns that insurers are not yet able to accurately measure cyber risk" (New York State Department of Financial Services, 2021).

The rapidly changing nature of cyber risk makes it challenging, but far from impossible, to determine its potential economic impacts. Moreover, only by understanding cyber risk in the same way as other economic risks can well-informed risk mitigation tactics be implemented that address litigation risk, business risk, and equity risk. Cyber economics is emerging as an extension of applied economics to do this. Cyber economics applies traditional economic theory with statistical methods and data elements specific to cyber risks, such as the growing body of historical threat data, cybersecurity intelligence data, and business-specific data with informed logic models and predictions around economic impacts. Potential cyber-related economic losses can and should be determined and monitored over time reflecting both an organization's cyber control environment and their changing threat landscape.

Estimating cyber losses needs to address the primary financial loss drivers of cyber risk that include ransomware, data breaches, business interruptions, and the misappropriation of assets and intellectual property. Detailed cyber economic loss calculations reflect the probability of the inherent cyber risks that face a company adjusted for the strength of its cyber risk controls, including their corporate governance approach to cybersecurity. The inherent cyber risks reflect the economic business

impacts of the unique threat context that faces an organization, including specific industry issues adjusted for the strength of its cyber defense measures and controls. This expected cyber loss or *residual cyber risk* can be monitored and tracked over time, similarly to other potential economic losses. Making this determination can be written as

$$E(Cyber\ Loss) = \Sigma_{i=1}^{7} Residual\ Cyber\ Risk_i * (P) Residual\ Cyber\ Risk_i$$

Cyber Economic Loss Formula Provided by Digital Directors Network and X-Analytics

Once determined and expressed in financial terms, expected cyber loss impacts can be segmented by economic loss type to inform and guide risk management activities such as transfer, mitigation, or acceptance. Once expected cyber losses are contextualized in economic terms, risk management activities can be applied in the context of where financial exposure lies to accommodate corporate board determined thresholds for risk appetite and risk tolerance.

Critical to these estimates is the realization that the organization's vast majority of economic loss from cyber risk is self-insured. Based on author estimates, less than 10 percent of the potential economic losses related to cyber risk have been insured in the United States. Corporate boards will not understand the implications of cyber risk until they begin to understand the potential economic value that is at risk beyond the risk that has been transferred through cyber insurance.

3.5 Governing Systemic Risk in Complex Digital Business Systems

In December of 2020, Collins J. Seitz, the U.S. Delaware Supreme Court Chief Justice, said in an interview that "Boards must be able to demonstrate credibly that they're thinking proactively about potential systemic risks" (Lewis, 2020).

The world is full of complex systems, natural ones such as the planetary system and humanmade ones such as the digital business systems that enable and power most companies. The intrinsic systemic risks within complex systems relate to the observation that complex systems have inherent levels of risk embedded in the very nature of the complex system. These risks are systemic because failure of one part

of a system can trigger "domino effects" or the potential for cascading impacts and more extensive failures throughout the much larger system. The non-linear nature of systemic risk is one of its hallmarks, as is the difficultly of understanding and predicting systemic risk levels and their extended impacts. In complex systems, small events or failures can significantly and negatively impact the more extensive system (Zukis *et al.*, 2022).

In 1986 the U.S. Space Shuttle Challenger exploded shortly after lift-off, killing the seven astronauts on board. The infamous "O-ring" failure in the Challenger's thrust system caused the entire complex system of the shuttle to fail catastrophically. While not related to the Shuttle's digital system, this simple mechanical failure illustrates the principles behind systemic risk. Systemic risk reflects the inherent risks that exist in and between the parts of a complex system that threatens the purpose of the system.

In 2009, as the worst of the global economic crisis known as "The Great Recession" started to recede and research into the crisis led central bankers from around the world to develop the standard known as Basel III. Basel III was intended to mitigate systemic risk in the global banking sector. Focused on strengthening the resilience of individual banks, Basel III addressed the concept of "too big to fail" by studying what contributed to the crisis and building capability that could identify and reduce systemic risk within the banking sector to prevent future economic disasters in the global financial system. Public financial services companies in the U.S. now address and disclose their systemically important role in the capital markets system in regulatory filings.

The global banking industry also now has a much better understanding of systemic risk throughout the global financial system. Global systemically important banks and financial institutions are now identified and monitored by the Financial Stability Board (FSB). The FSB is an international body that works with national financial authorities and standard setters to monitor and make recommendations about the global financial system. Its decisions are not legally binding on its members; they are instead bound by a shared dependency of a well-functioning global financial system (Financial Stability Board, 2020).

There is not yet a similar body focused on the systemic risks inherent throughout the connected digital world. Industry groups and business ecosystems may begin to form similar bodies to help govern and understand systemic risks throughout their extended ecosystems.

COVID-19 is a catastrophic systemic failure of healthcare systems around the world. Systemic risk within healthcare systems and the critical constraint of providing intensive care at scale created cascading problems for the entire healthcare system. As the toll of COVID-19 started to explode at the beginning of the pandemic, the threat of healthcare systems starting to fail become real. Reactions and decisions taken to this risk in healthcare triggered actions that then started a cascade of systemic impacts as risk spread and entered many other complex systems causing damage and disruption to worldwide economic, social, political, and business systems.

Late in 2020, it was discovered that the SolarWinds Orion software product, which manages and optimizes IT environments for thousands of customers and government agencies, had been corrupted and made into a weapon that attackers leveraged to attack SolarWinds client base. The corruption of this critical part of SolarWinds digital business system gave attackers an efficient and systemic way to "piggyback" through a key process that would gain them trusted access into the SolarWinds customer base. This efficiently scaled their attack to create as much damage as possible (Panettieri, 2021).

The hack into Colonial Pipeline's network in 2021, reportedly through the simple vulnerability of a compromised password, caused the largest fuel pipeline in the United States to be shut down barely an hour after the ransomware attack was initiated. Colonial's leadership decided to shut down their pipeline, and later that day, its CEO decided to pay the USD 4.4 million ransomware demand (Turton and Mehrotra, 2021). However, not before the shutdown created systemic damage with fuel shortages and widespread disruption well beyond the controlled shutdown of the pipeline. The CEO decided to pay the ransomware extortion and bring the pipeline back online after admitting the company did not understand the risks related to the hack (Eaton and Volz, 2021). A simple password failure, together with a lack of understanding of the risks that their complex digital business system could carry into

their operating pipelines, created an operating system shutdown that had far-reaching systemic effects that negatively impacted millions of people and businesses.

In situations where systemic risk is not understood in complex systems, leadership generally has two decision paths when the system begins to fail. First, ignore the risk and let the failures and their implications run their course. Second, shut the system down. Political leaders in the United States and worldwide chose both of those two paths as COVID-19 was spiraling out of control in 2020. The U.S. federal government initially chose to ignore the risk, while some states took the other path and shut down most social interactions with stay-at-home orders.

CNA Insurance, a top 10 cyber insurer in the U.S., suffered a ransomware attack in 2021 and reportedly ended up paying USD 40 million in ransom to bring their systems back online (Mehrotra and Turton, 2021). Reports indicated that attackers could have been interested in identifying customers who were insured against cyber risk to identify their terms of coverage (Hope, 2021). This would have allowed attackers to target these customers with a ransomware attack specific to the insurance policy coverages that CNA Insurance had underwritten. However, CNA has disclosed that they do not believe policyholder data was targeted or misused (CNA Financial Corporation, 2021). Attackers who exploit a weakness or leverage point in one part of a complex digital business system to inflict much broader damage across the system reflects the definition of systemic risk.

As defined in the context of digital business systems, a *system* is a "Combination of interacting elements organized to achieve one or more stated purposes" (ISO/IEC/IEEE 15288, 2015, First Edition, p. 9). The interacting elements that compose a digital system include hardware, software, data, humans, processes, procedures, facilities, materials, and naturally occurring entities.

Built-up and evolving over time, digital business systems contain massive amounts of data and collections of disparate and interconnected parts. They are complex because of the rules and regulations that dictate their design and purpose and their dependencies on third parties who are part of the inter-connected system. Moreover, the diverse

skills, practices, and policies needed to manage and secure the system compounds its complexity and increases inherent levels of systemic risk within the system.

The inherent complexity of the modern digital business system is introducing a level of vulnerability and risk that has not previously existed for companies, economies, and societies. Systemic risk exists in many other complex systems built by humankind from healthcare to transportation, to energy. The increasing dependency of each of these systems on complex information systems has intertwined many different types of risks to create an unprecedented level of systemic risk worldwide.

Systemic risk is a new dimension of enterprise risk that most boards and organizations do not yet understand, govern, or manage. Lack of disclosure is one indication of this, as is the emphasis regulators are putting on the cyber insurance industry to understand it. The NY DFS *Cyber Insurance Risk Framework* explicitly addresses systemic risk and the growing risk that these threats introduce to the cyber insurance risk transfer industry (New York State Department of Financial Services, 2021):

> As part of their cyber insurance risk strategy, insurers that offer cyber insurance should regularly evaluate systemic risk and plan for potential losses. Systemic risk has grown in part because institutions increasingly rely on third-party vendors and those vendors are highly concentrated in key areas like cloud services and managed services providers. Insurers should understand the critical third parties used by their insureds and model the effect of a catastrophic cyber event on such critical third parties that may cause simultaneous losses to many of their insureds. Examples of such events could include a self-propagating malware, such as NotPetya, or a supply chain attack, such as the SolarWinds trojan, that infects many institutions at the same time, or a cyber event that disables a major cloud services provider. A catastrophic cyber event could inflict

> tremendous losses on insurers that may jeopardize their financial solvency.

Third-party risk is only one aspect of systemic risk within complex digital business systems. There is also systemic risk inherent throughout the system. Systemic risk can relate to data corruption or failure of a software component in one part of the system that creates risks that spread and degrade the performance of the more extensive system. Systemic risk increases with the integration of information technology and operational technology, introducing widespread risks that can impair foundational business processes and critical infrastructure (Zukis, 2020).

Corporate disclosure of systemic risk also indicates how immature governance and management activities are currently around this issue. While financial services firms address systemic risk in the context of their role in the capital markets due to the regulatory reforms put in place after 2008, systemic risk disclosures in the context of the digital business system are virtually non-existent in the United States. Based upon a review of the risk disclosures of companies in the U.S. R3000 index, Walmart was identified as the only company that makes a comprehensive systemic risk disclosure within the context of their digital business system (author emphasis) (Walmart Inc., 2021, p. 19):

> Our compliance programs, information technology, and enterprise risk management efforts **cannot eliminate all systemic risk.** Disruptions in our systems caused by security breaches or cyberattacks – **including attacks on those parties we do business with** – could harm our ability to conduct our operations, which may have a material effect on us, may result in losses that could have a material adverse effect on our financial position or results of operations, or may have a **cascading effect that adversely impacts our partners, third-party service providers, customers, financial services firms, and other third parties that we interact with on a regular basis.**
>
> In addition, such security-related events could be widely publicized and could materially adversely affect our reputation with our customers, members, associates, vendors

> and shareholders, **could harm our competitive position particularly with respect to our eCommerce operations, and could result in a material reduction in our net sales in our eCommerce operations, as well as in our stores thereby materially adversely affecting our operations, net sales, results of operations, financial position, cash flows and liquidity.** Such events could also result in the release to the public of confidential information about our operations and financial position and performance and could result in **litigation** or other legal actions against us or the imposition of penalties, fines, fees or liabilities, **which may not be covered by our insurance policies**. Moreover, a security compromise or ransomware event could require us to **devote significant management resources** to address the problems created by the issue and to **expend significant additional resources** to upgrade further the security measures we employ to guard personal and confidential information against cyberattacks and other attempts to access or otherwise compromise such information and could result in a disruption of our operations, particularly our digital operations.

This disclosure reflects the foundational inability of Walmart to completely eliminate systemic risk and its material and far-reaching impacts. Along with addressing multiple business risks, the disclosure also addresses litigation risk and Walmart's self-insured exposure to these risks.

Investor disclosures are a potential useful indicator of how well boards and companies understand systemic risk and its implications for business, litigation, and equity risk. Accurate and meaningful disclosure is an expectation and requirement to protect investor interests in public companies and is a foundation of public capital markets worldwide.

The work done after "The Great Recession" to understand systemic risk in capital markets and the complex inter-connected financial industry demonstrates that it is possible to understand and mitigate systemic risk. This work now needs to expand into other domains beyond the

financial system. All of our humanmade systems constantly evolve to serve a changing and growing collection of needs and wants and the systemic risks inherent within them will also continue to evolve and grow alongside this evolution.

Incident disclosure practices also remain inconsistent as several SEC enforcement actions and fines in the United States have identified weaknesses in cyber incident disclosure controls (Patterson Balknap Webb and Tyler, LLP., 2021). Rapid disclosure of incidents is also a tactic in mitigating systemic cyber risk. The SEC wants companies to provide cybersecurity disclosures that are specific to the organization. They do not want generic disclosure, but they acknowledge the need to walk the fine line of providing a "roadmap" that could make the company more susceptible to a cybersecurity incident. The 2018 SEC guidance also explicitly requests U.S. public companies to consider the range of harm that could be caused to customers and suppliers in determining materiality, i.e., systemic impact. In August 2021, Pearson plc (NYSE: PSO), a UK company that trades on the London Stock Exchange and also lists its American Depository Receipts on the New York Stock Exchange, settled charges for US$ 1 million that it misled investors related to a 2018 cyber intrusion involving the theft of millions of student data records (U.S. Securities and Exchange Commission, 2022a).

Some companies are doing a much better job on cyber risk disclosure than others. FedEx (NYSE: FDX), a company that receives an "A" grading on their boardroom digital and cybersecurity policies and practices (Digital Directors Network, 2021b), made the following cybersecurity-related Form 10-K disclosure for their fiscal year ended May 31, 2021 (FedEx Corporation, 2022):

> **A significant data breach or other disruption to our technology infrastructure could disrupt our operations and result in the loss of critical confidential information, adversely impacting our reputation, business or results of operations.**
>
> Our ability to attract and retain customers, to efficiently operate our businesses, and to compete effectively depends in

part upon the sophistication, security and reliability of our technology network, including our ability to provide features of service that are important to our customers, to protect our confidential business information and the information provided by our customers, and to maintain customer confidence in our ability to protect our systems and to provide services consistent with their expectations. For example, we rely on information technology to receive package level information in advance of physical receipt of packages, to track items that move through our delivery systems, to efficiently plan deliveries, to execute billing processes, and to track and report financial and operational data. We are subject to risks imposed by data breaches and operational disruptions, including through cyberattack or cyber-intrusion, including by computer hackers, foreign governments, cyber terrorists, cyber criminals and malicious employees or other insiders of FedEx or third-party service providers. Data breaches of companies and governments have increased in recent years as the number, intensity and sophistication of attempted attacks and intrusions from around the world have increased and we, our customers and third parties increasingly store and transmit data by means of connected information technology systems. Additionally, risks such as code anomalies, "Acts of God," transitional challenges in migrating operating company functionality to our FedEx enterprise automation platforms, data leakage, cyber-fraud and human error pose a direct threat to our products, services, systems and data and could result in unauthorized or block legitimate access to sensitive or confidential data regarding our operations, customers, employees and suppliers, including personal information.

The technology infrastructure of acquired businesses, as well as their practices related to the use and maintenance of data, could also present issues that we were not able to identify prior to the acquisition. See "Failure to successfully

implement our business strategy and effectively respond to changes in market dynamics and customer preferences will cause our future financial results to suffer." below for additional information on risks related to our recent acquisition of ShopRunner and launch of FedEx Dataworks.

We also depend on and interact with the technology and systems of third parties, including our customers and third-party service providers such as cloud service providers and delivery services. Such third parties may host, process or have access to information we maintain about our company, customers, employees and vendors or operate systems that are critical to our business operations and services. Like us, these third parties are subject to risks imposed by data breaches, cyberattacks and other events or actions that could damage, disrupt or close down their networks or systems. We have security processes, protocols and standards in place, including contractual provisions requiring such security measures, that are applicable to such third parties and are designed to protect information that is held by them, or to which they have access, as a result of their engagements with us. Nevertheless, a cyberattack could defeat one or more of such third parties' security measures, allowing an attacker to obtain information about our company, customers, employees and vendors or disrupt our operations. These third parties may also experience operational disruptions or human error that could result in unauthorized access to sensitive or confidential data regarding our operations, customers, employees and suppliers, including personal information.

A disruption to our complex, global technology infrastructure, including those impacting our computer systems and websites, could result in the loss of confidential business or customer information, require substantial repairs or replacements, resulting in significant costs, and lead to the temporary or permanent transfer by customers of some or

all of their business to our competitors. The foregoing could harm our reputation and adversely impact our operations, customer service and results of operations. Additionally, a security breach could require us to devote significant management resources to address the problems created. These types of adverse impacts could also occur in the event the confidentiality, integrity or availability of company and customer information was compromised due to a data loss by FedEx or a trusted third party. We or the third parties with which we share information may not discover any security breach and loss of information for a significant period of time after the security breach occurs.

We have invested and continue to invest in technology security initiatives, information-technology risk management, business continuity and disaster recovery plans, including investments to retire and replace end-of-life systems. The development and maintenance of these measures is costly and requires ongoing monitoring and updating as technologies change and efforts to overcome security measures become increasingly more frequent, intense and sophisticated. Despite our efforts, we are not fully insulated from data breaches, technology disruptions, data loss and cyber-fraud, which could adversely impact our competitiveness and results of operations. For instance, in 2017 TNT Express worldwide operations were significantly affected due to the infiltration of an information-technology virus known as NotPetya. In 2017 FedEx was one of many companies attacked by the rapidly spreading ransomware described as WannaCry that exploited vulnerability in a third-party software program and infected computers using that program, encrypting files and holding them for ransom. During 2018, we discovered an unsecured server hosted by one of our third-party cloud service providers, which exposed some archived account information related to a service discontinued after our 2015 acquisition of Bongo International, LLC. The server has

> been secured, and we have found no indication that any information has been misappropriated in connection with the incident. Additionally, we have experienced continual attempts by cyber criminals, some of which were successful, to gain access to customer accounts for the purposes of fraudulently diverting and misappropriating items being transported in our network. None of the WannaCry ransomware attack, unsecured server or fraudulent cyber activities caused a material disruption to our systems or resulted in any material costs to FedEx.
>
> While we have significant security processes and initiatives in place, we may be unable to detect or prevent a breach or disruption in the future. Additionally, while we have insurance coverage designed to address certain aspects of cyber risks in place, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise. See "Our business is subject to complex and evolving U.S. and foreign laws and regulations regarding data protection." below for additional information on risks related to legal and regulatory developments with respect to data protection.

This comprehensive cyber risk disclosure reflects digital issues specific to FedEx, along with the vital role their digital business system has throughout their business. The FedEx disclosure explicitly addresses issues in systemic risk along with the inherited cyber risks related to acquisitions. This is a lesson they learned when they suffered a ransomware attack during 2017 in their TNT Dutch subsidiary, an acquisition they made the year before. As a result of the attack, they disclosed USD 300 million in operational impacts along with the fact that they did not have cyber insurance at the time. They now disclose that they have cyber insurance in this recent disclosure.

In addition to this comprehensive disclosure, the FedEx board organizes digital and cybersecurity risk oversight through a Cyber and Technology Oversight Committee with a comprehensive charter applied by four self-reported digitally savvy directors who they believe bring

deep and broad digital expertise and experience to the FedEx boardroom. The former chair of this committee at FedEx, John Inglis, was appointed as the first U.S. National Cyber Director by President Joe Biden and advises the President on cybersecurity policy and strategy (The White House, 2022).

FedEx's leading self-regulatory approach to digital and cyber risk is an exception. Similar policies and practices are observed elsewhere and are addressed in the next section. Collectively, these leading practices offer a blueprint that regulators and any corporate board can follow to rapidly advance digital and cyber risk oversight.

4

Self-Regulation: National Codes and Other Standards

The explicit reference to digital or cyber risk or specific governance expectations in national codes worldwide is the rare exception, not the rule. Where digital and cybersecurity governance practices are in place in the boardroom, they are being implemented voluntarily by progressive boards innovating into the issues as they learn from and create leading practices along the way. This self-regulated approach has not created broad based boardroom transformation in digital and cyber risk oversight. Legal requirements such as corporate laws, listing requirements, or other "hard law" directives that impose specific digital and cybersecurity governance requirements on boardrooms and corporate directors are not yet common.

However, some of the self-regulating digital and cyber governance standards and codes that do exist are fairly comprehensive and some have existed for a relatively long time. Along with these voluntary standards, a collection of common leading practices is starting to emerge. Together, these precedents offer a roadmap for the development of digital and cybersecurity governance policies and practices.

This section explores these voluntary standards and highlights the developing nature of regulatory views in several economies worldwide. Not intended to be a comprehensive review of all legal and regulatory

jurisdictions, this analysis identifies key pieces to the puzzle to create a mosaic of how digital and cybersecurity governance is evolving, and can further develop worldwide.

While broad based global regulatory reform in digital and cybersecurity governance is not yet happening, there is a rapidly expanding amount of legislation already imposing data privacy and cybersecurity rules onto management teams and their organizations. These laws are being implemented to hold corporations to new levels of digital and data accountability and codify citizens' rights around their data. The Global Data Protection Regulation (GDPR) was adopted in 2016 by the European Union and has served as a model for many other data protection regulations worldwide, such as the California Consumer Privacy Act (CCPA). CCPA went into effect in 2020. Over €1.6 billion of fines have been levied under GDPR through April 2022 (CMS Law, 2022).

China's Personal Information Protection Law (PIPL) went into effect on November 1, 2021. It imposed far-reaching requirements and significant penalties of up to 5% of annual revenue on information processors within and without China (Dezan Shira & Associates, 2021). The law also provides for individual liability and requires information processors to conduct compliance audits and impact assessments. China's Data Security Law (DSL) went into effect in September of 2021 and introduced new rules for any company operating in China on how they process and protect data. The DSL also introduced new civil and criminal penalties for noncompliance (Jones Day, 2021).

While most of these laws do not directly enact or create corporate governance reforms, they all impact the responsibilities of the board and corporate directors to understand and govern how their companies comply with the laws and address these issues. Global regulators have recognized that digital and cybersecurity issues have implications that are in the interests of the public, investors, the economy, and national security.

With the slow pace of digital and cyber governance reform the boardroom is lagging the national strategies that are being established around the world to create long-term sustainable digital economies. These initiatives require private-sector leadership, involvement, and

support in order for digital economies to emerge and thrive sustainably. This is causing the gap to expand between the boardroom's ability to govern digital and cyber risk and the real market, litigation and business risks facing organizations and management teams as a result of their digital business systems.

Leaving digital and cybersecurity governance reform up to voluntary self-regulated transformation will mean that the pace of change remains slow, guaranteeing that the gap between effective governance and risk will continue to grow. Given what is at stake, the author believes there needs to be more corporate governance focused legal and regulatory reform to rapidly advance boardroom transformation and close this gap. Policy recommendations in Section 5 reflect a range of suggested "hard" and "soft" corporate governance reforms for regulators and corporate boards worldwide.

National codes and standards in digital and cybersecurity governance can vary widely, and the development of the guidance so far is fairly arbitrary. The adoption of leading digital governance policies and practices in the boardroom is equally irregular. However, the national codes that do explicitly address digital and cybersecurity governance can provide insight to any corporate director to consider in the context of their own boardroom. By viewing these practices and policies as leading practices to be learned from, corporate directors have the ability to self-regulate and materially improve their approach to governing these issues.

The following analysis is not intended to be an inventory of every explicit digital or cyber requirement or reference in the many national corporate governance codes or laws that exist around the world. These observations highlight and illustrate the main trends in director skills, boardroom structure, and scope of risk disclosure from a collection of nations who are on a faster track towards corporate governance reform in these areas.

4.1 Australia

Recognized as the world's first ICT-focused corporate governance standard, *AS8015 Corporate Governance of Information and Communication*

Technology formalized the first structured governance approach to help corporate directors govern information technology when it was published in 2005.

AS8015 was intended to be a universal standard for public and private companies, government entities, and not-for-profits regardless of size. Widely acclaimed, *AS8015* would go on to be the blueprint that was adopted by the International Organization for Standardization (ISO) as *ISO/IEC 38500* in May 2008. A second edition was published in 2015. *AS8015* now aligns with the ISO standard. This leading practice standard, *ISO/IEC 38500:2015* represents one of the most mature and comprehensive ICT governance standards worldwide. The standard is currently being reviewed as part of ISO's regular five-year review cycle. Details of some of its features are addressed in Section 4.7.

4.2 Japan

Changes to Japan's Corporate Governance Code have been made as a result of the Tokyo Stock Exchange's (TSE) market segmentation initiative which was implemented on April 4, 2022. Reorganizing into three market segments; Prime Market, Standard Market, and Growth Market, companies wishing to be listed in the TSE's Prime Market segment have now had to strengthen their corporate governance policies and practices. The goal behind the stock exchange reorganization and the commensurate raising of corporate governance standards is for Japanese companies to better meet the needs of global institutional investors (Institutional Investor, 2021).

Guidelines for "Investor and Company Engagement" under Japan's Corporate Governance Code now include explicit expectations on digital and cybersecurity. The following revision has been included within the supplemental investor engagement guidelines under the category of "Management Decisions in Response to Changes in the Business Environment" (author emphasis) (Revisions of Japan's Corporate Governance Code and Guidelines for Investor and Company Engagement, (2021)):

> Does the company appropriately respond to changes in the environment surrounding the business, such as increasing social demand for and interest in [Environmental, Social and Governance] ESG and [Sustainable Development Goals] SDGs, **progress in digital transformation, the need to address cyber security**, and the need for fair and appropriate transactions throughout the supply chain in its management strategies and plans? Further, does the company have a structure in place, such as the establishment of a committee on sustainability under the board or the management side, to review and promote sustainability-related initiatives on an enterprise-wide basis? [Provisional Translation]

The Japanese Code follows the "comply or explain" principle to drive thoughtful governance around oversight. While not prescriptive in requiring structured corporate governance reform in digital and cyber risk oversight, the Japanese Code nonetheless is directed towards greater investor engagement and disclosure in the company's path towards safely shaping their digital future. Engaging investors on both digital transformation and cyber risk is a strong leading worldwide practice in corporate governance.

4.3 Malaysia

The *Malaysian Code On Corporate Governance (MCCG)* was updated in April 2021 and included several explicit references to cyber risk governance including recommending a risk management committee that includes cyber security within its scope (author emphasis) (Securities Commission Malaysia, 2021):

> The board should, in its disclosure, include a discussion on how key risk areas such as finance, operations, regulatory compliance, reputation, **cyber security** and sustainability were evaluated and the controls in place to mitigate or manage those risks. In addition, it should state if the risk

> management framework adopted by the company is based on an internationally recognised risk management framework.

The MCCG also recommends that "good cyber hygiene practices are in place including data privacy and security to prevent cyber threats" along with the suggestion for listed companies to leverage technology to facilitate voting and remote shareholder participation. The MCCG notably moves cyber security out from underneath the audit committee with the risk committee alignment and guidance on how cyber risk management should be governed and managed.

Notably, the Malaysian code is not based on the "comply or explain" principle common in many other countries. It adopts the CARE principle, or Comprehend, Apply and Report, an "apply or explain an alternative" principle. Instead of explaining the reasons for non-compliance, CARE is intended to identify the thought processes and provide a meaningful explanation for the corporate governance practices utilized.

In addition to the MCCG recommending that boards of listed companies adopt a risk management committee it encourages private companies to follow the code. Governing information security risk in a risk management committee, and assuming the committee members have the requisite cyber competencies to understand these issues, would allow for more focus and better alignment than the common worldwide practice of tasking cyber risk to an audit committee.

Malaysia's largest bank and one of its most prominent companies, Maybank (Malayan Banking Berhad), does just that. In their disclosures under the MCCG that describe their Risk Management Committee's (RMC) responsibility, they disclose, "The RMC is responsible for formulating policies and frameworks to identify, measure, monitor, manage and control the material risk components impacting the businesses including IT-related risk" (Malayan Banking Berhad, 2020, p. 52). The Maybank board has 12 directors and six RMC members. The RMC held ten meetings during the year with 100% attendance.

Specific training and education course/event disclosures are also made for each director during the year. Four directors attended cyber-specific training events, including the chairman. Course or event disclosures include: "Cybercrime," "Cybersecurity & Work-From-Home

Security Challenges Amidst COVID-19 Pandemic," "Cybersecurity Challenges & Response," and "Cyber Security in the Boardroom."

Disclosing corporate directors' specific actions to remain current and informed is not a commonly observed disclosure practice. However, the disclosure of director training, including cybersecurity courses alongside the stated governance responsibility within the committee charter for "IT-related risk," are leading practices in a digital and cybersecurity governance system to demonstrate the efforts corporate directors are making to understand and effectively govern issues relevant to the company.

4.4 Nigeria

The *Nigerian Code of Corporate Governance 2018 (NCCG)* adopts an "apply and explain" principle to its standards. In the overall charter for the board, the NCCG plainly states that the board's responsibilities include "providing oversight of Information Technology governance" (Financial Reporting Council of Nigeria, 2018, Section 1.10).

The Code makes a strong recommendation that the Board should consider a risk management committee and within this committee, the Code explicitly addresses the oversight of information technology, both its upsides and downsides within the scope of this committee's mandate. Where a risk committee and audit committee both exist, the Code recommends at least one multi-committee director to reduce information asymmetries between these two committees.

The Code also requires the chair of the risk committee to be a non-executive director and a requirement to meet at least twice per year. The Code recommends alignment with business strategy, the performance of IT, third-party risk, and cyber threats as core boardroom oversight areas. The Code also requires periodic independent assessment of the company's IT activities. Recommendations for this committee include (Financial Reporting Council of Nigeria, 2018, Section 11.5.6.6):

> Review and recommend for approval of the Board, at least annually, the Company's Information Technology (IT) data

> governance framework to ensure that IT data risks are adequately mitigated and relevant assets are managed effectively. The framework may include:
>
> (1) (a) Development of IT strategy and policy;
> (2) (b) Proactive monitoring and management of cyber threats and attacks as well as adverse social media incidents;
> (3) (c) Management of risks relating to third-party and outsourced IT service providers;
> (4) (d) Assessment of value delivered to the Company through investments in IT; and
> (5) (e) Periodic independent assurance on the effectiveness of the Company's IT arrangements.

Guaranty Trust Bank, Nigeria's largest company with almost US$ 2.5 billion in revenue, has a Board Risk Management Committee tasked with a wide range of risks, including credit risk, reputational risk, operations risk, technology risk, market risk and liquidity risk.

However, they also have a Board Information Technology Strategy Committee to bring even more focus to the governance of the specific digital issues and risks impacting the bank. With seven committee members, it met twice during the year ended December 31, 2020. Three of these committee members are multi-committee directors with their Board Risk Management Committee. They also disclose in their annual report that they provide training for all staff that includes cybersecurity and corporate governance.

The scope of responsibility for this dedicated IT committee is disclosed as (Guaranty Trust Bank plc., 2021, p. 18):

> The Board Information Technology Strategy Committee is responsible for the provision of strategic guidance to Management on Information Technology issues and monitoring the effectiveness and efficiency of Information Technology within the Bank and the adequacy of controls.

> The Terms of Reference of the Board Information Technology Strategy Committee include:
>
> - Provide advice on the strategic direction of Information Technology issues in the Bank;
> - Inform and advise the Board on important Information Technology issues in the Bank;
> - Monitor overall Information Technology performance and practices in the Bank.

Guaranty Trust Bank plc also makes a specific systemic risk management disclosure statement in their annual report. While not uncommon to be mentioned in financial services firm disclosure statements in the context of a bank's systemic role within capital markets, Guaranty Trust Bank also references cyber risk within the overall statement on systemic risk management:

> **Systemic risk management:** The Bank's Enterprise Risk Management (ERM) division works with relevant units in the bank in managing risks in our business operations and activities. There are several risk management units in charge of managing different risks such as environmental and social, credit, operational, reputational, market, legal, cyber risks, among others (p. 37).

Guaranty Trust Bank's digital and cybersecurity governance practices go beyond the national code. A dedicated Board Information Technology Strategy Committee reflects a leading worldwide practice in digital and cybersecurity risk oversight.

4.5 South Africa

The *King IV Report on Corporate Governance for South Africa (King IV Report)* replaced King III in its entirety in 2016. King IV, like many national codes, is a voluntary set of principles and leading practices. It offers a progressive and comprehensive standard around ICT governance and is one of the world's most comprehensive standards in this regard.

King IV is a leading national framework in ICT, and its ICT governance elements were first introduced with King III in 2009. As a mature and comprehensive ICT standard, it is well integrated within the broader general corporate governance principles of South Africa. King IV presents a clear case for technology and information governance that is being driven by "advances in data analytics, the Internet of things, robotics, artificial intelligence, 3D printing, nanotechnology, and biotechnology and their profound impacts on supply chains, industries, and business models" (Institute of Directors In Southern Africa NPC, 2016).

Within King, IV is the declaration that "Technology is now part of the corporate DNA. Thus, the security of information systems has become critical. Technology governance and security should become another recurring item on the governing body's agenda" (p. 10). This statement articulates the importance of, and urgent need for corporate governance reform in digital and cybersecurity governance policies and practices around the world.

King IV made a shift from the principle of "apply or explain" to "apply and explain." This shift requires more thoughtful corporate governance from directors and brings greater transparency to the board's thinking in applying the King IV principles and practices. The core King IV technology and information governance principle includes eight recommended practices. These cover boardroom accountability, a wide range of specific oversight responsibilities, outcomes related to information architecture, privacy and security, and emerging technology. The board receiving independent assurance on the organization's technology and information effectiveness and disclosure of overview practices, incidents, performance assessments, and future plans are also recommendations. King IV also covers critical digital governance responsibilities in business resilience, third-party risk, the integrated system of people, process and technology, technology ethics, return on investments, and technology disposal. This suggested depth and breadth of information technology oversight stands out amongst countries worldwide.

As an outcome-focused set of principles, several specific tactics related to digital and cybersecurity governance were rejected during public commentary for King IV. During the public comment period

for King IV, it was suggested that King IV be more prescriptive in requiring information and communication technology competencies in board composition. The King Committee rejected this as too prescriptive and broad to implement because it could potentially introduce an infinite set of specialist skills to be considered. Instead, King IV leaves this issue up to the governing body to determine the requisite ICT skills required on the board.

It was also suggested that King IV should recommend an IT Committee. Again, this was not incorporated into the code to be consistent with the fact that King IV is generally non-prescriptive in any committee recommendations, once again leaving this up to the governing body on a needs basis (Institute of Directors Sourthern Africa KING IV, 2016).

Shoprite, one of South Africa's largest public companies and Africa's largest fast-moving consumer goods retailer, prepares a comprehensive King IV compliance report. They also prepare an annual report filed according to the rules of the Johannesburg Stock Exchange. They have identified information and technology as the fourth most material issue facing the company. They disclose several specific upside and downside issues that are driving the materiality of these risks to their business as well as enhancements to their IT governance (Shoprite Holdings Ltd., 2020, p. 45):

> Continued investment in technology and data analysis remains a priority as the Group strategically positions itself for optimising the business to create new opportunities and grow into new markets. The initial disruptions caused by the implementation of the integrated ERP system in FY 2019 have been addressed. The system has led to significant improvements in operational efficiency, enhanced customer insight and data analytics, and the ability to roll out technology-based initiatives at scale and on demand. This is shown in certain brands being able to target new market segments and the use of real-time inventory data to optimise and manage stock levels. Greater emphasis has

> been placed on our IT governance – with a focus on data security and privacy – to provide appropriate and sustainable IT governance.

Their disclosure of the significant business risks that accompany a large-scale digital systems project, such as enterprise resource planning (ERP) system implementation is notable. In describing the information technology and cyber risks that Shoprite is facing, their annual report also makes the following disclosure:

> IT and cyber risk includes any threat to Shoprite's business data, critical systems and business processes associated with the adoption of, operation, ownership and use of information technology. This risk includes compromised business data due to unauthorised access or use, failure to protect data and prevent cyberattacks, an inability to access IT systems needed for business operations, and reduced productivity due to slow or delayed access to IT systems (p. 49).

As a somewhat generic statement, this risk disclosure does not address outbound or inbound systemic risks. According to their King IV report, Shoprite tasks their Audit and Risk Committee (ARC) with IT governance. The ARC charter explicitly addresses their responsibilities related to IT governance. Moreover, the ARC requires that at least one-third of its members have expertise or experience in information technology and information systems, amongst other skills. They have three committee members on their ARC for an eight-person board. However, director skill disclosures in information technology or information systems are not present, including cybersecurity competencies, training, or education.

The ARC committee monitors and evaluates significant IT investments at every meeting, reviews IT risks including disaster recovery, monitors asset management, system availability, global data leakage prevention, and legal and regulatory compliance issues according to their King IV compliance report (Shoprite Holdings Ltd., 2020).

Shoprite's disclosures reflect the positive impact that a comprehensive "self-regulated" national code such as King IV can have to drive precise levels of boardroom accountability and breadth and depth around

digital and cybersecurity risk oversight. However, observed gaps in director expertise and experience in information management and information systems fall short of global leading practices, suggesting potential weaknesses in the application of their digital and cybersecurity oversight policies. But generally, both KING IV and Shoprite's digital and cybersecurity governance policies and practices are significantly more mature than most standards or practices for companies around the world.

4.6 The United States

The United States is a corporate governance laggard in many respects in digital and cybersecurity risk oversight. That might be about to change as proposed SEC rules would significantly change how U.S. public company boardrooms govern these issues.

As the most cyber-attacked country in the world, the United States national cyber and corporate weaknesses are no secret to attackers (Ang, 2021). Regulatory mandates in cyber governance or the widespread adoption of voluntary codes or other leading practices within most U.S. boardrooms lags the reality of this risk environment. Recently suggested SEC legal reforms could change this quickly.

A small body of leading digital and cyber governance practices is however emerging from a few well-known U.S. companies. These boardroom policies are mature enough to be assessed and graded to document a standard in digital and cyber risk governance that other boardrooms can learn from (Table 4.1). Several leaders and their reported grades include:

Table 4.1: Digital and cybersecurity governance grades determined by qualitative assessment of boardroom skills, structure and scope of risk disclosure by Digital Directors Network

Company	Card Grade
Citrix, Inc. (NASDAQ: CTXS)	A
FedEx, Inc. (NYSE: FDX)	A
GM, Inc. (NYSE: GM)	B+
HealthEquity, Inc. (NASDAQ: HQY)	B+
Hasbro, Inc. (NASDAQ: HAS)	B

Source: Digital Directors Network (2021b).

The boardroom policies and practices of these companies reflect a system of digital and cybersecurity risk oversight that starts with corporate directors who have both breadth and depth in digital expertise. These boards also organize their digital governance activities with a technology and/or cybersecurity committee, and they make comprehensive disclosures on digital and cybersecurity risk. Grades are determined by applying the DiRECTOR framework in Appendix Exhibit 2 using qualitative data analysis techniques to assess relevant publicly available information (Zukis, 2021b). These self-regulated U.S. reforms mirror some of the leading practices identified in national codes and applied by companies in Malaysia and Nigeria.

The SEC is also ramping up its focus on accountability and has issued several enforcement actions related to cyber incident disclosure (Ferrillo *et al.*, 2021). Relying upon regulators and courts to establish standards after the fact is costly and inefficient. Many of the remediations that they force companies to enact in addition to fines and penalties mandate improvements in corporate governance over these issues and include reforms in director skills, boardroom structure and heightened accountability from the board and management on digital and cyber risk.

In 2022, the SEC has released proposed rules in cyber security that could significantly advance corporate governance and management practices for U.S. listed companies that builds upon their prior guidance in 2011 and 2018 (U.S. Securities and Exchange Commission, 2022). See Section 3.1 for a discussion of these proposed reforms.

The U.S. Congress has also proposed legal reforms on cyber expertise in the boardroom. Proposed federal Bill *S. 808 Cybersecurity Disclosure Act of 2021* would amend The Securities and Exchange Act of 1934 to require disclosing whether any governing body member has experience or expertise in cybersecurity (117th Congress, 2021). This proposed Bill has been reintroduced into the fourth straight U.S. Congress, demonstrating U.S. regulator's persistent efforts on mandating some basic corporate governance reform on these issues. This simple disclosure Bill would likely drive significant board reform. *S. 808* is similar to the reforms imposed with the Sarbanes-Oxley Act of 2002 when that

risks in American businesses will also continue to increase and create large-scale economic, business, and social risks. While U.S. regulators are legislating more corporate accountability in data privacy and cybersecurity, they have not yet legislated more boardroom and director accountability. The SEC looks set to leapfrog existing approaches to cyber governance with their proposed rules.

4.7 International Organization for Standardization (ISO)

ISO is an independent, non-governmental federation of national standards bodies which shares knowledge and develops market-based and voluntary standards to solve global problems. They have a membership base comprised of 165 national standards bodies. ISO/IEC has two related standards that address digital and cybersecurity governance. Their information security-focused standard also addresses several critical issues related to systemic risk within the digital business system.

The current *ISO/IEC 38500* standard on information and communication governance is identical to the Australian standard. Initially, it was based upon the Australian *AS8015 Corporate Governance of Information and Communication Technology* standard created in 2005. The current second edition of ISO 38500 has a stated objective "... to provide principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of information technology (IT) in their organizations" (ISO/IEC, 2015, p. 5).

ISO/IEC 38500 is generally viewed as the leading international standard for digital governance. It is focused on opportunity risk, or the digital upside of how corporate governance over the application of information technology creates business value. In justifying the need for this governance standard, ISO/IEC explicitly acknowledges the poor return on investment that many companies experience with their substantial spending on IT as the reason why the standard is needed. They also address the most common source of these poor returns, "The main reasons for these negative outcomes are the emphasis on the technical, financial, and scheduling aspects of IT activities rather than emphasis on the whole business context of use of IT" (p. 5).

This particular insight remains a common problem in governing information technology. The lack of leadership recognition that economies and businesses are already heavily dependent upon digital systems for much, if not most of the value that their economies and companies are creating remains a barrier to boardroom reform.

ISO/IEC 38500 lists a range of foundational benefits that develop from the effective corporate governance of IT:

- innovation in services, markets, and business;
- alignment of IT with business needs;
- appropriate implementation and operation of IT assets;
- clarity of responsibility and accountability for both the supply of and demand for IT in achieving the goals of the organization;
- business continuity and sustainability;
- efficient allocation of resources;
- good practice in relationships with stakeholders;
- actual realisation of the expected benefits from each IT investment; and
- assuring conformance with obligations (regulatory, legislation, contractual) concerning the acceptable use of IT (pp. 4–5)

The standard also integrates six-core behavioral principles intended to guide decision-making with a model focused on three main corporate governance tasks for directors to evaluate, direct and monitor the current and future use of IT. The standard is not intended to prescribe how IT governance should be applied but instead focuses on what should happen. The six principles address the need for corporate boards to ensure that the following objectives are being met:

> Responsibility: Ensure that IT accountabilities within the organization at the group and individual levels are understood, accepted, and executable.

Strategy: Make sure that the current and future IT capabilities are aligned to the changing strategic needs of the organization.

Acquisition: Have confidence that IT investments are supported by a balanced business case that addresses benefits, opportunities, costs, and risks over the short and long term that is monitored.

Performance: Ensures that IT performs at the service levels needed to meet current and future business requirements.

Conformance: Has confidence that IT complies with all legislation, regulations, and rules, and IT policies and practices are also defined, implemented, and enforced.

Human Behaviour: Understand and ensure that IT policies, practices, and decisions respect all human stakeholders' current and evolving needs.

The ISO standard is a simple and overarching framework that articulates the basic governance requirements for any governing body over IT. Focused mainly on digital risk and how the business strategically leverages and operationalizes information technologies, it does not encompass cybersecurity or systemic risks within modern IT systems. It is currently undergoing a scheduled five-year review.

A related ISO/IEC standard addresses the governance of information security risks. *ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security* offer boardrooms guidance for governing the digital downside. ISO/IEC 27014:2020 expects the board to take responsibility for the organization's effective information security management system.

Reflecting the same director tasks of evaluating, directing, and monitoring, the standard introduces the importance of communications in IT security governance by acknowledging the importance of cyber risk disclosure to interested parties such as shareholders. Emphasis is also included on the importance of the board receiving reliable and relevant reporting about information security activities. The timely and accurate disclosure of cyber risks and incidents is essential in protecting

investor interests and is becoming a focus and enforcement cudgel for regulators in the United States.

ISO/IEC 27014:2020 also addresses several issues related to the board's governance of systemic risk. Explicitly stated is a systemic risk-based information security governance objective focused on "preventing the organization's information technology from being used to harm other organizations" (ISO/IEC 27014 2nd edition 2020–12, 2020, p. 4). Other tasks placed squarely on the governance function by the standard include defining risk appetite, approving information security strategy, and promoting a positive information security culture.

The standard also explicitly addresses the need to govern situations where a third party could manage the information security function. This systemic risk issue can relate to situations where a managed service provider is outsourcing a security function, or a third-party provides a service such as cloud computing capability, e.g., Amazon Web Services. Notably, the standard also emphasizes the need to understand the scope of information security related to systemically essential issues such as external requirements, interfaces, and other dependencies. Adopting a risk-based approach to information security is also a focal point of the standard whereas a technical approach is still commonly applied and is the focus of many boardroom communications from IT management teams.

The ISO/IEC standards are comprehensive and leading global frameworks that can be readily adopted by any corporate boardroom or governing body to guide their approach to digital and cybersecurity governance.

4.8 The DiRECTOR Framework for Systemic Risk Governance

The DiRECTOR framework is a qualitative systemic risk assessment framework designed for corporate boards to help them understand and govern systemic risk in complex digital business systems, see Exhibit 2 (Zukis, 2019). Developed by the author, DiRECTOR complements the ISO standards by providing structure and a qualitative framework to analyze systemic issues that drive digital value creation and protection.

A stakeholder value-aligned framework, DiRECTOR identifies the eight-core domains inherent within every digital business system that need to work together for the system to fulfill the purposes for which it was designed and built. DiRECTOR aims to improve the understanding and recognition of systemic risk and how the parts of a digital business system work together to create and protect value for all stakeholders.

The framework also incorporates the five core elements that contribute to systemic risk levels within complex digital business systems. The framework was developed based upon research into the evolution of the international regulatory accord named Basel III that started in 2009 after the 2008 financial markets driven recession. The five essential elements that drive systemic risk into complex digital business systems are replaceability, inter-connectedness, size, complexity, and the x-jurisdictional requirements upon and between the parts of any complex systems (Zukis *et al.*, 2022). By identifying and assessing these issues across each of the eight DiRECTOR domains through the lens of these five forces of systemic risk, corporate leaders are gaining a better understanding of systemic risks inherent within digital business systems.

Corporate directors and technology executives are applying DiRECTOR to create a common language around systemic risk related to the digital business system and to introduce a structured approach to understanding, identifying, governing and managing systemic risk. DiRECTOR and its eight domains also provide a useful model for assessing digitally savvy director competencies, the alignment of boardroom structure and responsibility within committee charters on digital and cybersecurity governance, and the scope of digital and cybersecurity risk disclosures.

5

Recommended Digital and Cybersecurity Governance Reforms

At present, developments in national codes and leading practices are relying upon self-regulatory initiative to shape existing boardroom practices in digital and cybersecurity oversight. The leading practices that are emerging are focused on director skills, board structure, and the scope of risk oversight with particular acknowledgement of and emphasis on systemic cyber risk. These comprehensive, albeit voluntary, global digital governance frameworks have existed for over a decade and are helpful starting points for any boardroom wanting to initiate a more effective corporate governance approach to these issues.

However, digital risks continue to grow at a rate far exceeding the pace of self-regulatory boardroom reform in cybersecurity. While legal and regulatory mandates in corporate governance are on the horizon, boardroom reform in digital and cyber risk oversight needs to be accelerated to drive faster corporate governance transformation. Suggested legal reforms for regulators and leading practice improvements are recommended below in three principal areas: director skills, boardroom structure, and risk disclosure.

5.1 Digital Diversity Quotas and Digital Skills Disclosure

Legal reforms are needed in boardroom cyber expertise. Boardroom gender diversity quotas have shown that legislative action can drive a faster rate of boardroom reform in director composition (National Women's Council, 2021). Digital and cybersecurity governance effectiveness starts with digitally savvy corporate directors. The critical mass correlation identified by MIT between business results and the presence of three digitally savvy directors on a board supports the need for much more digital diversity in the corporate boardroom than exists at present.

Legal reform is needed to drive digital and cyber director capabilities onto corporate boards more quickly and broadly. Legal reform to corporate governance related laws should initially address the urgent need to have cybersecurity expertise and experience on corporate boards. Current proposed SEC rules and the Bill being proposed in the United States Senate to require disclosure of boardroom cyber expertise is the blueprint for this legal reform. Either of these legal reforms will amend The Securities and Exchange Act of 1934 if passed into law and require covered companies to disclose whether any member of the board has cybersecurity experience or expertise. Effective digital and cybersecurity governance is not possible without the boardroom skills to understand these issues. Protecting the enormous amount of economic and business value already being enabled by complex digital business systems is the starting point for foundational digital and cybersecurity governance reform and requires the certainty and urgency created by legal mandate. Listing standards worldwide, or other related corporate laws should reflect this foundational need for both public and private companies.

Additional "soft" self-regulatory reforms should focus on updates to national corporate governance codes that drive digital diversity breadth into the boardroom to reflect the comprehensive capabilities needed to govern the totality of the digital business system. Recommendations should be added to national codes for detailed disclosure of director digital expertise. Some leading digital governance practices in the U.S. already identify director competencies in data, information architecture, risk communications, emerging technology, cybersecurity, IT operations, and regulatory experience.

Following the lead of Malaysia firm Maybank, we believe national codes should also recommend the disclosure of director training received during the year and the nature of director education programs in these areas. Identifying expertise and digital and cyber literacy of corporate directors is a key step in advancing director professionalism and performance on these issues.

5.2 Board Structure and a Technology and Cybersecurity Committee

"Soft" reforms should be made in how corporate boards organize their activities and responsibilities in governing digital and cyber risk. Committee structures drive a focused approach to the issues being governed, bring more accountability, and send a strong internal and external signal. The frequent approach of conducting cybersecurity risk oversight through an audit committee introduces a range of problems ranging from the likely misalignment of director skills to the marginalization of the cybersecurity risk oversight agenda.

A "soft" reform approach to committee structure is recommended with an update to national corporate governance codes in countries around the world and through regulatory guidance and leading practice identification. With "comply and explain" or more explanatory principles in place within many national codes, a self-regulated reform will enable corporate boards some flexibility in committee design. However, this will nonetheless hold corporate boards to the higher standard by requiring an explanation of how the board has made the decisions it has made to organize corporate governance activities to effectively govern the full digital and cybersecurity governance agenda.

Updated national codes should recommend the leading practice of a technology and cybersecurity committee. This would place a fourth committee alongside the common requirement or practice of a standing audit committee, nominating committee, and remuneration committee. Governing the digital upside alongside its downside in a technology and cybersecurity committee is already a leading practice that adds efficiencies and effectiveness to the oversight of these issues.

This is recommended as a "soft" reform even though it is a leading practice because other committees such as a risk management committee can incorporate these responsibilities through their charter. This reform allows boards to be transparent and thoughtful with their organizational approach by explaining how the same scope of oversight is achieved with a different committee design. Ensuring active governance of the comprehensive digital and cybersecurity agenda is the primary goal, and committee design is secondary.

5.3 Cyber and Systemic Risk Disclosure

Legal reform is needed in cyber and systemic risk disclosure, not self-regulatory guidance. Cyber-attack strategies and tactics evolve and emerge quickly, faster than the ability of defenders to launch protective countermeasures. Attackers have shifted their strategy from monetizing the data they exfiltrate on secondary markets to now holding companies, critical processes, and the public interest hostage. The "crown jewel" for every company and organization is its ability to function, i.e., to transact; to move fuel through a pipeline; to keep the lights on. Attackers are now attacking the ability of digital economies and general economies to function.

Systemic risk is the risk that exists between the parts of a complex connected system and is a new challenge in enterprise risk management. The growing complexity and inter-connectedness of digital economies creates new risks. With the growing complexity of digital systems, attackers have figured out that the system itself is the weak point. Attackers are now exploiting these complex systems with attacks targeted at their systemic weak points, such as the SolarWinds attack.

Incident and risk disclosure reforms are needed in cybersecurity and systemic risk disclosure to ensure that investors have a useful explanation of the systemic risk environment inherent with the company and throughout the ecosystem the company functions within. Management teams need to do much more work in understanding systemic risk and boardroom accountability on this issue will drive immediate progress.

"Soft" expectations in the United States from the SEC already address cyber risk disclosure, but experience has shown this suggested

guidance to be ineffective. India has recently introduced mandated reforms in place for incident disclosure in its ICT industry to reduce the spread of systemic risks. Suggestive guidance does not go far enough and has not resulted in the quality of disclosure required to inform investors effectively. Moreover, systemic risk disclosure related to the digital business system is virtually non-existent in the United States. These indications suggest that these risks are not yet well understood by boards and management teams.

Understanding cyber risk materiality requires an understanding of the financial impacts of cyber risk. While disclosure of the financial amount of expected cyber losses is too prescriptive, which could be helpful information for attackers, disclosure of a company's assessment and monitoring program overseeing projected cyber economic losses is relevant information for investors. These disclosures would provide investors with helpful information that allows them to understand the maturity of the practices and policies being deployed to govern and manage the organization's self-insured cyber risk levels.

Legal reform in systemic risk disclosure should focus on the organization's specific systemic risk environment and how management is monitoring and mitigating systemic risk. A minimum disclosure should qualitatively address non-generic issues in the digital business system and the organization's systemic risk environment, including the approach and methodology used to assess and monitor systemic risks.

Explicit legal reforms should also require that boards receive an independent third-party assessment of cybersecurity programs and of the organization's systemic risk levels. Accounting rules should also be updated to address the need to account for projected cyber losses that are probable and can be estimated. Disclosure reforms are vital to investors, and also offer a useful defense for companies to the growing amount of litigation risk in these areas. Ultimately however, understanding these risks leads to a more effective approach in managing them and reducing them and that is the goal.

6

Conclusions

Corporate boards and directors worldwide have a duty and responsibility to govern and understand digital and cybersecurity risks. Investors, customers, and other stakeholders are paying the price for the slow adoption of digital and cybersecurity risk oversight policies and practices.

The need for corporate governance reform in digital and cybersecurity risk oversight is worldwide. New cyber risks and systemic threats are introducing new dangers to economies and businesses alike. The companies that have shown digital boardroom leadership have demonstrated positive differentiated business results in revenue growth, profitability, return on assets, and market capitalization. Boardroom leadership and effective digital and cyber governance on these issues has a material business and economic impact.

Well-developed and applied leading practices and standards are currently available to voluntary enable digital and cybersecurity board reform. While this type of self-regulated digital boardroom reform is occurring, it is the exception, not the rule. Legislative reform is urgently needed to advance corporate governance practices and policies worldwide in response to this significant and evolving risk.

Legislative reform that requires competent directors capable to govern these issues with digital director quotas will support national digital mandates, investor and public interests, and national security interests. Legislative quotas for digitally savvy directors must first address the acute need for cybersecurity expertise in the boardroom. Legal reform is also needed to mandate this core boardroom competency to drive much faster board transformation.

"Soft" reforms in self-regulatory codes and practices are suggested in boardroom organizing principles around digital and cybersecurity risk. But legal reforms are needed in cyber and systemic risk disclosure to better inform investors, and ultimately drive more effective systemic risk reduction practices.

Boardrooms and their corporate directors are critical parts of the complex system that powers every company's digital future and every country's digital destiny. Digital economies need high-performing digital businesses and digitally effective boardrooms. Boards and policymakers need to drive faster corporate governance reform on these issues to protect stakeholder, investor, and national interests.

The development of digital and cyber governance policies and practices is long overdue. This monograph documents and illustrates the state of these issues where practices and policies are emerging to assemble a body of representative and actionable guidelines and tactics. Any corporate board around the world currently has the ability to self-regulate their way to an effective approach in governing digital and cyber risk. Corporate governance reform will reduce real levels of business risk while also driving digital transformation and its many benefits.

Appendix

Exhibit 1

Job Summary:

The Chief Information Officer will develop, plan, and implement an information technology (IT) strategy that meets the company's business needs, delivers optimal return on investment, and maintains utmost security.

Supervisory Responsibilities:

- Oversees projects and assignments within the Information Systems (IS) department.
- Leads efficient operation of the team so that prompt modernization and upgrades of IS are performed as needed.
- Conducts performance evaluations that are timely and constructive.

Duties/Responsibilities:

- Collaborates with members of the executive team to identify ways IT can assist the company in achieving business and financial goals.
- Identifies new IS developments and technologies; anticipates resulting organizational modifications.
- Ensures that IT and network infrastructure adequately support the company's computing, data processing, and communications needs.
- Develops and implements the IT budget.
- Communicates goals, projects, and timelines of the company to the department; plans ways to execute those goals within the department.
- Establishes long-term IS needs and plans and develops strategies for developing systems and acquiring software and hardware necessary to meet those needs.
- Assists as top-level contact for end users in determining IS requirements and/or solutions.
- Ensures compliance with government regulations that apply to systems operations.
- Performs other related duties as assigned.

Required Skills/Abilities:

- Excellent verbal and written communication skills.
- Proficient in Microsoft Office Suite or related software.
- Excellent ability to conceptualize long-term business goals and develop orderly processes to accomplish those goals.
- Excellent managerial skills (SHRM, 2021).

Exhibit 2

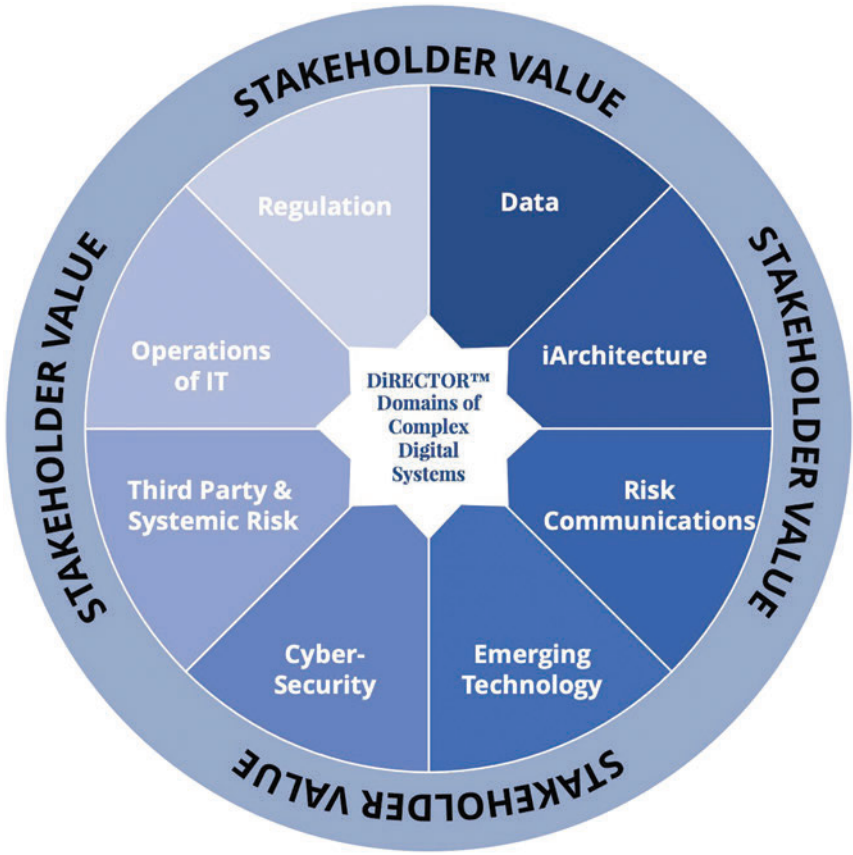

Figure A.1: The DiRECTOR framework for qualitatively assessing systemic risk in complex digital business systems.

Source: Digital Directors Network (2019).

Exhibit 3

Leading Practices Boardroom Technology and Cybersecurity Committee Charter

Purpose

The Technology and Cybersecurity Committee (the "Committee") is appointed by the Board of Directors (the "Board") to provide oversight and counsel on matters relating to information technology and cybersecurity risk oversight.

Responsibilities

The basic responsibility of the members of the Committee is to act in what they reasonably believe to be in the best interests of the Company, its shareholders, and stakeholders. In discharging that obligation, the Committee has the following authority and responsibilities:

(1) To review and discuss the overall strategy of the Company as it pertains to digital and cybersecurity governance, in order to make recommendations to the Board on strategies, operations and related issues regarding:

   (i) Trends in information technology that could significantly affect the competitive position of the Company and the industries in which it operates and the creation of digital and business value.

   (ii) Emerging technologies, device management, and investment in information technology hardware and software lifecycle management.

   (iii) The architecture of the digital business system and related risks and opportunities.

   (iv) Monitoring cyber threat intelligence and cyber threat risk mitigation and ensuring business continuity and recovery in the event of a cyber breach.

(v) The projected economic impacts of cyber risk including the Company's self-insured exposure and the strategies and tactics to transfer this risk, mitigate it or accept it.

(vi) Systemic risk within the digital business system and issues related to inbound and outbound systemic risks that could impact the company or others, including third-party IT risk management

(vii) Data and information lifecycle management, including data privacy issues.

(viii) IT portfolio project management and IT services delivery.

(ix) Social media monitoring and risk management.

(x) Digital and cybersecurity regulatory issues, requirements, and potential fines.

(xi) Operations of IT including staffing, retention, performance, and development, including enterprise-wide awareness, preparedness programs, internal and third-party risk communications, and incident response.

(2) To track and measure the relationship between the Company's digital and cybersecurity governance mechanisms and its performance, competitive position, prospects for growth, overall digital risk profile, and business value at stake.

(3) To set risk tolerances and assess and monitor risk appetite for digital investments and strategies that drive and support business value.

(4) To carry out other activities consistent with this Charter, the Bylaws, and applicable laws that the Committee or the Board may deem necessary or appropriate.

Committee Members

The Committee will consist of at least three Board members, as appointed annually by the Board on the recommendation of the Nominating and Governance Committee. Each member of the Committee will

serve a one-year term or until his or her earlier resignation, removal, or death. At least two Committee members will be independent Qualified Technology Experts (QTE) who have significant familiarity and experience with information technology or technology transformation and cybersecurity matters, as shown to the Board by way of educational background and demonstrated relevancy of skills and competencies including relevant field experience. At least one Committee member will be a cybersecurity expert with the requisite cybersecurity field expertise needed by the Company to oversee the protection of business value.

Chairperson

The Chairperson of the Committee will be a Qualified Technology Expert (QTE) or cybersecurity expert. The Chairperson will be an Independent Director appointed by the Nominating and Governance Committee of the Board and may be removed by the Board at any time, with or without cause. If the Chairperson is not available to perform his/her responsibilities or attend a Committee meeting, the Chairperson will temporarily delegate his/her responsibilities to an acting chair.

Meetings

The Committee will meet as often as it determines appropriate or necessary, at a minimum of four times per year. The Chairperson of the Committee will preside at each meeting and may direct appropriate management and staff members to prepare draft agendas and background information for each meeting. The Chairperson will review and approve any draft agenda and distribute it to the Committee at least one day before the meeting. All meetings of the Committee will be held per the Bylaws of the Company, and written minutes of each meeting, in the form approved by the Committee, will be filed in the Company records. In the absence of the Chairperson of the Committee, an acting chair will review and distribute the agenda and any background materials to members at least one day in advance of the meeting. The Chairperson of the Committee (or acting chair) will report to the Board on matters addressed at the Committee meeting at its subsequent meeting,

including quarterly reports on economic exposures of cyber risk and the Company's cybersecurity risk profile. The Committee may include members of the Company's management, other members of the Board, or third parties in its meetings.

Oversight

The Committee may delegate authority to subcommittees consisting of one or more Committee members when appropriate. The Committee has the power to retain outside experts or advisors to carry out its responsibilities. It has the sole authority to approve the fees and retention terms of any such individuals at the Company's expense. The Committee will evaluate the fulfillment of its responsibilities, review its charter, and recommend any proposed changes to the Nominating and Governance Committee and the Board for review and approval annually (Digital Directors Network, 2021b).

References

117th Congress (2021). *S. 808 Cybersecurity Disclosure Act of 2021*. URL: https://www.congress.gov/bill/117th-congress/senate-bill/808/text.

Accenture (2022). *Global Incident Report: Russia-Ukraine Crisis | April 21*. Accenture.

Ang, C. (2021). *The Most Significant Cyber Attacks from 2006–2020, by Country*. URL: https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/.

Bayarma, A., C. Hubers, T. Schwanen, and D. E. Martin Dijst (2011). "Anything, anywhere, anytime? Developing indicators to assess the spatial and temporal fragmentation of activities (Alexander Anything Spatial and Temporal Relevance, P. 1: 1250)". *Environment and Planning*: 678–705.

BNP Media (2020). *Security*. (B. Media, Producer) Security: URL: https://www.securitymagazine.com/articles/93062-ransomware-victim-travelex-forced-into-bankruptcy.

Bordoff, J. (2021). *Foreign Policy Voice*. URL: https://foreignpolicy.com/2021/05/17/colonial-pipeline-crisis-cyberattack-ransomware-cybersecurity-energy-electicity-power-grid-russia-hackers/.

Braue, D. (2021). *ACS Information Age*. ACS Information Age: URL: https://ia.acs.org.au/article/2021/hold-company-directors-liable-for-cyber-attacks.html.

Brynjolfsson, E. and A. McAfee (2011). *Race Against the Matchine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Emplyoment and the Economy*. Lexington, Massachusetts, USA: Digital Frontier Press.

Chakravorti, B., R. Shankar Chaturvedi, C. Filipovic, and G. Brewer (2020). *Digital in the Time of Covid: Trust in the Digital Economy and Its Evolution Across 90 Economies As the Planet Paused for a Pandemic*. Medford, MA: The Fletcher School at Tufts Unviersity.

Chen, K. D. and A. Wu (2016). *The Structure of Board Committees*. Boston: Harvard Business School.

CMS Law (2022). *Enforcement Tracker*. GDPR Enforcement Tracker: URL: https://www.enforcementtracker.com/?insights.

CNA Financial Corporation (2021). "Form 10-Q". In: *Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934*. Chicago, IL, USA.

Commonwealth of Australia (2021). *Strengthening Australia's Cyber Security Regulations and Incentives—A Call for Views*. Commonwealth of Australia.

Cyentia Institute LLC (2020). *IRIS 20/20 Extreme: Analyzing the 100 Largest Cyber Loss Events of the Last Five Years*. Cyentia Institute LLC.

Dezan Shira & Associates (2021). *The PRC Personal Information Protection Law (Final): A Full Translation*. URL: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/.

Digital Directors Network (2019). Systemic Digital Risk: Understanding and Overseeing Complex Digital Environments with the DiRECTOR™ and RISCX™ Frameworks.

Digital Directors Network (2021a). Boardroom Solutions: URL: https://www.digitaldirectors.network/cpages/briefings.

Digital Directors Network (2021b). *Digital Governance Maturity Model*. Los Angeles: DDN LLC.

Dittmar, J. (2011). *Information technology and economic change: The impact of the printing press*. voxeu.org: URL: https://voxeu.org/article/information-technology-and-economic-change-impact-printing-press.

Eaton, C. and D. Volz (2021). *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*. URL: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

Eddy, M. and N. Perlroth (2020). *Cyber Attack Suspected in German Woman's Death*. The New York Times: URL: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

European Commission (2020). *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission.

FASB of the Financial Accounting Foundation (2010). *FASB Exposure Draft Proposed Accounting Standards Update Contingencies (Topic 450)*. FASB.

Federal Trade Commission (2019). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. URL: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

FedEx Corporation (2022). *FORM–10K*. Memphis: FedEx Corporation.

Ferrillo, P., B. Zukis, and C. Veltsos (2021). *The SEC's Clear Reminder About the Need for Quality Cybersecurity Disclosures*. URL: https://corpgov.law.harvard.edu/contributor/bob-zukis/.

Financial Reporting Council of Nigeria (2018). *Nigerian Code of Corporate Governance 2018*. Financial Reporting Council of Nigeria Act.

Financial Stability Board (2020). *2020 list of global systemically important banks*. URL: https://www.fsb.org/2020/11/2020-list-of-global-systemically-important-banks-g-sibs/.

Galloway, A. (2021). *'Real and Present Danger:' Government considers making company directors personally liable for cyber attacks*. The Sydney Morning Herald: URL: https://www.smh.com.au/politics/federal/real-and-present-danger-government-considers-making-company-directors-personally-liable-for-cyber-attacks-20210712-p588vz.html.

Gomez, B. (2021). Vice President, Equilar. (B. Zukis, Interviewer).

Greig, J. (2022). *Bridgestone still struggling with plant closures across North America after cyberattack*. ZD Net: URL: https://www.zdnet.com/article/bridgestone-still-struggling-with-plant-closures-after-cyberattack/.

Guaranty Trust Bank plc. (2021). *2020 Annual Report*. Lagos: Guaranty Trust Bank plc.

Hasbro, Inc. (2020). *Form 10-K*. Rhode Island: Hasbro, Inc.

Haverstock, E. (2021). *Inside The Global 2000: The Value of the World's Largest Public Companies Soars, As Sales And Profits Falter*. Forbes.Com: URL: https://www.forbes.com/sites/elizahaverstock/2021/05/13/inside-the-global-2000-the-value-of-the-worlds-largest-public-companies-soar-as-sales-and-profits-falter/?sh=1d8369aa26d4.

Hawkins, A. J. (2022). *Toyota shuts down its Japanese factories after reported cyberattack*. URL: https://www.theverge.com/2022/2/28/22954688/toyota-cyberattack-factory-shut-down-cars-output.

Ho, J. (2021). *Corporate boards: Don't underestimate your role in data security oversight*. Contrary to popular belief, data security begins with the Board of Directors, not the IT Department.

Hope, A. (2021). *Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customers*. URL: https://www.cpomagazine.com/cyber-security/cyber-insurance-firm-suffers-sophisticated-ransomware-cyber-attack-data-obtained-may-help-hackers-better-target-firms-customers/.

Huang, K., R. Ye, and S. Madnick (2019). *Both Sides of the Coin: The Impact of Cyber Attacks on Business Value*. Cambridge: MIT Sloan School of Management.

Huawei and Oxford Economics (2017). *Digital Spillover—Measuring the True Impact of the Digital Economy*. Shenzen: Huawei Technologies Co., Ltd.

IBM Security (2021). *Cost of a Data Breach Report 2021*. IBM.

IDC (2020). *IDC FutureScape: Worldwide Digital Transformation Predictions 2021*. Framingham: IDC.

Insitute of Directors Southern Africa KING IV (2016). *Draft King IV Report—Responses to the summarised public comments 2016*. Insitute of Directors Southern Africa.

Institute of Directors In Southern Africa NPC (2016). *KING IV Report On Corporate Governanace For Southern Africa*. Johannesburg: Institute of Directors In Southern Africa NPC.

Institutional Investor (2021). *Japan's Corporate Governance Code Revised in Anticipation of "Prime Market" Segment Coming to TSE*. URL: https://www.institutionalinvestor.com/article/b1spy621t219ny/Japan-s-Corporate-Governance-Code-Revised-in-Anticipation-of-Prime-Market-Segment-Coming-to-TSE.

International Monetary Fund (2018). *Measuring The Digital Economy*. Washington, D.C.: International Monetary Fund.

International Organization Of Securities Commissions (2021). *Environmental, Social and Governance (ESG) Ratings and Data Products Providers*. Madrid: International Organization Of Securities Commissions.

International Telecommunication Union (2018). *Assessing the Economic Impact of Artificial Intelligence*. Geneva: International Telecommunication Union.

ISO/IEC (2015). *Internation Standard ISO/IEC 38500 2nd edition Information technology-Governance of IT for the organization*. Geneva: ICO/IEC.

ISO/IEC 27014 2nd edition 2020–12 (2020). *Information security, cybersecurity and privacy protection — Governance of information security (ISO_IEC_27014_2020(en). P. 1:0)*. Geneva: ISO/IEC.

ISO/IEC/IEEE 15288 (2015). *Systems and software engineering—System life cycle processes*. First edn. Geneva and New York: ISO/IEC/IEEE.

ISS (2021). *Governance QualityScore*. URL: https://www.issgovernance.com/esg/ratings/governance-qualityscore/.

Jones Day (2021). *China Finalizes Data Security Law to Strengthen Regulation on Data Protection*. URL: https://www.jdsupra.com/legalnews/china-finalizes-data-security-law-to-4249871/.

Lee, C. (2021). *Vietnam digital economy expected to contribute 20 percent of GDP by 2025*. URL: https://vietnamtimes.org.vn/vietnam-digital-economy-expected-to-contribute-20-percent-of-gdp-by-2025-21229.html.

Lewis, M. J. (2020). "Independent Directors Mitigate Legal Risk". *Private Company Director*: 56.

Malayan Banking Berhad (2020). *Corporate Governance Report*. Kuala Lumpur: Malayan Banking Berhad.

Marsh & McLennan Companies Ltd. Inc. and Global Network of Director Institutes (2021). *Global Network of Directors Institutes 2020–2021 Survey Report*. Marsh & McLennan Companies Ltd, Inc. | Global Network of Director Institutes.

Mehrotra, K. and W. Turton (2021). *CNA Paid $40 Million in Ransom After March Cyber Attack*. URL: https://www.insurancejournal.com/news/national/2021/05/21/615373.htm.

Morgan, S. (2020). *Cybercrime Magazine*. Cybercrime Magazine: URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Munter, P. (2021). *Statement on OCA's Continued Focus on High Quality Financial Reporting in a Complex Environment*. URL: https://www.sec.gov/news/statement/munter-oca-2021-12-06.

MyLogIQ (2021). *S&P 500 and R3000 Technology and Cybersecurity Oversight*. San Juan: MyLogIQ.

National Center for Incident Readiness and Strategy for Cybersecurity (2021). *Outline of Japan's Next Cybersecurity Strategy*. NISC: URL: https://www.nisc.go.jp/eng/.

National Women's Council (2021). *Increasing Gender Balance on Boards: The case for Legislative Gender Quotas in Ireland*. Dublin: National Women's Council.

Neuberger, A. (2021). *White House*. White House: URL: https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf.

New York State Department of Financial Services (2021). *Insurance Circular Letter No. 2*. URL: https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

OECD (2015). *G20/OECD Principles of Corporate Governance*. Paris: OECD Publishing.

Panettieri, J. (2021). *SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details*. URL: https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/4/.

Patterson Balknap Webb and Tyler, LLP. (2021). *SEC Signals Renewed Interest in Cybersecurity Disclosure Enforcement*. URL: https://www.jdsupra.com/legalnews/sec-signals-renewed-interest-in-6695892/.

Perez, S. (2021). *Walmart to sell it's e-commerce technologies to other retailers*. TechCrunch.com: URL: https://techcrunch.com/2021/07/28/walmart-to-sell-its-e-commerce-technologies-to-other-retailers/.

Powell, J. (2021). 60 Minutes. URL: https://www.cbsnews.com/news/jerome-powell-full-2021-60-minutes-interview-transcript/ (S. Pelley, Interviewer).

Pritchard, S. (2022). *India to introduce six-hour data breach notification rule*. URL: https://portswigger.net/daily-swig/india-to-introduce-six-hour-data-breach-notification-rule.

Reuters (2021a). *Business: AIG is reducing cyber insurance limits as cost of coverage soars*. URL: https://www.reuters.com/business/aig-is-reducing-cyber-insurance-limits-cost-coverage-soars-2021-08-06/.

Reuters (2021b). *Revisions of Japan's Corporate Governance Code and Guidelines for Investor and Company Engagement*. Tokyo: The Council of Experts Concerning the Follow-up of Japan's Stewardship Code and Japan's Corporate Governance Code.

Ross, R., M. McEvilley, and J. Carrier Oren (2016). *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Gaithersburg: U.S. Department of Commerce/National Institute of Standards and Technology.

Securities Commission Malaysia (2021). *Malaysian Code on Corporate Governance (as at 28 April 2021)*. Kuala Lumpur: Securities Commission Malaysia.

Shoprite Holdings Ltd. (2020). *Application of the King IV Code Principles*. Johannesburg: Shoprite Holdings Ltd.

SHRM (2021). *Job Description Chief Information Officer*. URL: https://www.shrm.org/ResourcesAndTools/tools-and-samples/job-descriptions/Pages/Chief-Information-Officer.aspx.

SpencerStuart (2017). *Boardroom Best Practice: Lessons learned from board assessments across Europe*. SpencerStuart.

The Hindu (2021). *Government to unveil national cyber security strategy soon: National Cyber Security Coordinator*. URL: https://www.thehindu.com/business/government-to-unveil-national-cyber-security-strategy-soon-national-cyber-security-coordinator/article35119538.ece.

The White House (2022). *Office of the National Cyber Director*. The White House: URL: https://www.whitehouse.gov/oncd/.

Tricor Group and FT Board Director Programme (2021). *2021 Asia Pacific Board Director Barometer Report*. Hong Kong: Tricor Group.

Turton, W. and K. Mehrotra (2021). *Hackers Breached Colonial Pipeline Using Compromised Password*. URL: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

UNCTAD (2019). *Digital Economy Report 2019 Value Creation And Capture: Implications For Developing Countries*. New York: United Nations.

U.S. Bureau of Economic Analysis (2021). *Updated Digital Economy Estimates,* U.S. Bureau of Economic Analysis. Washington, D.C.: U.S. Bureau of Economic Analysis (BEA).

U.S. Securities and Exchange Commission (2021). *Cybersecurity Risk Governance*. URL: https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202104&RIN=3235-AM89.

U.S. Securities and Exchange Commission (2022a). March 9. *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*. URL: https://www.sec.gov/news/press-release/2022-39.

U.S. Securities and Exchange Commission (2022b). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure File No. S7-09-22*. Washingto, DC: Securities and Exchange Commission.

Walmart Inc. (2021). *Form 10-K*. Bentonville: Walmart Inc.

Weill, P., T. Apel, S. L. Woerner, and J. S. Banner (2019). *Assessing The Impact Of A Digitially Savvy Board On Company Performance*. Boston: MIT Management Sloan School Center For Information Systems Research (CISR).

World Economic Forum (2019). *Our Shared Digital Future Responsible Digital Transformation—Board Briefing*. Geneva: World Economic Forum.

Zukis, B. (2016). *Are Cyber Experts On Boards Inevitable?* URL: https://www.conference-board.org/blog/postdetail.cfm?post=5917.

Zukis, B. (2019). *DDN Releases DiRECTOR The Only Systemic Risk Framework Focused On Complex Digital Systems*. URL: https://www.digitaldirectors.network/blogs/ddn-releases-director-the-only-systemic-risk-framework-focused-on-complex-digital-systems.

Zukis, B. (2020). *Ransomware Has A New And Very Valuable Hostage In Sight*. URL: https://www.forbes.com/sites/bobzukis/2020/06/18/ransomware-has-a-new-and-very-valuable-hostage-in-sight/?sh=2f8ba91d170f.

Zukis, B. (2021a). *China, Fred Astaire And The Countries Dancing Towards The Digital Future*. URL: https://www.forbes.com/sites/bobzukis/2021/07/21/china-fred-astaire-and-the-countries-dancing-towards-the-digital-future/?sh=147ed10e6394.

Zukis, B. (2021b). "The Boardrooms Leading America's Digital Transformation". *NACD Directorship*: 24–30.

Zukis, B. (2022). *The SEC Is About To Force CISOs Into America's Boardrooms*. URL: https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/?sh=7e7bf1ed68a9.

Zukis, B., P. Ferrillo, and C. Veltsos (2022). *The Great Reboot—Succeeding in a Complex Digital World Under Attack From Systemic Risk*. 2nd edn. Los Angeles: DDN Press.