DIGITAL DIRECTORS NETWORK

The Definitive Boardroom Guide on Cybersecurity Governance:

The DOMINO Guide

PLUS: The SEC's Final Disclosure Rules

Bob Zukis

CEO, Digital Directors Network

www.digitaldirectors.network

ISBN: 978-1-7350430-6-7 (Paperback)

Suggested reference: Bob Zukis, “The Definitive Boardroom Guide on Cybersecurity Governance: DOMINO 23,” DDN Press, Manhattan Beach, 2023

About Digital Directors Network

Digital Directors Network (DDN) is the premier boardroom network of IT and cybersecurity executives, corporate directors, and organizations working together to shape and secure the digital future. Collectively we are committed to advancing the practice and profession of digital and cybersecurity risk governance. DDN was founded in 2017 and has over 1,300 members who represent many of the world's leading boardrooms and organizations. DDN and its members are at the forefront of shaping policy and solutions to enable directors and executives to effectively govern digital and cybersecurity risk.

CPD CERTIFIED
The CPD Certification Service

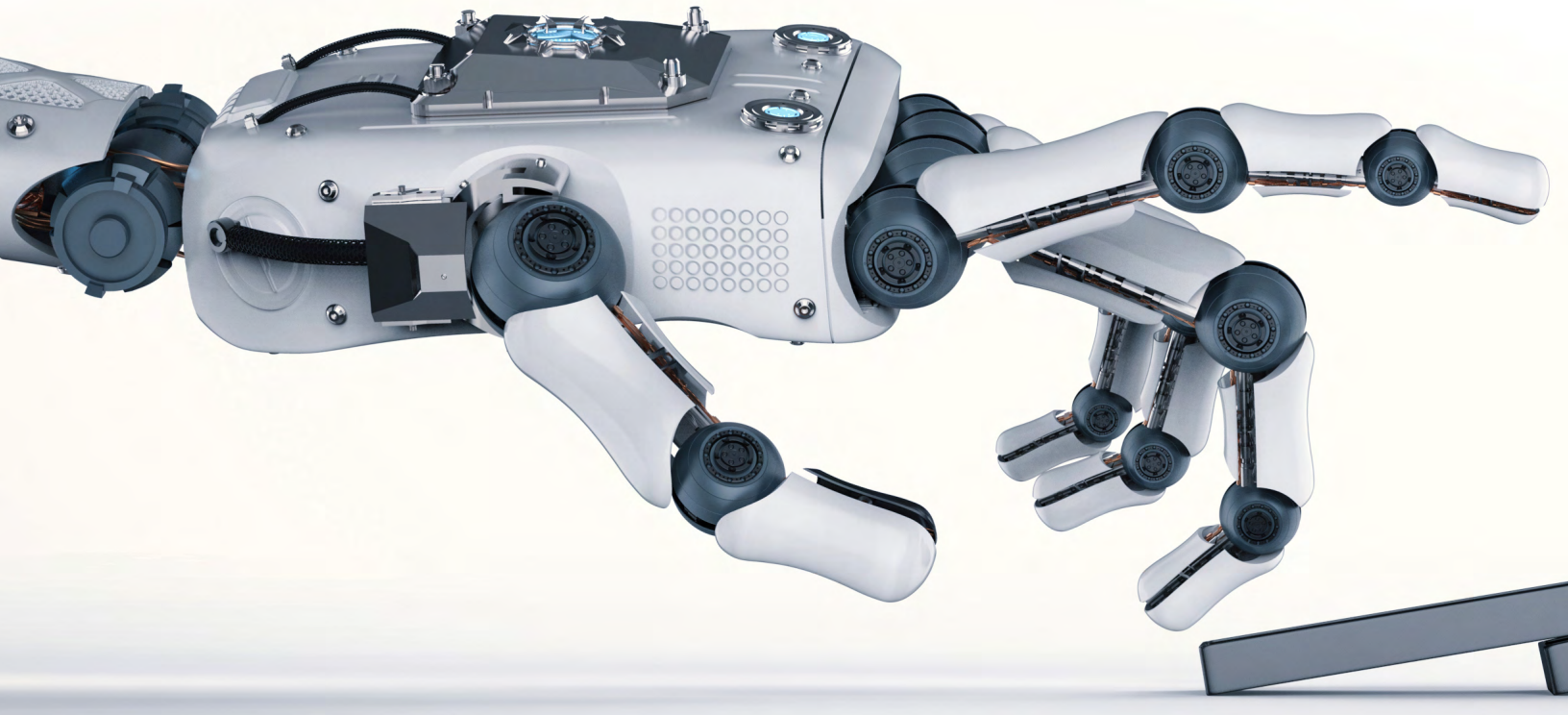
About *The DOMINO Guide*

***The DOMINO Guide* is a product of DOMINO 23, the inaugural boardroom and executive learning event of DDN. The DOMINO Guide provides an implementation blueprint for boards to optimize digital and cybersecurity governance.**

DOMINO 23 brought together more than 160 policy, boardroom, IT, cybersecurity, and business leaders at The University of Chicago Booth School of Business on May 16 and 17, 2023. A combination of classroom-based lectures and deep interactive working sessions were led by subject-matter experts, corporate directors, and industry leaders to advance the mission of DDN to develop digital and cybersecurity governance as a high-performing part of boardrooms around the world.

The focus at DOMINO 23 was on developing and advancing policy, practices, and capabilities in digital and cybersecurity governance ahead of the finalization of the U.S. Securities and Exchange Commission's cyber governance disclosure rules. SEC Commissioner Jaime Lizárraga provided the opening keynote and his comments are published on the SEC website.

Policy leaders and executives and directors from the SEC, NIST, Amazon, Disney Studios, HP, Korn Ferry, Overstock, PNC Bank, RGA, Target, UPS, Bucknell University, and others enriched the DOMINO 23 executive learning experience with their perspectives and insights.



Leading the overall learning experience were DOMINO content partners who brought their deep insights and practical solutions to the challenges of digital and cybersecurity oversight including Proofpoint, X-Analytics, White & Case, Kudelski Security, Telos, Corporate Board Member, TDI, Cyversity, Equilar, ISC2, and IDC.

The various masterclasses, policy discussions, expert lectures, and practitioner-led working sessions delivered the depth and actionable insight that boardroom leaders need to effectively govern digital and cybersecurity risk. These included:

- An analysis and discussion of SEC Commissioner Lizarraga's comments by DDN leadership with two cybersecurity and boardroom leaders.
- A masterclass on determining cyber materiality through economic analysis and quantification of cyber risk from the leading experts pioneering new approaches to these issues.
- One of the world's leading law firms teaching a masterclass on the then proposed SEC rules and what they mean including risk and incident disclosure requirements and the role of useful disclosure.
- A masterclass taught by the world's leader in securing people as a systemic risk vector with in-depth examples on how to monitor and reduce the unique challenges of this risk.
- Case studies of recent incidents using the DiRECTOR™ framework to identify sources of systemic risk in complex digital business systems led by a leading global advisory firm with deep practitioner backgrounds.
- An engaging lecture on systems thinking by one of the world's foremost professors in complex systems science from Bucknell University.
- A special all-hands working keynote with leadership from the National Institute of Standards and Technology (NIST) to shape and influence the next generation of the Cybersecurity Framework (CSF) that incorporates governance as a discrete domain.
- An interactive peer panel of IT and cybersecurity leaders from Disney, Target, and UPS who provided insights on the use of the DiRECTOR™ framework for understanding systemic risk in complex digital business systems.
- A moderated Q&A with boardroom recruiters who offered tips on how CIOs and CISOs should prepare for directorship and what boards need and want from them.
- A closing presentation and discussion from a DDN working group of CISOs and directors on their efforts to create *The Ultimate Board Deck in Cybersecurity Governance* that connects cyber risk to materiality.

Pre-event participants also attended the widely acclaimed *DDN QTE 501 Boardroom Masterclass for IT and Cybersecurity Executives*. All attendees enjoyed opportunities to network including an evening reception and dinner at the Adler Planetarium where more than 5,000 dominoes fell as Talking Heads' *Burning Down the House* closed out the evening.

The DOMINO Guide reflects the key content from DOMINO 23 along with insights that will help corporate directors understand and develop their ability to implement effective policies and procedures that successfully and securely govern their company's journey into the digital future. It will also help directors and senior leadership teams understand and implement the SEC's final cybersecurity disclosure rules.

DOMINO 23 was CPD Certified as an executive learning event and attendees earned 12 hours of CPD credit. Participants who attended the *QTE 501 Boardroom Masterclass for IT and Cybersecurity Executives* on May 14, 2023, earned another 13 hours of CPD.

DOMINO 23: A Focus on Cybersecurity Governance Implementation

Welcome to the leading edge of digital and cybersecurity risk oversight. The time has passed for handbooks comprised of random collections of anecdotal opinions, lists of questions for corporate directors, and narrow and haphazard views celebrating the problem of governing cybersecurity. It's time for boardroom action and solutions.

DOMINO 23, its participants, and all of DDN's members share a mission to solve the boardroom governance challenges created by digital innovation and the new risks they have created. Recognizing that the corporate governance community cannot solve problems that they did not create and may not fully understand, these leaders are working together to transform digital and cybersecurity governance. Our mission is to strengthen the boardroom and business leadership as a critical control around the complex digital systems powering the world.

The SEC has now finalized transformative new cybersecurity disclosure rules as economic output and corporate value propositions grow their reliance upon complex digital business systems. The digital threats and risks related to the general economy and every business have never been greater. Only recently, MGM, Toyota and United Airlines have experienced cyber attacks and accidental cyber occurrences that have created significant business continuity issues.

Corporate boards must now move with a sense of urgency to implement policies and practices that strengthen their role as a critical control in their company's system of digital and cybersecurity risk oversight. Too much is at stake for boards to be passive participants in their company's journey towards the digital future—and that stake will only continue to grow.

Through initiatives pioneered by boardroom leaders, including DDN, the practice and profession of digital and cybersecurity governance exists as an important part of corporate governance. The good news is that because of these efforts, we know what needs to be done to solve the puzzle of digital and cybersecurity risk governance.

Throughout history, information technologies and innovations regularly emerge and transform economies, human behaviors, and corporate value propositions. *The Definitive Boardroom Guide on Cybersecurity Governance* (*The DOMINO Guide)* moves beyond admiring the problem of digital and cybersecurity risk by providing private and public company directors with tactical guidance to build governance systems that are adaptive to the dynamic reality of these changes. Every corporate board can optimize their digital and cybersecurity governance effectiveness by focusing on three areas central to this puzzle:

1. Learning from established standards to assess existing boardroom digital and cybersecurity governance policies and practices against.
2. Developing the board's digital and cybersecurity governance system against gaps in that assessment.

3. Implementing and monitoring a comprehensive system of digital and cybersecurity risk oversight that reflects and governs the full breadth of risks across the complex digital business system.

The DOMINO Guide provides implementation details and guidance for each of these steps—both defining what these concepts mean and providing actionable advice to optimize the role of the boardroom and the effectiveness of corporate directors on these important economic and business issues.

Notably, effective standards already exist which any boardroom or director can learn from to develop basic digital and cybersecurity governance capabilities. Regulators in the United States and elsewhere are also defining new standards by starting to force boardrooms to do what so far most have been unwilling, or unable, to do themselves. The path forward has also been paved by a growing group of visionary boardroom and industry leaders who are defining and implementing new standards in digital and cybersecurity governance.

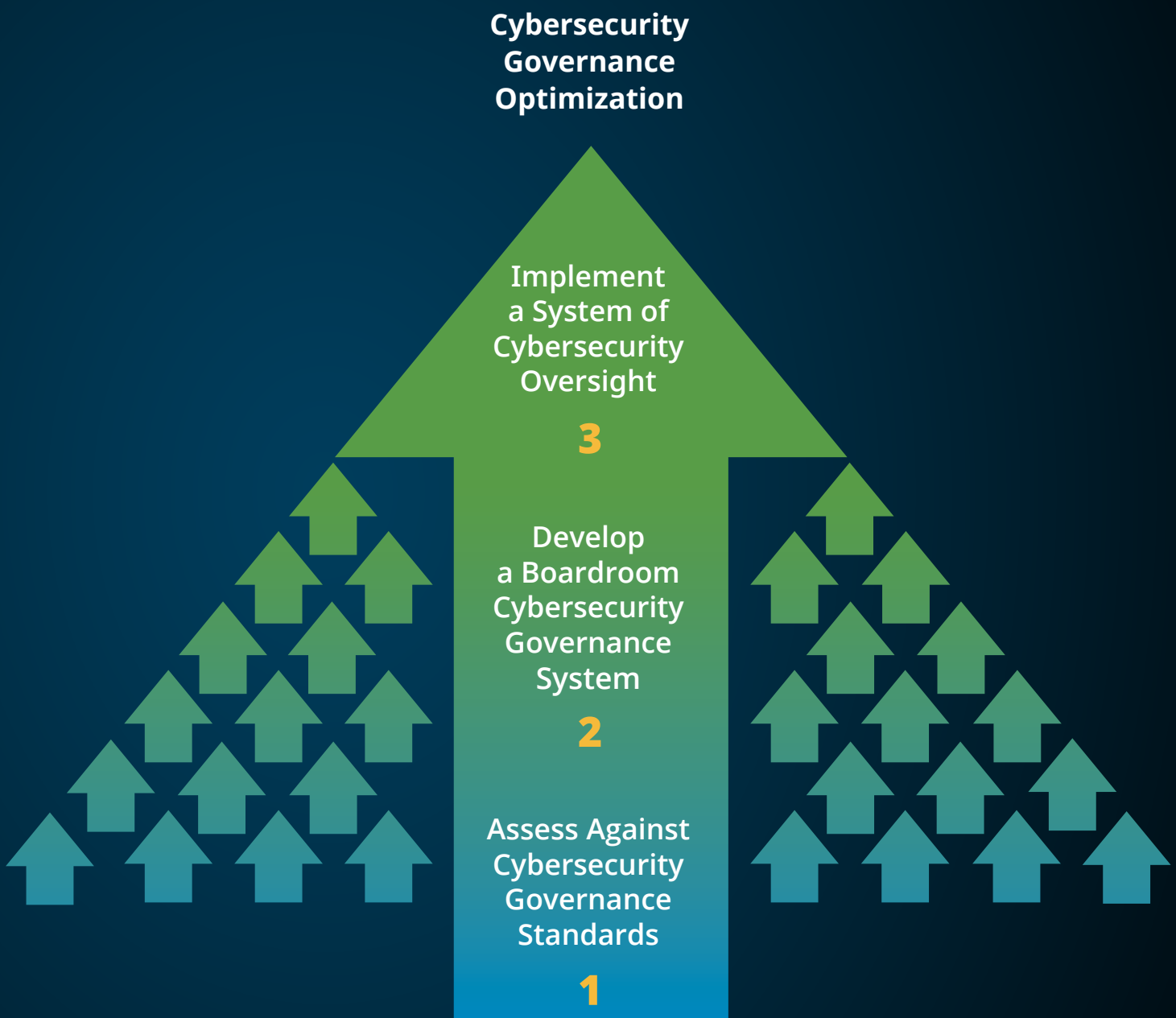
This work is a product of DOMINO 23, the most influential boardroom and executive learning event focused exclusively on digital and cybersecurity governance. This focus, combined with the work, insights, and thought leadership of over 1,300 DDN members during the last six years is creating new knowledge which coalesces and is shared at annual DOMINO events. Through this ongoing mission we will fulfill the goal of continuing to define, document, and distribute practical thought leadership that defines thought leadership on the leading edge of digital and cybersecurity governance. **While all these initiatives are fragmented, uncoordinated, and unfamiliar to many, the goal of *The DOMINO Guide* is to bring the pieces of this puzzle together to define a coherent and concise plan of implementation for boardrooms around the world.**

An oft-heard comment during DOMINO 23 was the imperative that corporate directors and digital and cybersecurity leaders desperately need a mutual understanding, if not a common language, when addressing digital opportunities and cybersecurity in the boardroom. The work of DDN, and the objective of *The DOMINO Guide* is focused on meeting this challenge.

Thank you to our members, DOMINO 23 attendees, our content partners, our boardroom certified Qualified Technology Experts (QTEs), SEC Commissioner Lizáragga, NIST Director Cheri Pascoe, and the other policy, boardroom, and business leaders who have stepped up to this leadership moment. The DDN community is the leading voice on solutions in digital and cybersecurity governance. We invite you to join us at future DOMINO executive education events to learn, share, and help advance the practice and profession of digital and cybersecurity risk oversight. Your investors and stakeholders will thank you, as do I, for being a leader working to shape and secure the digital future.

Bob Zukis

DDN Founder and CEO
bob@digitaldirectors.network


Cybersecurity Governance Optimization
Implement a System of Cybersecurity Oversight
3
Develop a Boardroom Cybersecurity Governance System
2
Assess Against Cybersecurity Governance Standards
1

The Boardroom Journey to Cybersecurity Governance Optimization

DOMINO 23 was the beginning of a transformative journey towards the digital future.

This journey recognizes that digital leadership is critical to the future and the digital ecosystem that powers it.

From the opening keynote by Securities and Exchange Commissioner **Jaime Lizárraga** to the final session on cybersecurity risk boardroom reporting, DOMINO 23 provided learning content that distilled the essence of these issues into actionable insights. Ones that enable corporate directors to effectively oversee increasingly complex digital business systems—both their upsides and downsides

The benefits of boardroom leadership in digital and cybersecurity oversight extends from value creation to business and litigation risk reduction.

While cybersecurity governance is today's fiery issue in the corporate boardroom, digital innovation is the platform upon which it burns.

Governing the convergence of digital innovation and cybersecurity is the core of the DDN mission, DOMINO 23, and *The DOMINO Guide*. Systemic risk has also emerged as a material threat to economic growth and output for nation states and businesses alike.

The DOMINO Guide mirrors the content structure from DOMINO 23 and provides any boardroom or corporate director with actionable insight that not only defines the digital and cybersecurity governance problem, but offers solutions to it along with a path for implementation.

Many of our comments are specific to the issue of cybersecurity governance, although we address the boardroom's role in governing digital innovation and the equal need for digital innovation governance reform where relevant. The solution to this puzzle has three layers to it.

We include 16 boardroom action items to offer a roadmap for implementation.

Boardroom Action Item #1: Segment the boardroom challenges in digital and cybersecurity governance into **three solutions areas**:

- **Standards:** Learn from and leverage existing standards as guidance and as an assessment baseline for creating a path towards digital and cybersecurity governance optimization. Adopt and develop new standards to optimize your board's governance effectiveness.
- **The Governance System:** Recognize that to be effective, governing digital and cybersecurity is a system in and of itself—this system is about how the board does its job. It is comprised of director skills, boardroom structure, and the proper scope of risk understanding and oversight related to the complex digital business system.
- **The Oversight System:** Understand the three types of digital and cybersecurity risk requiring boardroom oversight. This system is about effective processes that enable governance of the unique types of risk related to digital

HEARD AT DOMINO 23

The objective behind cyber expertise in the boardroom is not about improving the questions that directors ask, but in improving the ability of corporate directors to understand the quality of answers from management about cybersecurity risk.

systems. Directors need to govern opportunity risk, cybersecurity risk and systemic risk related to the complex digital business system.

Boardroom Action Item #2: Prioritize self regulation as the most effective way to optimize digital and cybersecurity governance policies and procedures. Do this by viewing the boardroom as a critical control point in digital and cybersecurity risk. Strengthening the boardroom strengthens the entire system. Regulators lag market realities; optimization requires leaders to define and implement new approaches.

The Final SEC Cybersecurity Disclosure Rules

The SEC cybersecurity governance disclosure rules are transformational in some respects but fall short in others. Notably, they fall short in further strengthening the boardroom and director capabilities as a critical cybersecurity control by leaving the cyber expertise disclosure proposal out of the final SEC rules.

However, leading boardrooms are optimizing digital and cybersecurity governance by already going beyond the SEC disclosure rules. While the SEC's regulatory actions represent a watershed moment that will begin to usher in a new era of regulatory driven digital and cybersecurity governance reform, they represent a starting point. The finish line will be defined by boardroom leaders worldwide, like you.

The SEC's final disclosure rules have common ground with DDN's thought leadership on digital and cybersecurity governance. From understanding the impact of cyber risk in the context of business value and materiality to addressing the unique nature of systemic cyber risk, the SEC's disclosure requirements reflect some of the leading governance practices that DDN has been on the forefront of identifying and advancing.

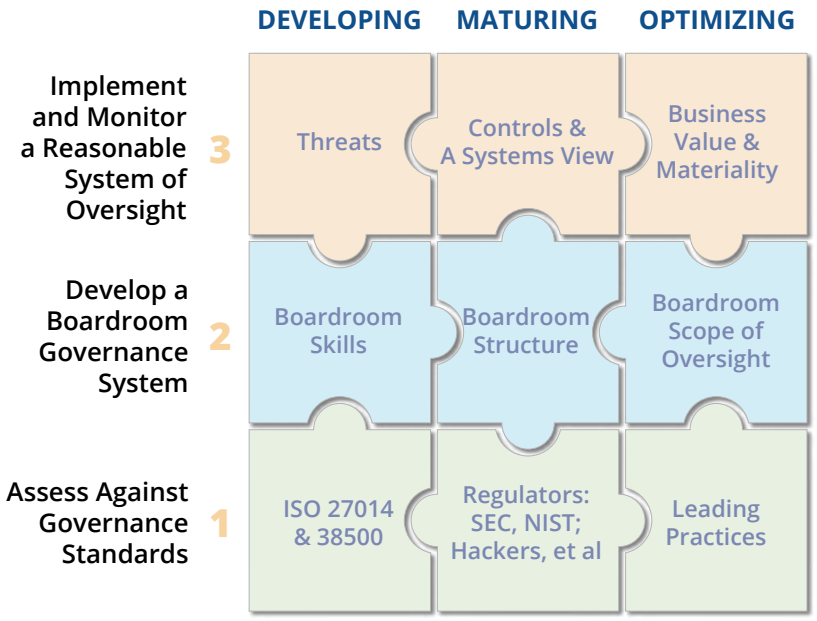
Throughout *The DOMINO Guide* we identify relevant issues related to the final SEC disclosure rules.

1. The Standard Bearers in Digital and Cybersecurity Governance

DOMINO 23 was a seismic turning point in the boardroom where corporate directors, IT, and cybersecurity leaders took the lead in digital and cybersecurity governance—one that moved well beyond admiring the problem to one focused on solving it. As the creators and purveyors of the risks their innovations have unleashed, there is no one better positioned to solve the challenges of digital and cybersecurity governance than the ones who have dedicated their careers to creating, implementing and protecting these technologies.

While digital and cybersecurity governance is an emerging issue, it is a governance domain not entirely without standards. These standards have been developed and are maturing from multiple sources and are both informal, i.e., suggestive, and formal regulatory requirements. All of these sources and standards bearers in and of themselves offer thoughtful and applied guidance for any corporate director or boardroom to learn about the basics on these issues. Together, however, they form a foundation and goal post that every board can use to advance and optimize their digital and cybersecurity oversight policies and practices as a high-performing part of their corporate governance processes.

CYBERSECURITY GOVERNANCE OPTIMIZATION



The starting point for any corporate board to establish a cybersecurity benchmark is ISO 27014.

Start with Basic Standards. The world's leading standard's setter, the International Organization of Standardization (ISO) has established a useful cybersecurity governance standard—*ISO 27014: Information security, cybersecurity, and privacy protection—Governance of information security*[1]. ISO is an organization that "brings together experts globally to share knowledge and develop voluntary, consensus-based, market relevant international standards that support innovation and provide solutions to global challenges.

ISO 27014 establishes the following six key cybersecurity governance objectives:

- Establish integrated comprehensive entity-wide information security.
- Make decisions using a risk-based approach.
- Align information security with new activities from innovation to operations.
- Ensure conformance with internal and external requirements.
- Foster a security-positive culture.
- Ensure the security performance meets current and future requirements of the entity.

ISO 27014 also recommends that there are four core governance processes that should work together to effectively enable the board to oversee information systems. Board policies and processes

for cybersecurity governance should enable directors to effectively evaluate, direct, monitor, and communicate on relevant cybersecurity issues. These processes reflect a system of proactive actions that corporate directors should perform to govern cybersecurity effectively. Notably ISO reinforces the need for corporate directors to be able to evaluate management's information security policies and programs, not just ask questions about them.

ISO has a well-developed standard focused on governing the digital upside: *ISO 38500 Information technology—Governance of IT for the organization*. Together these two standards reflect a basic foundation of processes, practices, and policies in digital and cybersecurity governance that have existed for some time, although many boardrooms have not been aware of, or taken advantage of them.

Boardroom Action Item #3: Benchmark your existing boardroom policies and practices against ISO 27014 and ISO 38500 to assess the board's current state of digital and cybersecurity governance against a reliable and foundational baseline.

Regulators are Maturing Cybersecurity Governance Standards. For the first time, regulators are recognizing the need for more directive policy that forces boardrooms to mature cybersecurity governance policies and procedures. Leading the way is the SEC with its recently announced cybersecurity disclosure rules.

Shaping and maturing the standards in digital and cybersecurity risk oversight was on the agenda at DOMINO 23.

NIST is updating its well-known Cybersecurity Framework (CSF) to address governance, which is due out in early 2024. On Day 2 of DOMINO 23, a unique all-hands working session was conducted between attendees and **Cherilyn Pascoe**, Director, National Cybersecurity Center of Excellence The session was facilitated by **Tony Cole**, DDN Advisory Board Member, retired CTO, and former lead information security executive at the Pentagon. Cole also leads the DDN working group providing advice to NIST on CSF 2.0. This all-hands working group provided the opportunity for DOMINO 23 attendees to help shape CSF 2.0 and provided NIST leadership with practical and actionable input.

Like its initial version, Pascoe explained, NIST CSF 2.0 will be mandatory for all federal government agencies and voluntary for industry. It is the first significant update to the widely adopted framework since the release of CSF 1.0 in 2018. CSF 1.0 has been implemented in organizations in many countries around the globe and across many large U.S. companies. Pascoe explained that the revisions "are intended to keep pace with technology and the evolving threat landscape, reflect lessons learned, and move best practice to common practice."

CYBERSECURITY GOVERNANCE OPTIMIZATION

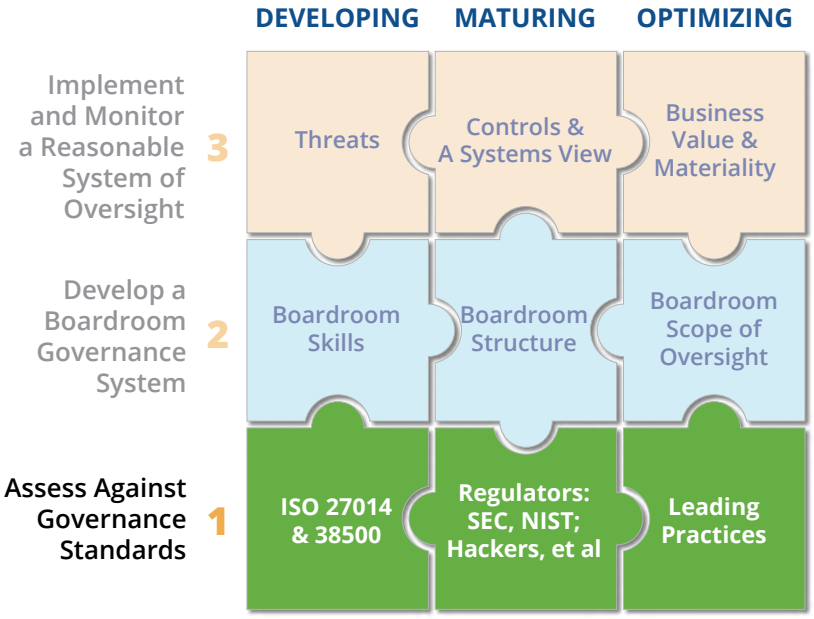


Figure 2 Cyber's Puzzle™

Of significance in CSF 2.0 is the proposed new *govern* function to join *identify*, *protect*, *detect*, *respond*, and *recover* as the existing CSF 1.0 functions.

Notable proposed additions to the NIST CSF 2.0 *govern* function reflect the core concepts in *The DOMINO Guide* and DiRECTOR framework. Identified below by their designations in the NIST CSF 2.0 Reference Tool, they include:

GV.OC-01: The organizational mission is understood and informs cybersecurity risk management.

- This important step aligns cybersecurity to business value. This critical anchor point also reflects the value behind moving cybersecurity governance

from the audit committee to a dedicated technology and cybersecurity committee.

GV.OC-02: Internal and external stakeholders are determined and their needs and expectations regarding cybersecurity risk management are understood.

GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed.

GV.RM-03: Enterprise risk management processes include cybersecurity risk management activities and outcomes.

- This function firmly affixes cybersecurity as a core part of enterprise risk management.

GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.

- Reflecting the important systemic function of "Risk Communications" within the DiRECTOR framework, this CSF 2.0 function extends the importance of cybersecurity risk communications beyond the organization to third parties. This function also aligns to the SEC disclosure requirements on third-party incidents and risk.

GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.

- This function is another regulatory step towards bringing the economic quantification of cybersecurity risk forward and also will support the SEC's disclosure requirement of determining incident materiality.

GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions.

- This function is all about "Opportunity Risk" within the DiRECTOR framework, one of the three key areas of risks that corporate directors have responsibility for in cybersecurity risk and systemic risk oversight.

GV.RR-01: Organizational leadership (e.g., directors) is responsible and accountable for cybersecurity risk and fosters a culture that is risk aware, ethical, and continually improving.

- Affirms that the board and corporate directors are critical to the cybersecurity system and not apart from it.

The SEC Changes the Game with New Cybersecurity Disclosure Standards. Disclosure is a useful SEC regulatory tool. It forces transparency, accountability, and critical thinking around issues that are of importance to investors and other stakeholders.

The SEC's new rules apply to U.S. domestic registrants as well as foreign private issuers subject to SEC rules. And as was the experience with the board reforms imposed because of the Sarbanes-Oxley legislation in 2002, we expect many private company boards and boards around the world to see the cybersecurity disclosure governance reforms now put in place by the SEC as maturing practices.

With the goals of better informing investors about cybersecurity risk management, strategy, and governance and to provide more timely and consistent notifications of material cybersecurity incidents, the SEC cybersecurity governance disclosure rules include advancements in several key areas:

1. Incident disclosure is now triggered when the company determines an incident to be "material" as defined by existing securities case law. This will have the effect of forcing companies to understand cybersecurity risk in a business value context and put the CISO at the front of the room with disclosure committees, the C-suite, and boardroom.
2. New disclosure requirements are now required for material incidents and risk from third parties. This will usher in systemic cyber risk as a new dimension in enterprise risk management. With the realization that risk in complex digital systems exists in a distributed and complex environment, this disclosure requirement will transform risk management.
3. A new disclosure requirement has been imposed to describe management's processes for assessing, identifying, and managing material risks from cybersecurity threats. This will drive critical thinking around the overall system, drive maturity, and expose gaps throughout the system.

The team had an "aha" moment when business leaders realized that they were building an analysis and decision matrix which would allow a corporate board to determine if a cyber incident is material under the SEC rules. Understanding an incident and how it impacts the organization's balance sheet, financial statement, market capitalization along with other direct and indirect value drivers both quantitatively and qualitatively gives management teams the foundation for making a materiality determination.

4. Disclosure is now needed of the board's oversight role including committee responsibility and risk communications in cybersecurity. This will improve transparency and maturity of the board's system of cybersecurity governance and its cybersecurity oversight.

DDN has prepared a detailed analysis of the new SEC rules. (See "Additional Reading," opposite page 34, for link to DDN's detailed analysis of the final SEC cybersecurity disclosure rules.)

From the United States to Nigeria and Malaysia, visionary corporate directors have not been waiting on regulators—they have been creating and implementing new cybersecurity governance policies and practices on their own.

Leading Boards Are Optimizing Cybersecurity Governance. As groundbreaking as the SEC's new disclosure rules are, there are other "standards" in the form of leading practices and policies which already go beyond these rules. These self-regulatory steps represent the leading edge in digital and cybersecurity risk oversight and are being advanced by thoughtful and informed directors and executives around the world.

These policies include transformational practices across the entire system of governance including director skills, boardroom structure, and the scope of the board's risk understanding and oversight, including:

- Boards are using an expanded competency matrix for corporate directors beyond cybersecurity to identify and assess digital director experience at a more detailed level.
- Boards are already adding and disclosing whether directors have cyber expertise on the board, e.g., GM discloses that five of its directors have cybersecurity experience.
- Boards are also adding multiple digital directors beyond cybersecurity with expertise across other domains within complex digital business systems, e.g., data, information architecture, risk communications, emerging technology, third-party and systemic risk management, and IT operations and regulation. MIT research has also identified that three digitally savvy directors on the board is the tipping point that drives significant positive financial impact for the business[2].
- Disclosures include the description of classes, programs, or certifications that directors receive on digital and cybersecurity issues and governance.
- Boards are moving cybersecurity governance to a committee other than the audit committee.
- Boards are establishing a Technology and Cybersecurity Committee (TCCC) on the board, e.g., over 200 boardrooms in the U.S. R3000 have taken this step.
- Boards have a detailed and comprehensive TCCC charter that reflects responsibilities across each of the domains of the complex digital business system.
- TCCC charters are tasking corporate directors as advisors to management in cyber and IT, e.g., FedEx.
- Boards are closing information asymmetries between committees focused on information systems risk and enterprise risk through multi-committee directors or explicitly written charter responsibilities for coordination between committees.
- Boardrooms and/or management are already quantifying the potential economic impacts of cyber risk to understand self-insured exposure levels in financial terms.
- Comprehensive disclosures are made that describe the board's policies and procedures in overseeing cybersecurity.

- Disclosures include the frameworks used by management and the board for understanding and monitoring systemic cyber risk.
- Risk disclosures are made that explain systemic risk issues into, or from, the organization's complex digital business system.
- Comprehensive risk disclosures are made that cover each of the domains of the complex digital business system, i.e., data, information architecture, risk communications, emerging technology, cybersecurity, third-party and systemic risk management, IT operations, and regulation.
- Management is monitoring third parties to identify leadership control gaps as a systemic cyber risk and reporting this along with other key systemic cyber risk metrics to the board.
- Boards regularly meet in executive session with the CISO or other information security executive.
- The board engages experts to perform third-party assessments of management's information security program and to educate and advise directors on cybersecurity.

These policies and procedures along with others, can be adopted and implemented by any corporate board interested in maturing and optimizing their processes in cybersecurity governance. From the courts to policy makers such as the SEC, NIST, and even The White House, cybersecurity governance policy reform is accelerating, as is regulatory accountability. The best performing boards on these issues are already ahead of the regulators.

The DDN DiRECTOR™ framework is the only governance and management framework focused on identifying systemic risk issues in complex digital systems. Several learning sessions on how some of America's leading companies are applying the framework for just this purpose were presented at DOMINO 23.

As the legal and regulatory environment begins to catch up, more corporate boards will be forced to evolve and advance their critical thinking about their approach to cybersecurity issues.

Boardroom Action Item #4: Evaluate the board's digital and cybersecurity practices against leading practices to identify gaps, establish the desired level of maturity in cybersecurity governance, and determine the actions needed to close the identified gaps.

Boardroom Action Item #5: Monitor regulatory developments and leading digital and cybersecurity governance practices from boardrooms around the world to continuously improve and optimize cybersecurity governance policies and practices.

The Final SEC Cybersecurity Disclosure Rules

Several definitions in the final SEC rules were clarified that are fairly profound. *Cybersecurity incident* is defined as an unauthorized occurrence but clarified in the final rules to include accidental occurrences. This expands the definition of a cybersecurity incident that requires disclosure to include material outages and failures not triggered by malicious activity. This correction/clarification is a fortunate one for investors and properly expands disclosure to reflect the reality of cybersecurity risks that the digital business system faces. Failures and errors will now be disclosable if deemed material. This will force management teams and boards to have a much deeper understanding of the systemic nature of the complex digital business system and where risk lies throughout the system.

Information system was also defined to include resources owned or used by the registrant. This will require disclosure related to the systems of third parties that the registrant uses for services such as cloud computing. This will also force management for the first time in many cases, to analyze, understand, and monitor the distributed risk environment inherent within their complex digital business systems.

2. Develop a Boardroom Cybersecurity Governance System

Corporate governance in and of itself is a complex system. At DDN, we are the leader in teaching concepts derived from complex systems science as they apply to the digital business system, corporate governance, and enterprise risk.

HEARD AT DOMINO 23

The biggest challenge has been the boardroom and CISO don't speak the same language or have similar backgrounds. But DiRECTOR is like a Rosetta Stone that translates systemic risk in the digital system effectively for both sides of the boardroom.

Implementing an effective approach to governing cybersecurity requires boardroom transformation to converge around two complex systems: the system of *corporate governance* by which directors approach cybersecurity governance, and the reasonable *system of oversight* that the board applies in overseeing the cybersecurity risks that the organization faces. These systems focus on *how* the board does its job, and *what* they oversee related to the digital business system.

In general, a high-performing system of corporate governance relies upon three critical and complementary parts of the boardroom working together that enables how the board performs its job:

1. The *skills* in the boardroom.
2. The *structure* of the board.
3. The boards *scope* of risk oversight.

This basic structure and system are ingrained in the significant corporate governance reforms imposed by the Sarbanes-Oxley Act of 2002. Effective cybersecurity governance relies upon all three parts of this complex system for governance to be a strong control in the overall system of cybersecurity for the organization. All three parts need to be consciously considered, and complementary in design and function for an effective cybersecurity governance system to emerge, e.g., a boardroom system without director cybersecurity expertise will be less effective than one with these director competencies.

Boardroom Action Item #6: Recognize that the digital and cybersecurity governance problem is a systems challenge requiring development, maturity, and coordination between three key parts of the governance system: director skills, boardroom organizing structure, and the board's scope of risk oversight.

Boardroom Cyber Skills. The director digital skills debate is about much more than cybersecurity expertise. While recruiting new corporate directors with cyber and digital governance expertise is not without its challenges, it would be wrong for corporate boards searching for qualified digital or cyber experts to view these executives too narrowly—an assertion unanimously refuted by experienced executive and boardroom recruiters at DOMINO 23. Where to find them, the number of them needed in the boardroom, and their ability to contribute to the broader boardroom agenda are the most frequent challenges heard. These challenges should not supersede the need for these director capabilities in the boardroom however.

CYBERSECURITY GOVERNANCE OPTIMIZATION

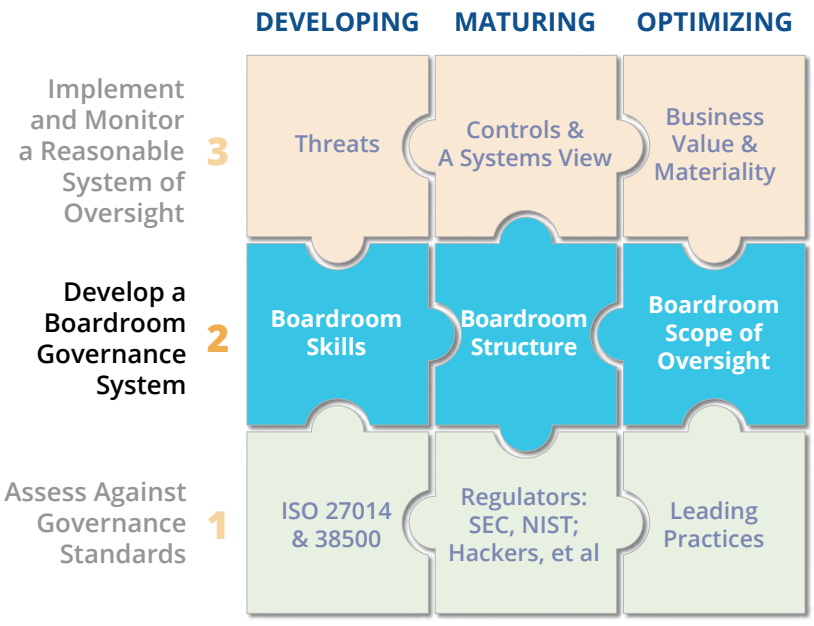


Figure 3 Cyber's Puzzle™

At

The Final SEC Cybersecurity Disclosure Rules

While the SEC left director cyber expertise disclosure out of its final rules, several of its new and final disclosure rules will nonetheless work to positively contribute to the CISO's journey into the boardroom. Moreover, leading practice boards are continuing to add these skills to the boardroom in recognition that the board is a critical control in the overall system of cybersecurity.

During the SEC's open webinar on the final rules, SEC Commissioners Caroline A. Crenshaw and Lizárraga acknowledged that this issue is something that both the SEC and the U.S. Congress could revisit. DDN believes that the director cyber expertise omission is the most significant shortcoming in the SEC's final rules—one that fails to implement a common sense, high impact/low effort disclosure requirement that would significantly benefit the boardroom and registrants by improving the cyber tone at the top of American business, reducing cybersecurity risk, and benefitting investors.

DOMINO 23, four leading boardroom and executive recruiters shared their insights and guidance on board preparedness in cybersecurity governance. The panel was comprised of recruiters who specialize in filling board seats and who are paying close attention to the boardroom cyber expertise issue: **David Arenas**, managing principal at James Drury Partners; **Jeff Anderson**, managing partner of The Goodwin Group in Atlanta; **Rochelle Campbell**, CEO of Leadership Elevated, and a National Cybersecurity Committee Member at the Private Directors Association; and **Jamie Lopez**, a partner at Korn Ferry.

Advice aimed at the CISOs and CIOs in the audience who are interested in securing their first board seat was to orient their roles and their impact to how the digital business system impacts the organization's value proposition including its balance sheet, financial statement, and market value. Something they will now be required to do under the final SEC cybersecurity disclosure rules.

By emphasizing the significant role that they have in protecting a vast majority of the organization's economic output and growth, CISOs will reframe their importance to the C-suite and boardroom. In addition, these leading boardroom recruiters suggested that CISOs should capitalize on the breadth of their experiences to show a progression of professional growth beyond their technical expertise. Emphasizing their crossfunctional teaming, broad business acumen, and breadth of general business competencies is helpful as these competencies are frequently sought after by corporate boards.

The trope that CISOs are one-dimensional specialists unprepared to contribute across the boardroom agenda, something frequently heard in the governance community, was widely refuted at DOMINO 23. It was noted during DOMINO 23 that this was also an inaccurate bias held against financial experts when SOX initially proposed a similar rule for director financial experts in 2002.

They also raised as a high-priority tactic for IT and cybersecurity leaders pursuing corporate directorship the importance of seeking the support of their CEO to ensure that their role as a CIO or CISO is board facing. This high-impact tactic is seen as a way to gain exposure to board work, dynamics, and possible mentorship on their pathway to the other side of the boardroom table.

Being recognized as a cyber expert is something that will open boardroom doors for CISOs as leading boards continue to add these capabilities, but CISOs still need to show distinction and accomplishments beyond this valuable boardroom competency to differentiate themselves if pursuing directorship. With the CEO and CFO heavily involved in disclosure controls and procedures, both the CIO and CISO have new opportunities to engage and reframe their value propositions as the new SEC disclosure rules will put them in the front of the room on these issues.

Other new rules, including the shift to "materiality" as the incident-disclosure trigger, will serve to push CISOs into disclosure committees and require CISOs to convey cybersecurity risk in business value and investor materiality terms. CISOs will need to take the lead on making a materiality recommendation

The General Motors boardroom was highlighted at DOMINO 23 for its leading practices in director cybersecurity experience disclosure. GM already discloses that five of its directors have cybersecurity experience. Leading boards are not waiting for regulation on this issue, they already recognize that adding digital cybersecurity experience and expertise is a foundational part of their system of cybersecurity governance.

related to a cybersecurity incident based upon a decision matrix or heuristic that they themselves will need to design and establish. This new opportunity to lead will demonstrate CISOs' capabilities beyond their technical competencies. Moreover, the complexity of the materiality discussion might challenge directors and force them to recognize that cybersecurity risk is a unique aspect of enterprise risk that does in fact require directors with cyber expertise in the boardroom.

Boardroom Action Item #7: Recruit directors with deep applied digital and cybersecurity expertise, and add this disclosure as it is useful information for investors. Leading practice is a critical mass of three digitally savvy directors.MIT research has identified that companies whose boards have a critical mass of three digitally savvy directors achieve significant business benefits in revenue growth, profitability, and market valuation[3]—supporting the conclusion that boardroom leadership in digital and cybersecurity governance matters.

Boardroom Action Item #8: Deliver annual training for all directors on each of the three aspects of risk management that relate to the complex digital business system. All directors should receive annual training on issues in digital innovation, cybersecurity, and systemic cyber risk.

Boardroom Action Item #9: Expand the digital competency model for corporate directors to include all of the domains of a complex digital business system. Assess corporate director experience across each of the domains of the DiRECTOR™ framework. Identify immediately if one director could be named as a cyber expert, and close this director gap if it exists as a priority leading practice.

Boardroom Organizing Structure. How the board organizes itself on any issue plays a significant role in how effectively the board oversees those issues. Leading and lagging practices in how boards organize their responsibilities and activities around cybersecurity was a focus of the *QTE 501 Boardroom Masterclass for IT and Cybersecurity Executives* held the day before DOMINO 23 started. With almost 40 IT and cybersecurity leaders attending, this issue was covered in depth through case studies on Solarwinds, FedEx, Ford, and others.

Research on the benefits of board committees identify the following advantages[4]:

- Task efficiency to these issues within the committee;
- Greater focus on the issues in depth and breadth;
- Knowledge specialization within the committee;
- Greater accountability around the issue to management and the full board.

The leading practice of moving cybersecurity oversight out from the audit committee and into a Technology and Cybersecurity Committee (TCCC) is already transforming over 200 of America's Russell 3000 boardrooms, including FedEx, GM, Hasbro, AIG, Verizon, and many other well-known companies.

DDN in 2018 called on U.S. public company boards to implement a Technology and Cybersecurity Committee (TCCC) as a significant step in maturing digital and cybersecurity governance[5].

TCCCs are powerful tools that establish an adaptive governance model for new information technology developments and innovations (e.g., AI). Given the broadening scope and reach of information technologies, these issues will only become more significant in their impacts on the organization, easily eclipsing the targeted scope and focus of an audit committee or the time and capability of the full board.

By defining and documenting responsibility and scope of digital and cybersecurity oversight in a TCCC charter, boards will establish an adaptive blueprint for effective oversight of the digital

HEARD AT DOMINO 23

Audit committees can become the "kitchen junk drawer" of corporate governance. The SEC's chief accountant has even questioned whether cyber belongs in the audit committee and whether the right director skills and attention are able to be provided to the dynamic nature of cyber risk when this is relegated to the busy agenda of the audit committee. Notably, the MGM board tasked its audit committee with cybersecurity risk oversight.

upside and its downsides—one overseen by a group of directors with the breadth and depth of digital and cybersecurity skills. DDN has created a leading-practices TCCC charter (available for DDN members online). Investors should look to this committee as a strong control related to the board's effective involvement in digital innovation and cybersecurity risk.

Boardroom Scope of Risk Oversight. The final part of the cybersecurity governance system that boards need to put in place focuses on the three dimensions of digital risk that are core to their oversight responsibilities. The risks related to complex digital systems are broader than how risk has been defined by many boards or management team, and includes not just what can go wrong, i.e., cybersecurity risk and systemic cyber risk, but also what needs to go right for the digital business system to drive economic growth and output i.e., opportunity risk.

Risk oversight of the complex digital business system had a front row seat at DOMINO 23. CISOs, CIOs, and corporate directors at DOMINO 23 weighed in on the scope and challenges of risk oversight as it relates to the digital business system that powers their companies. The point was made that every corporation, its board, and its digital business systems are products of their unique composition, culture, and circumstances. This was emphasized by former cybersecurity executive and current public and private company corporate director, **Linda Medler**.

> "If you've served on a board then you've served on one board," observed Medler, QTE, retired U.S. Air Force Brigadier General, and a director who serves on multiple corporate boards. The same can be said of most digital systems: they are built over time to serve an increasing array of functions. The introduction of every new digital product and/or service increases the cyber threat vectors that contribute to changing dynamics in risk appetite and risk tolerance analysis in the boardroom and corporate decision-making," she said.

Medler's comments caution against the dangers of making or relying on generalizations on these issues and the need to build adaptable and resilient systems that deal with them. General Medler hosted a veterans' leadership and networking breakfast at DOMINO 23 for DDN members and QTEs from the armed forces who are now leading their organization's approach on cybersecurity governance.

The Final SEC Cybersecurity Disclosure Rules

The SEC did specifically address the issue of disclosure related to boardroom structure of cybersecurity oversight in its final rules. The new rules now require annual disclosure of whether a board committee or subcommittee is responsible for cybersecurity oversight. Disclosure is also required of the board's role in the oversight of cybersecurity risk and the processes by which the board or committee is informed about cybersecurity risk.

With the majority of public company boards currently relegating cybersecurity governance to the audit committee, disclosure transparency may now create some critical thinking as to whether this is an effective practice.

Cybersecurity is but one important part of the scope of director's responsibilities. Risk oversight for the high-performing corporate boardroom should cover three distinct aspects of digital risk:

- **Opportunity risk:** The transformative value-creating impacts, economic growth and output implications of digital innovation.
- **Cybersecurity risk:** The active and malicious cyber threat environment that the organization faces because of the digital business system.
- **Systemic cyber risk:** The inherent risks within the complex digital system that threaten the purpose of the system within the enterprise, and beyond.

While regulators are focused on cybersecurity and ensuring boards effectively govern the malicious and value-destroying threats to digital systems and their impacts on consumers, investors, and other stakeholders, leading boardrooms also govern the economic value-creating aspects of these technologies.

Defining the proper scope of director risk oversight and adopting processes that reflect this comprehensive definition of digital and cybersecurity risk oversight has been a major shortcoming in advancing the effectiveness of many boardrooms in overseeing digital and cybersecurity risk.

Systemic cyber risk is also a new and very unique dimension of enterprise risk. A symptom of the complex human-made world, this risk is going ungoverned and unmanaged in many organizations, but is front of mind for attackers.

Boardroom Action Item #10: Define the scope of the board's digital oversight responsibilities more broadly to include opportunity risk. Update disclosures to reflect all three aspects of risk.

Boardroom Action Item #11: Implement a Technology and Cybersecurity Committee as a leading practice in boardroom structure and organization, moving cybersecurity oversight out from the audit committee. Use the DDN leading practices charter as your guide for defining the scope of risk oversight for this committee.

Boardroom Action Item #12: Train directors and executives on concepts of complex system science to develop an understanding of systemic risk and the nature of distributed risk inherent within the complex digital business system.

Boardroom Action Item #13: Ensure management adopts disclosure controls and procedures to reflect systemic risk including third-party risk. Consider boardroom and executive training and adoption of the DiRECTOR™ framework for governing and managing systemic risk.

CYBERSECURITY GOVERNANCE OPTIMIZATION

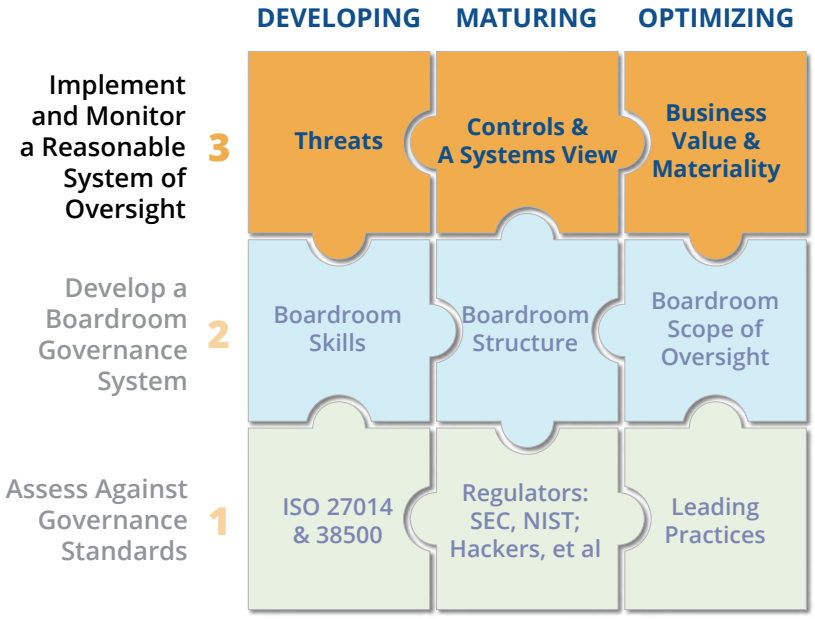


Figure 4 Cyber's Puzzle™

The Final SEC Cybersecurity Disclosure Rules

The SEC recognized economic dependency and the unique nature of systemic risk related to information systems in its final rules when they said, "...an ever-increasing share of economic activity is dependent on electronic systems, such that disruptions to those systems can have significant effects on registrants and in the case of large-scale attacks, systemic effect on the economy as a whole"[6].

Notably the SEC also now requires incident disclosure and risk disclosure related to processes to oversee and identify material third-party risks. This is a significant new development in risk management that will challenge most companies and boards. Currently, visibility into and understanding of the organization's distributed risk environment and how risk can spread between highly interconnected systems is an underdeveloped area of enterprise risk management.

The SEC also clarified that its cybersecurity incident disclosure definition includes accidental occurrences. The omission of this in its proposed rules indicates the Commission's lack of a full understanding of the changing nature of risk related to complex digital business systems.

3. Implement and Monitor a System of Cybersecurity Oversight

Once a system of effective governance is in place that empowers the board with the right skills, an efficient organizing structure, and the proper scope of risk understanding, an effective boardroom system of oversight can develop.

In the SolarWinds shareholder derivative complaint related to its well-known cybersecurity breach, the complaint charged the board for "...their utter failure to implement or oversee any reasonable monitoring system..."[7].

The legal responsibilities of corporate boards and directors are familiar to many directors in the concepts of *duty of care* and *duty of loyalty*. In common parlance in the U.S., the legal responsibility for corporate directors is articulated in the SolarWinds case—to "implement a reasonable system of oversight, and then to monitor it." Fulfilling this legal standard requires a systems view and solution to governing digital and cybersecurity risk. This system of oversight extends from the threat and risk environment facing the organization, through to the controls that management has implemented, to how the digital systems creates value for the organization and to what a reasonable investor would consider material in the event of an attack or error related to the system.

HEARD AT DOMINO 23

What it boils down to is that directors need to know four things:

1. What are we trying to protect?

2. What risks are we worried about?

3. What are we doing about it?

4. And how are we doing?

What boards oversee and how they understand the risk environment related to the digital business system is a critical part of implementing a system of boardroom oversight.

A challenge for many boards and the governance community has been in understanding how to translate new domains of risk, such as digital innovation, cybersecurity, or systemic risk, into a *reasonable system of oversight*.

Based upon the ISO 27014 standard of cybersecurity governance, implementing a reasonable system of cybersecurity oversight for the corporate boardroom involves directors who can effectively evaluate, direct, monitor and communicate around a cybersecurity system that enables them to understand several key issues:

- How cybersecurity and an incident are and can become material in the context of reasonable investor considerations.
- How the complex digital business system drives business value including financial statement, balance sheet, and market value impacts along with other direct and indirect value implications.
- What the parts of the complex digital business system are and how the parts work together to create and deliver business value.
- How management assesses and identifies the threats to the digital system and how those risks can impair business value.
- What controls have been implemented to mitigate those threats, how are the controls performing and what controls are being planned or are missing.
- How much uncontrolled or self-insured cybersecurity risk has the company assumed now and over time, and how much risk has been transferred into the cyber insurance market.

The comprehensive system of oversight that directors implement and monitor needs to address the three areas of risk that emerge from digital systems: opportunity risk, systemic risk, and cyber risk.

The upside of digital innovation or *opportunity* risk is frequently left to the busy schedule of the full board agenda. However, when there is a Technology and Cybersecurity Committee in place, as there is with

FedEx and many other boards, then this issue receives a lot more attention and focus by directors with relevant competencies. At DOMINO 23, the board of FedEx was often cited as a pioneer in digital and cybersecurity policy and practices. It has had this committee on its board since 2000. FedEx was highlighted as earning the grade of **A** from DDN for its policies and practices in digital and cybersecurity governance.

CIOs and CISOs through their boardroom interactions and reporting should strive to inherently fulfill all of these requirements. Corporate directors should also be able to determine if a system of cybersecurity and systemic risk oversight is *reasonable* when they see it.

Cybersecurity incident disclosure for SEC registrants now requires an understanding of materiality in the context of U.S. securities law and the SEC's definitions which are contextual to "a reasonable investor." This requires the development of a materiality decision matrix or heuristic led by the CISO. By leaving this to registrants to determine, the SEC has given management teams a considerable amount of latitude, discretion, and relief from an urgency perspective. However, the SEC's expectation is that making this determination is an informed and deliberative process which will require management teams and boards to have a much more structured view and understanding of the overall digital system and its business value impacts.

Boardroom Action Item #14: Ensure that management has a deliberative process for understanding the impacts of a cybersecurity incident in the context of investor materiality

The Final SEC Cybersecurity Disclosure Rules

The SEC introduced a significant new disclosure that requires a description of the processes that management has implemented for assessing, identifying, and managing material risks from cybersecurity threats. The SEC's expectation is that this is articulated in enough detail for a reasonable investor to understand those processes. This requirement begins to institutionalize the concept of the *system of oversight* that management has in place for cybersecurity risk. This transparency and the critical thinking that will go into documenting and articulating these processes will mature management's system of cybersecurity oversight as a complex process and should be a welcome development for investors.

The SEC focused on "processes" as opposed to "policies and procedures" to avoid providing threat actors with any type of prescriptive insight or roadmap for where a vulnerability could reside. Moreover, the SEC has an expectation that this description will allow investors to identify if there is a risk assessment program in place in enough detail for them to understand the registrant's cybersecurity risk profile.

The SEC also wants registrants to disclose the management responsibility, including committees for assessing and managing material risks and the relevant expertise of such persons with those responsibilities. Risk communications is also an important part of new SEC disclosure rules including how those committees or persons report risks to the board and the processes by which responsible persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents.

The SEC also expects a description of how the cybersecurity processes described are integrated within an overall risk management system or process. **And in another significant development, the SEC also wants to see disclosure about the use of third-party assessors, consultants, or auditors in connection with these processes to indicate for investors how much cybersecurity expertise is insourced or outsourced. This is a curious bit of information that may force issuers to rethink their approach to cybersecurity management as investors develop perceptions of quality as it relates to insourcing versus outsourcing of cybersecurity.**

On March 1, 2023, the White House released a national strategy setting a strong tone at the top of the nation focused heavily on systemic cyber risk. With an unprecedented focus on systemic cyber risk, The White House raised the profile of this new dimension of enterprise risk with the release of its National Cybersecurity Strategy (WHNCS)[2].

The WHNCS establishes the cybersecurity objectives for the nation with the statements:

Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences.

The world is entering a new phase of deepening digital dependencies. Driven by emerging technologies and ever more complex and interdependent systems, dramatic shifts in the coming decade will unlock new possibilities for human flourishing and prosperity while also multiplying the systemic risks posed by insecure systems.

and regularly reviews this. Conduct a tabletop exercise with a cross-functional group of executives on incident to materiality analysis. materiality analysis.

Threats, Controls, and a Systems View. Risk isn't static as new innovations often create new threats and new types of risk. These new risks are commonly unfamiliar to those without experience with them or an understanding of the related innovation. To believe that cybersecurity risk can be governed and managed within the context of legacy risk management competencies and perspectives, is incorrect, as the cyber insurance industry has discovered. Corporate boards and management teams need new capabilities and perspectives to understand and manage these news risks.

The current deliberations around artificial intelligence reflect the challenges in understanding these innovations and the risks they introduce, as many experienced on social media and cloud computing over the last decade. New risks are also frequently only understood in hindsight, when their impacts have been experienced first-hand, as is the case for many cybersecurity incidents.

CISOs already had a difficult job addressing a rapidly evolving threat environment. Systemic cyber risk now compounds that difficulty as these risks exist inherently within every complex digital system. Systemic weaknesses are also increasingly being targeted and leveraged with wide-ranging impact and effect from malicious actors as occurred at MGM.

SolarWInds is an example of a systemic attack where the objective was to efficiently reach SolarWinds customer base—comprised of tens of thousands of companies and government users. Notably, shortly after the SolarWinds breach its board added a technology and cybersecurity committee to the board.

The threat environment that every company faces is unique to that organization and its attractiveness as a target. The controls that any organization has in place are also unique to that company. As the cyber risk landscape changes and new risks emerge, control gaps constantly appear that require ongoing investment to close.

Boards and directors also need to be adaptive in their cybersecurity governance capabilities by staying informed and attuned to the changing risk landscape facing their organizations. These dynamics strongly support the case for annual director cybersecurity training and director digital and cyber experts who have the background and applied experience to understand the existing and emerging risk landscape.

The New World of Systemic Risk in Cybersecurity. A new dimension of risk has arrived in enterprise risk management: systemic risk.

Levels of systemic cyber risk are as high as they have ever been and have been brought about by the sheer complexity and unique traits inherent within the complex digital systems that power economies and businesses around the world.

Systemic risk is the inherent risk within complex systems that can jeopardize the purpose of the entire system because of the failure of one or more parts within the system.

Nowhere was systemic cyber risk more in focus than at DOMINO 23. DDN has pioneered the only framework for governing and understanding systemic risk in complex digital systems known as DiRECTOR™. Almost 500 directors, CIOs and CISOs from leading companies around the world have been trained and certified on it.

In a world of complex digital systems, a new way of understanding systemic cyber risk is needed.

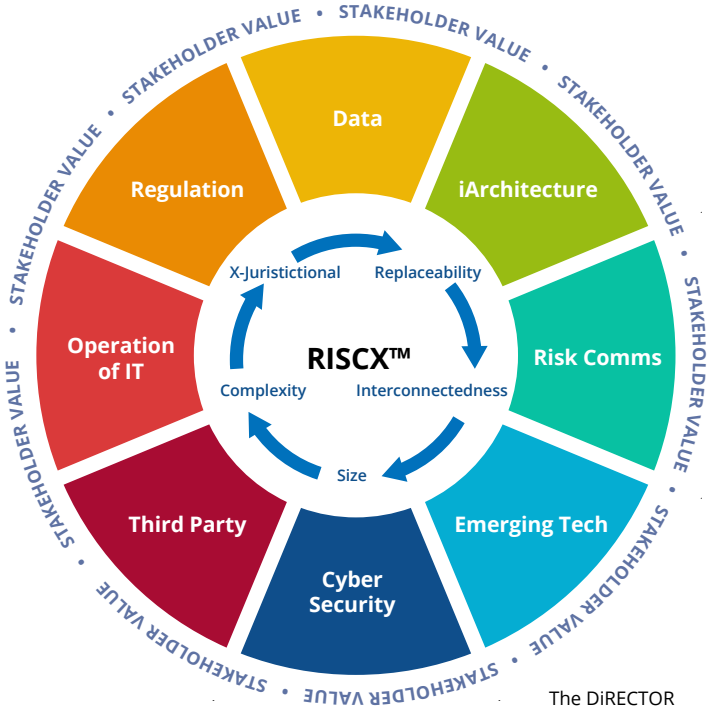
DOMINO 23 was heavily focused on developing these competencies on both sides of the boardroom table. More than 100 of DDN's boardroom certified Qualified Technology Experts (QTEs) attended DOMINO 23. They are experts at understanding and applying these concepts in the context of business value and digital risk and were taught and certified on the DiRECTOR™ framework. Developed by DDN, this framework is the leading structured approach that helps both sides of the boardroom table understand how the complex digital business creates value, what the systemic threats to that value are and how to mitigate them.

Tales from inside corporate cyber commands during DOMINO 23 on the application of the DiRECTOR™ framework took center stage for a highly engaging interactive peer panel learning session led by **Josh Salmanson**, QTE and senior vice president of Telos Corp. Sharing insights and gamely fielding audience questions were **Brenda Bjerke**, QTE, senior director of cyber risk at Target Corp., **Ken Finnerty**, QTE, and president of IT application development at UPS; and **David McLeod**, QTE, and vice president and information security officer, at The Walt Disney Studios.

The audience chuckled when McLeod, asked to describe his role at Disney replied, "Secure the magic." More directly, he emphasized the importance of resilience in the creative production process and the need to have a common understanding of systemic risk. "Our people care about resilience more than anything else, you cannot stop production…We mapped out the [DiRECTOR] framework against all these stakeholders and our conversations with them and found a way to have a single view that mattered."

And what matters, McLeod said, is having a common perspective on systemic risk and its impact on business value. "I'm not going in saying, 'Hey, let me walk you through my internal audit-driven risk management framework.' Instead, I can say, 'I know you care about resilience: here's our initiatives around that, here's funding—are we too high or too low?' I have to choose one conversation that lends itself to a starting point. And that's why [DiRECTOR] is excellent."

Finnerty provided some insights on "data" as the starting point of the DiRECTOR framework and the importance of linking value and risk: "…the inclusion of data, the recognition that data is really the essential ingredient in a digital product is so important. And if you think about it, the framework sets up the idea that you have to understand both the value you're creating as well as the risks associated with it."



The DiRECTOR Framework for Governing Systemic Cyber Risk

The World Economic Forum recently declared systems thinking to be a top skill required of future business leaders[8] and even the SEC called out systemic impacts in the analysis of its final cybersecurity disclosure rules. Both value protection and value creation require corporate directors to be adept at understanding the downside and upside of digital transformations. While systems thinking is not a new concept—it originated at MIT in the 1950s—its application in the boardroom to digital and cybersecurity opportunities and risks is emerging. Embraced by DDN as part of its curriculum, systems thinking was explained at DOMINO 23 by Professor **Joseph Tranquillo** of Bucknell University, who also has published several books on the topic.

With the advent of greater innovations in artificial intelligence, machine learning, and quantum computing, the implications of these new technologies on corporate risk and governance cannot be understated. These advances will add new layers of complexity to an already complex system. In his wrap-up, Tranquillo reiterated some key points: "Systems thinking can be learned. All systems—made up of parts, structures, and flows—can be adapted to solve or create new products or services." The greatest challenge for directors may be opening their minds to new ways of thinking.

A lesson embedded in Professor Tranquillo's engaging talk was the issue of how boards adapt and respond to these types of continuous IT-driven disruptions—building an adaptive corporate governance system is the answer.

Systems thinking and remediating critical systemic vulnerabilities can also create a catalyst for innovation.

DDN's mission in many respects revolves around making the boardroom and business leaders better systems thinkers.

Applying systems thinking concepts to understand business value protection and creation is a dynamic and sustainable way to understand the increasingly complex and interconnected systems that companies rely upon that extend well beyond their direct control.

A masterclass on the most common, but often underappreciated systemic cyber threat, was led by Proofpoint's **Lucia Milică Stacy**. Lucia recently became the CISO of Stanley Black & Decker, Inc. While ransomware receives a lot of attention and is frequently the first topic raised in the boardroom on cybersecurity, the greatest cybersecurity threat resides within the company itself: its people, according to Lucia.

Citing data from the Verizon Data Breach Report, Stacy told DOMINO 23 attendees that 85% of all breaches were caused by a human element versus 3% for a technical vulnerability. Lucia provided two important takeaways for boards:

- Understand that cyber risk is a unique business risk and very different controls are needed to adapt to the systemic threat landscape especially people risk, which is a key systemic vulnerability at every level.
- Make sure that the board has implemented a comprehensive system of cyber risk oversight that addresses both cybersecurity risk and systemic cyber risk, and that both issues are diligently monitored and documented.

Boardroom Action Item #15: Deliver director and executive education on concepts in complex systems science and systems thinking. Full boards and individual directors can join DDN where these concepts are being taught and developed.

Boardroom Action Item #16: Adopt cyber risk quantification determination as a core practice. Nothing focuses a boardroom or management team more than when they understand the economics of their cybersecurity self-insurance levels. Quantifying the amount of business value dependent upon the digital business system along with the controlled and uncontrolled levels of cyber risk is the starting point of any materiality analysis. This will become a key part of cybersecurity incident materiality determinations which will also need to consider qualitative implications..

Business Value and Materiality. The SEC has raised the stakes on cybersecurity by shifting cyber disclosure to when a registrant determines an incident to be material.

Business value that is at risk because of the digital business system is the starting point for any corporate board in effectively governing cybersecurity, but it is not often articulated clearly in communications between boards and CISOs.

This is one of the most transformational new disclosure requirement within the final SEC rules. While it is a positive development for investors, implementation will come with some challenges.

The topic of materiality was a focus during DOMINO 23 masterclasses led by content partners Secure Systems Innovation Corp.'s X-Analytics, the leader in cyber-risk economics analysis and quantification, and the law firm White Case.

X-Analytics delved deep into cyber economics to showcase its framework for determining digital value in financial terms. The proprietary models stem from applied economics—the combination of traditional economic theory and specific field-based statistical methods and data analytics—to project the financial impacts of cyber-based events.

Determining the amount of business value at risk in dollars and cents enables management, boards, and technology executives to clearly understand the linkages between information systems, their value, and evaluate whether the actions being taken to protect and mitigate risks to that value are sufficient.

Kevin Richards of X-Analytics, who taught the masterclass, added this:

"Many CISOs believe that the way they present cyber risk to their corporate leaders and board members is effective—and it may have been. But corporate directors and executives now want and need cyber risk to be presented in financial terms—in line with other enterprise risks and business interests. This is also being driven by the transformational focus of the SEC on materiality as the proposed new trigger for disclosure.

"With that, the stakes and approach will necessarily need to change. Cyber risk decisioning isn't a backward-looking effort, it is a future-looking activity—with many variables. But we can make these determinations, just like we do in other domains based upon our growing knowledge, experience, and deep understanding of the risk environment and what is at stake. The good news is the journey works. The new financial context will be used to align cyber investments to business priorities and will bridge the gap to better cyber understanding and cyber risk governance ultimately benefitting investors and all stakeholders."

Richards has worked in recent years with many boards, CISOs, and the insurance industry, and these approaches are helping directors understand and project the expected economic exposures facing their organizations. Similar in concept to the determinations that companies make for expected liabilities and losses in other areas such as doubtful accounts, warranty liabilities, or loan loss reserves the formal development of cyber risk economics as an area of practice provides a solid basis for determining the impact of cybersecurity on the key financial conditions of the organization. This determination will be an important part, but not the only part, of any materiality determination under new SEC disclosure rules.

Materiality, as viewed by the SEC, is an "eye of the beholder" test that puts the burden on issuers to determine whether cybersecurity incidents would be material to a reasonable investor[9]. Disclosure is a powerful regulatory tool and useful indicator of how the board and management views, understands, and oversees the risk environment. Useful and meaningful risk disclosures also serve to reduce litigation risk.

However, guidance from the SEC on materiality does little to make its definition easy, noted White & Case Partners **F. Paul Pittman** and **Lawson Caisley** in a masterclass devoted to a deeper understanding of digital and cyber risk disclosure practices. Per SEC guidance on this issue, information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available." The "reasonable shareholder" standard was set by the U.S. Supreme Court and has been reaffirmed in subsequent case law.

"The new SEC rules will make a reality of regulators' repeated warnings over the years that cybersecurity is a boardroom issue, not just an IT issue," Caisley said. The SEC rules leave plenty of room for different interpretations and views as to what disclosures may be required and when. Although it is hoped that the SEC will provide some ongoing guidance and comment that will assist companies' understanding of what the SEC expects in practice and what it considers will amount to adequate disclosure, subjective judgment calls will inevitably have to be made around the boardroom table.

"Boards should be aware that their disclosure decisions may subsequently be scrutinized and challenged, either by the SEC or by third parties in litigation," Caisley said. "Hindsight can often be unfairly applied by those seeking to challenge a board's assessment, and so there can be real value in ensuring that the reasons for a board's decisions are clearly recorded. Protection will come from being able to demonstrate that the directors considered the relevant factors and information available at the time and came to a decision in good faith."

The Final SEC Cybersecurity Disclosure Rules

The most significant new disclosure rule is the requirement for cybersecurity incidents to be disclosed when the issuer now determines them to be material, as opposed to when they are discovered. This will drive a significant level of transformation in how management and boards understand the nature of the digital business system and the risks relative to the company's dependency upon it. It is also a disclosure requirement that will involve a significant amount of effort to implement.

The SEC expects incident disclosure to reflect the impacts of a material cybersecurity incident, or reasonable likely material impacts, to be disclosed within four days from when the registrant determines it to be material. This does not impose a new sense of urgency on management teams, quite the opposite as the materiality determination is controlled by the registrant. The materiality standard under existing U.S. case law centers around whether a reasonable shareholder would consider the information important in making an investment decision.

The SEC expects disclosure to describe the material aspects of the incident including its nature, scope, and timing along with (not exclusively) the impact from a financial, operational, brand, customer, vendor, competitiveness, and strategic, legal, regulatory perspectives.

The SEC wants registrants to make this disclosure "as soon as reasonably practicable." Certain delays are available where national security or public safety are involved.

For the first time, incident disclosure is also required where incidents occur in third-party systems, introducing an entirely new systemic risk dimension and communications issues throughout the highly interconnected world of the modern digital business system. This will present some unique implementation challenges.

4. CISO Boardroom Reporting

In the words of Ken Finnerty, president, IT Application Development at UPS: "The foundation of any successful relationship is a mutual understanding." A lot of discrepancy exists in what CISOs have been and should have been reporting to their boards. This critical risk communication interaction now takes on new meaning and importance with the SEC's final disclosure rules and the new cybersecurity incident materiality trigger.

To date, CISO board reporting is commonly focused on threats and controls. **CISOs and their boardroom communications are now at the forefront of establishing a mutual understanding of how the digital business system creates business value, both quantitatively and qualitatively, and what the far-reaching cyber risks to it are**. Disclosure committees, CEOs, and CFOs will look for CISOs to establish this process and make recommendations. The SEC expectation is that this is a deliberative process, not a random exercise.

Leading up to DOMINO 23, a working group of corporate directors and executives from Pfizer, Amazon, RGA, DDN, and X-Analytics took on the challenge of redefining the board reporting model around cybersecurity. The goal was to create a new standard that fulfills the board's obligations and need for information that reflects the implementation and monitoring of a reasonable system of oversight.

> **The most significant weakness in board reporting was identified as the challenges in conveying the linkages between the information system and how it creates and drives value for the organization.**

The need to clearly demonstrate, articulate, and link universal business value concepts to the digital business system and the threats to it, was the overriding objective of the working group.

Recommendations were made for a master board deck that reflects the following six elements:

- **Business and Digital Value at Risk**: Identifies total quantifiable business value as a starting point, starting with revenue, and the amount of that value derived directly and indirectly from the digital business system. Trendlines are useful to reflect the changing digital dependency of the organization. Direct digital revenue source include e-commerce revenue, digital products and services and platforms. Revenue that would be impaired if the digital system were shut down in the next level and then sources of value such as employee productivity, customer service, convenience, choice, etc. comprise the indirect value drivers of digital systems.
- **How the Complex Digital System Creates Value:** Drives a systems view and understanding of the systemic nature of the information system. Includes key descriptions in each key part of the complex system using the DiRECTOR framework and metrics that reflect how the digital business system creates business value alongside key observations on systemic risk issues.
- **The Threat Environment and Trends:** Conveys views and trends on the current threat landscape and trendlines by markets and within the sector.
- **Controls Status and Performance:** Identifies key controls in place, the value they are protecting, their maturity, their tested effectiveness, and controls planned and needed.
- **Residual Cyber Risk:** Reflects the amount of digital value at risk that is uncontrolled alongside risk transfer levels and costs. Also reflects self-insurance value/cost ratios as compared to risk transfer value/cost ratios as a critical metric.
- **Management Actions and Plans:** Explains management recommendations, actions, and progress against plans and management's system of cybersecurity risk management.

This story empowers directors with a meaningful understanding of the connections between business and digital value and the risks related to the complex digital system.

HEARD AT DOMINO 23

Understanding and determining how much value is at risk because of the complex digital business system is the critical piece that's been missing in cybersecurity governance and is a required part of any materiality determination.

Business Value and Materiality. CISOs have responsibilities to protect key economic measures captured and reflected on the organization's balance sheet, financial statements, and in their market valuation. CIOs have responsibilities focused on creating value, including revenue growth, with the tools and digital technologies at their disposal. Materiality as the determinative trigger for cybersecurity incident disclosure will reflect not only the quantitative and financial implications of cyber risk, but also qualitative implications.

A ransomware attack or accidental outage can impair tangible and intangible assets reflected on a balance sheet. Incident remediation costs and litigation can deplete balance sheet assets and create expenses that will appear on the organization's financial statements. Ransomware can stop or impair operations which can negatively impact revenue and create unanticipated expenses. These impacts can also impair investor trust and the market value of the organization.

After a major data breach, stock price performance has been shown to underperform the broader market by 11.9%[10] even after two years. These direct financial impacts can certainly be material to a *reasonable investor* and the indirect impacts of a cybersecurity incident can also impair a wide range of business value drivers that a reasonable investor would view as material.

For example, as a digital native almost all of Amazon's business value is derived from complex digital systems. Amazon's CISO focuses on threats and controls that could directly impair US $513BN in revenue, $12BN in profitability, balance sheet assets of $420BN, and a market value of $1.32TN as of June 24, 2023[11].

However, cyber risk does not threaten all balance sheet assets equally even for Amazon. Cash and other liquid assets and intellectual property may be higher cyber risk asset categories than plant, property, and equipment (PP&E). However, PP&E can be impaired because of cyber risk, which would then create other implications across Amazon's financial statements.

A massive and sustained outage of the digital products and services that hundreds of thousands of Amazon's customers rely upon to run their own business functions could significantly impair Amazon's revenue and profitability and uniquely impair market confidence and Amazon's stock price. Remediation costs, and the direct financial impacts of such a breach including regulatory fines, litigation, and third-party liability could reduce Amazon's balance sheet assets and negatively impact its profitability. Notably, under new SEC disclosure rules companies that rely upon Amazon's digital services could also be required to provide an cybersecurity incident disclosure if deemed material. And yes, the SEC has considered that the same material incidents could be disclosed multiple times, potentially thousands of times, under these rules.

Materiality as a trigger for incident disclosure will require management teams and boards to gain a new understanding of the nature of a specific incident and how it can uniquely impact each of these core financial measures, and beyond, both quantitatively and qualitatively.

Many companies are not digital natives like Amazon, but are still heavily reliant upon their digital systems. Toyota's recent accidental occurrence, a cybersecurity incident under new SEC rules, shut down all of its manufacturing plants in Japan. These companies still rely upon digital systems for many parts of their overall value proposition including e-commerce, customer service, manufacturing and assembly, employee productivity, supply chain management, product performance, product quality, etc.

While investor materiality is the SEC's end game in cybersecurity risk, this determination needs to go through business value first. Any reasonable system

of oversight requires corporate directors to oversee the business value implications of the digital business systems that power a growing proportion of their economic output and growth. Investors are well served by this part of the SEC's final disclosure rules.

The Final SEC Cybersecurity Disclosure Rules

The SEC narrative in its final disclosure rules stated that "...a materiality determination necessitates an informed and deliberative process." Given the objective nature of the concept of materiality, and the discretion that management brings in making this determination, the SEC's expectation is that registrants will bring some critical and structured thinking to this issue. This is the transformative requirement within its new rules. By imposing its materiality definition upon cybersecurity, the SEC is forcing registrants to develop and mature their understanding of cybersecurity risk and how their digital business system creates and sustains business value.

5. The Boardroom Journey Forward

Self-regulation is the leading practice in digital and cybersecurity governance and management. Regulators lag the reality of market risks, as the SEC has proven over the last decade.

Corporate boards can immediately transform and improve their approach to digital and cybersecurity governance with self-regulatory reform. They do not need to—nor should they—wait for regulators to do it for them or to them. The best boardrooms and management teams are already self-regulating their processes, practices, and procedures well beyond the SEC's disclosure rules.

DOMINO 23 brought together the leaders who are defining the leading edge of these issues. *The DOMINO Guide* establishes a blueprint that any boardroom can follow and apply. The pieces of the puzzle are brought together to present the solution in three parts:

1. Standards
2. The board's system of digital and cybersecurity governance
3. The digital and cybersecurity oversight system of the board

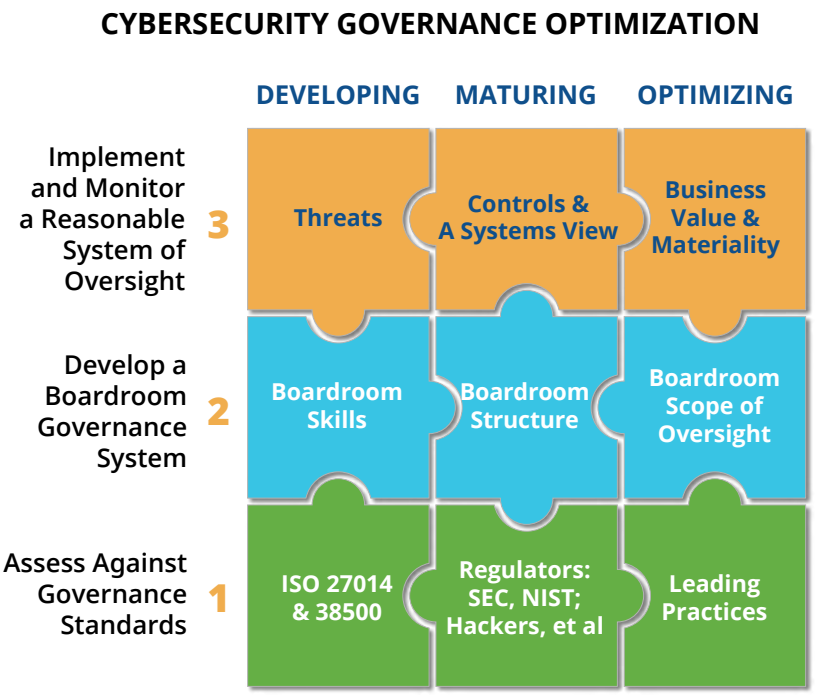


Figure 5 Cyber's Puzzle™

New innovations create new risks. Cybersecurity risk will continue to evolve because the digital systems that power a growing percentage of global economic output and growth will continue to transform the world.

Every boardroom has a vital role to play in shaping and securing their company's path into the digital future. Corporate directors and governance are important parts of solving these problems. The IT and cybersecurity leaders at DDN and DOMINO 23 are doing their part to step up to this leadership moment.

At DDN we invite you to join us on this journey — your shareholders and many stakeholders will thank you. We are glad to share our collective efforts with you along with the learnings from DOMINO 23 in *The Definitive Guide on Cybersecurity Governance: The DOMINO Guide*.

Footnotes

[1] *ISO/IEC 27014:2020 (E) Information security, cybersecurity and privacy protection — Governance of information security*. 2nd Edition (2020).

[2] Weill, Peter, Stephanie L. Woerner, Tom Apel, and Jennifer S. Banner. Companies with a *Digitally Savvy Board Perform Better. MIT CISR Research Briefing XIX*, no. 1 (2019).

[3] Ibid.

[4] Chen, Kevin D., and Andy Wu. *The Structure of Board Committees*. Harvard Business School Working Paper 17-032, (2016).

[5] *DDN Calls for a Technology & Cybersecurity Committee on US Public Company Boards*. Business Wire. DDN LLC, September 5, 2018. https://www.businesswire.com/news/home/20180905005332/en/DDN-Calls-for-a-Technology-Cybersecurity-Committee-on-US-Public-Company-Boards.

[6] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. Washington, D.C.: U.S. Securities and Exchange Commission. 2023.

[7] Construction Industry Laborers Pension Fund, Central Laborers' Pension Fund, Lawrence Miles, and Brian Seavitt, derivatively on behalf of Solarwinds Corp., Plaintiffs, vs. Mike Bingle, William Bock, Seth Boro, Paul J. Cormier, Kenneth Y. Hao, Michael Hoffman, Dennis Howard, Catherine R. Kinney, James Lines, Easwaran Sundaram, Kevin B. Thompson, Jason White, Michael Widmann (Court of Chancery of the State of Delaware, November 4, 2021).

[8] Oliveri, Stefano. *These 4 Skills Can Make the World Better after Covid-19*. World Economic Forum, August 5, 2020. https://www.weforum.org/agenda/2020/08/the-four-skills-to-make-the-world-better-after-covid-19/.

[9] Zukis, Bob, Christopher Veltsos, and Paul Ferrillo. *Boards Should Care More About Recent Caremark Claims and Cybersecurity*. The Harvard Law School Forum on Corporate Governance, September 15, 2020. https://corpgov.law.harvard.edu/2020/09/15/boards-should-care-more-about-recent-caremark-claims-and-cybersecurity/

[10] Huang, Keman, Xiaoqing Wang, William Wei, and Stuart Manic. *The Devastating Business Impacts of a Cyber Breach. Harvard Business Review*, May 4, 2023. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyberbreach.

[11] Amazon 2023 Annual Report https://ir.aboutamazon.com/annual-reports-proxies-and-shareholder-letters/default.aspx

The Leaders Advancing Digital and Cybersecurity Governance

DOMINO 23 was produced and taught by some of the world's leading companies at the forefront of advancing the practice and profession of digital and cybersecurity governance. Our Content Partners joined DDN to deliver an an unparalleled executive education experience for DOMINO attendees.

Proofpoint is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber-attacks.
www.proofpoint.com

X-Analytics is a patented and validated cyber risk-decisioning platform developed by Secure Systems Innovation Corp. SSIC is a cyber risk analytics firm whose mission is to improve how businesses manage cyber risk through the power of data analytics.
www.x-analytics.com

White & Case is a global law firm with longstanding offices in the markets that matter today. Based in New York City and founded in 1901, the firm has 46 offices in 31 countries worldwide and has been ranked among the top ten firms worldwide by revenue.
www.whitecase.com

Kudelski Security is a world leader in cybersecurity solutions and services. We help organizations navigate an increasingly complex cyber environment to reduce business risk and become resilient against threats. We enable clients to identify and adopt the right security strategies, accelerate secure digital transformation, and innovate securely in everything they do.
www.kudelskisecurity.com

Telos Corporation offers solutions that empower and protect the world's most security-conscious enterprises. We protect our customers' information assets on-premises and in the cloud so they can safely conduct their global missions. We empower them with secure solutions that leverage mobile communication, organizational messaging, and identity management.
www.telos.com

ISC2 is the world's leading cybersecurity professional organization. An international nonprofit membership association for information security leaders, ISC2 is committed to helping its members learn, grow, and thrive. Nearly 330,000 members, associates, and candidates strong, ISC2 empowers professionals who touch every aspect of information security.
www.isc2.org

TDI Security For over 20 years, TDI's one and only passion has been delivering cybersecurity solutions to effectively manage the business of cyber. At the global vanguard of innovation, it created Cybersecurity Performance Management (CPM) and the industry-leading CPM platform, CnSight®. Combining CnSight® with its remarkable historical experience and exceptional capabilities of cyber operations and compliance, TDI offers Managed Cybersecurity Performance, a first-of-its-kind managed CPM offering.
www.tdisecurity.com

IDC is the most trusted IT research advisory firm in the market. IDC's IT Executive Programs support businesses globally in the Digital Transformation (DX) of their organizations. Our IT advisory services not only advise on the technologies underpinning digital transformation (e.g., cloud, analytics, IoT, mobility, 3D printing), but also on effectively leading and executing Digital Transformation (DX) initiatives across both IT and the line of business.
www.idc.com

Corporate Board Member through Chief Executive Group's peer networks, live events, proprietary research, and flagship publications—including *Chief Executive and Corporate Board Member*—connecting CEOs, senior leaders, and public company directors of nearly every sizable company in the United States, to share their experiences, insights, and hard-won wisdom to mutually benefit each other.
www.boardmember.com

Equilar DDN partners with Equilar and the Equilar Diversity Network which is the "registry of registries" connecting candidates from more than 50 diversity organizations with boardroom opportunities. The Network is accessible exclusively through Equilar BoardEdge, a data platform including more than 1.5 million executive and board member profiles.
www.equilar.com

Women Business Collaborative works to accelerate the advancement of all women business leaders and to spotlight the need for gender, diversity, and pay parity in the workplace.
www.wbcollaborative.org

Optimizing Cybersecurity Governance

Throughout *The DOMINO Guide* are 16 well-defined "action items" to optimize cybersecurity governance. These action items are the result of learnings at DOMINO 23, which for the first time brought together corporate directors and technologists charged with oversight of the evolving complex digital systems that power the world of business today.

These items are intended to provide any boardroom or corporate director with actionable insights, both defining the cybersecurity governance problem and, most importantly, offering real solutions on the path toward implementation. Context for each of these action items is detailed throughout *The DOMINO Guide*.

Boardroom Action Item #1

Segment the boardroom challenges in digital and cybersecurity governance into three solutions areas: standards, the governance system, and the oversight system.

Boardroom Action Item #2

Prioritize self-regulation as the most effective way to optimize digital and cybersecurity governance policies and procedures. Do this by viewing the boardroom as a critical control point in digital and cybersecurity risk. Strengthening the boardroom strengthens the entire system. Regulators lag market realities; optimization requires leaders to define and implement new approaches.

Boardroom Action Item #3

Benchmark your existing boardroom policies and practices against ISO 27014 and ISO 38500 to assess the board's current state of digital and cybersecurity governance against a reliable and foundational baseline.

Boardroom Action Item #4

Evaluate the board's digital and cybersecurity practices against leading practices to identify gaps, establish the desired level of maturity in cybersecurity governance, and determine the actions needed to close the identified gaps.

Boardroom Action Item #5

Monitor regulatory developments and leading digital and cybersecurity governance practices from boardrooms around the world to continuously improve and optimize cybersecurity governance policies and practices.

Boardroom Action Item #6

Recognize that the digital and cybersecurity governance problem is a systems challenge requiring development, maturity, and coordination between three key parts of the governance and the board's scope of risk oversight.

Boardroom Action Item #7

Recruit directors with deep applied digital and cybersecurity expertise and add this disclosure as it is useful information for investors. Leading practice is a critical mass of three digitally savvy directors. MIT research has identified that companies whose boards have a critical mass of three digitally savvy directors achieve significant business benefits in revenue growth, profitability, and market valuation[3]—supporting the conclusion that boardroom leadership in digital and cybersecurity governance matters.

Boardroom Action Item #8

Deliver annual training for all directors on each of the three aspects of risk management that relate

to the complex digital business system. All directors should receive annual training on issues in digital innovation, cybersecurity, and systemic cyber risk.

Boardroom Action Item #9

Expand the digital competency model for corporate directors to include all the domains of a complex digital business system. Assess corporate director experience across each of the domains of the DiRECTOR™ framework. Identify immediately if one director could be named as a cyber expert, and close this director gap if it exists as a priority leading practice.

Boardroom Action Item #10

Define the scope of the board's digital oversight responsibilities more broadly to include opportunity risk. Update disclosures to reflect all three aspects of risk.

Boardroom Action Item #11

Implement a Technology and Cybersecurity Committee as a leading practice in boardroom structure and organization, moving cybersecurity oversight out from the audit committee. Use the DDN leading practices charter as your guide (available online for DDN members) for defining the scope of risk oversight for this committee.

Boardroom Action Item #12

Train directors and executives on concepts of complex system science to develop an understanding of systemic risk and the nature of distributed risk inherent within the complex digital business system.

Boardroom Action Item #13

Ensure management adopts disclosure controls and procedures to reflect systemic risk including third-party risk. Consider boardroom and executive training and adoption of the DiRECTOR™ framework for governing and managing systemic risk.

Boardroom Action Item #14

Ensure that management has a deliberative process for understanding the impacts of a cybersecurity incident in the context of investor materiality and regularly this. Conduct a tabletop exercise with a cross-functional group of executives on incident to materiality analysis.

Boardroom Action Item #15

Deliver director and executive education on concepts in complex systems science and systems thinking. Full boards and individual directors can join DDN where these concepts are being taught and developed.

Boardroom Action Item #16

Adopt cyber risk quantification determination as a core practice. Nothing focuses a boardroom or management team more than when they understand the economics of their cybersecurity self-insurance levels. Quantifying the amount of business value dependent upon the digital business system along with the controlled and uncontrolled levels of cyber risk is the starting point of any materiality analysis. This will become a key part of cybersecurity incident materiality determinations which will also need to consider qualitative implications.

Additional Reading From DDN

Learn more from these recent publications that detail the SEC's final cybersecurity rules, how leaders harness systemic risk in their vast hyperconnected digital business systems, and the status of governance codes and standards that are emerging around the globe.

The Final SEC Cybersecurity Rules: What's In and What's Out: Impact/Effort Analysis and Comments for Directors and CISOs, by Bob Zukis, founder and CEO, Director Directors Network, August 2023. **Click here.**

The Great Reboot: Succeeding in a Complex Digital World Under Attack from Systemic Risk, by Bob Zukis, Paul Ferrillo, and Chris Veltos, 2nd edition, 2022. Available on Amazon. **Click here.**

Digital and Cybersecurity Governance Around the World, by Bob Zukis, *Annals of Corporate Governance, 7:1*, August 30, 2022. Available on Amazon. **Click here.**

DIGITAL DIRECTORS NETWORK

DIGITAL DIRECTORS NETWORK

www.digitaldirectors.network

Chicago and Los Angeles

info@digitaldirectors.network