Nasdaq

Best Practices in Cyber Risk Governance

Building a Foundation Based on People, Processes and Technology

Digital technologies have created enormous opportunities for modern enterprises, helping them design innovative products, services and business models. However, somewhere at the intersection of innovation, transformation and disruption lies **cyber risk.** It's a topic no company or its board can afford to ignore.

Attacks have become more sophisticated and exposure points have grown, in part due to the growing array of connected devices, systems and networks. Consider:

- Research indicates that global cybercrime now tops almost $600 billion[1] and one breach costs a typical company about $3.86 million.[2]
- Consulting firm Accenture, meanwhile, found that while spending for cybersecurity is at an all-time high at $89.1 billion in 2017 — an 8% increase over the previous year — many organizations continue to struggle with technology and processes.[3]

Amid daily breaches, breakdowns and security failures, a company's leadership team can no longer stand on the sidelines. It must actively oversee and manage risk. Boards and executive leadership must understand and address strategic concepts, how technology works and what constitutes best practices in managing cyber risk. A **best practice approach** is possible, and it is built upon a **foundation of people, processes and technology.**

DID YOU KNOW?

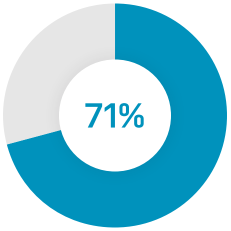
85% of companies share access to data with business partners; however, only **28%** of companies have security standards for sharing this data, according to an AT&T Business report.[4]

[1] Center for Strategic and International Studies and McAfee, "The Economic Impact of Cybercrime—No Slowing Down," February 2018. [2] Ponemon Institute, "2018 Cost of Data Breach Study," July 11, 2018. [3] Accenture, "Gaining ground on the cyber attacker," April 10, 2018. [4] AT&T, "Cybersecurity for today's digital world," 2018.

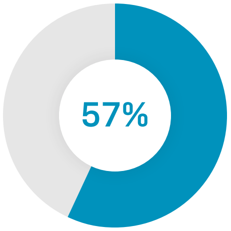
Cyber Risk Has Reached a Tipping Point

Once upon a time, organizations were protected by technology alone. It was possible to use firewalls, intrusion detection, password authentication and malware protection to secure systems and block attacks.

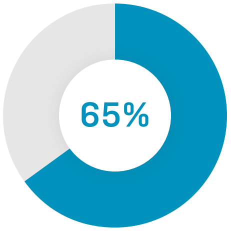
However, as cybercriminals have adopted increasingly sophisticated attack methods, the variety of possible attack surfaces has expanded. Hardly a day goes by without news of a new and more ingenious technique to break into devices, systems and networks.



Accenture reports that **71%** of respondents to its *2018 State of Cyber Resilience* indicated that cyberattacks are a bit of a "black box," and that they "don't know how they're going to affect their organization."[5]



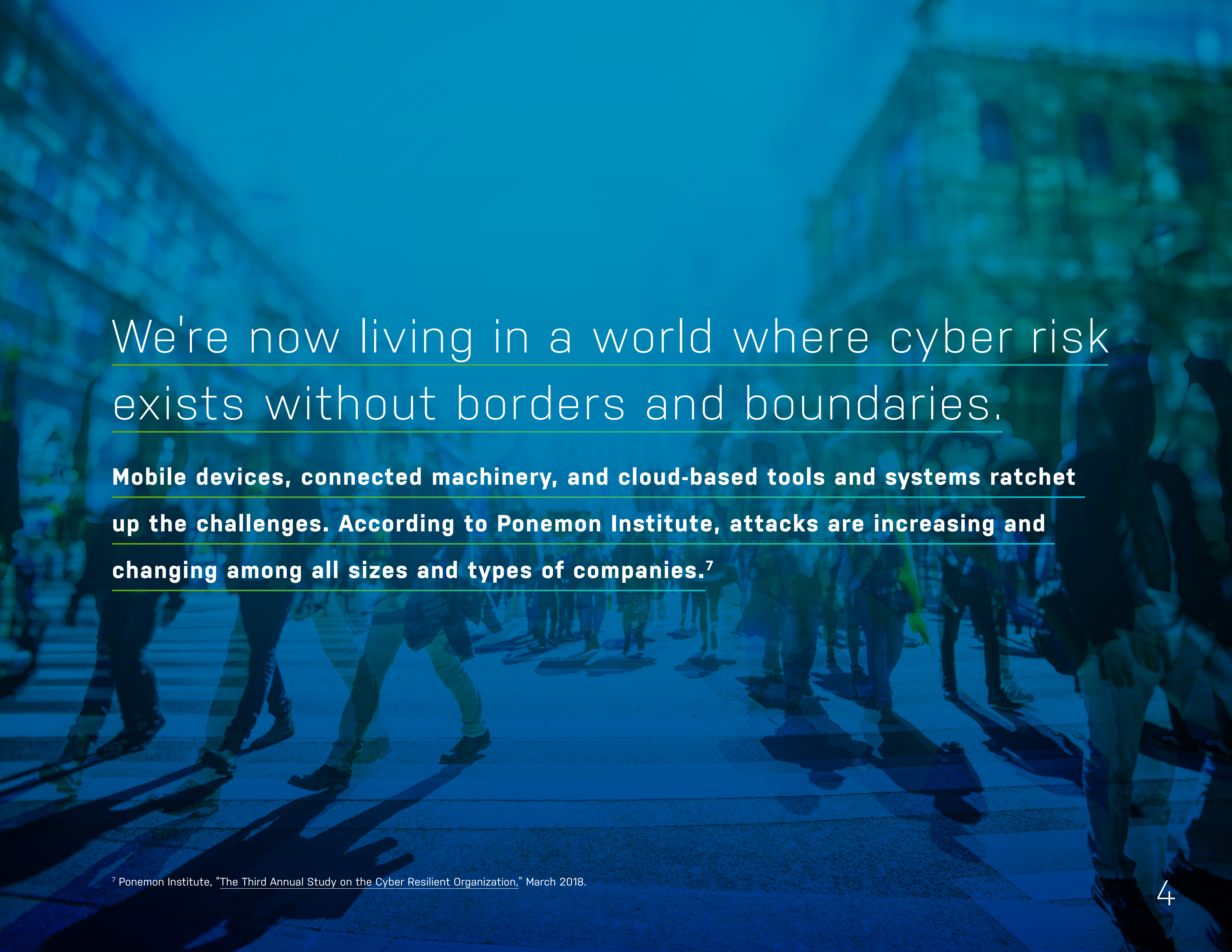
Ponemon Institute reported in *The Third Annual Study on the Cyber Resilient Organization* that "organizations globally continue to struggle with responding to cybersecurity incidents."



Overall, **57%** of respondents said the time to resolve an incident has increased and **65%** reported the severity of attacks has increased.[6] These risks extend to senior-level executives and boards.

[5] Accenture, "Gaining ground on the cyber attacker," April 10, 2018.

[6] Ponemon Institute, "The Third Annual Study on the Cyber Resilient Organization," March 2018.



We're now living in a world where cyber risk exists without borders and boundaries.

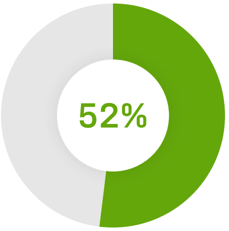
Mobile devices, connected machinery, and cloud-based tools and systems ratchet up the challenges. According to Ponemon Institute, attacks are increasing and changing among all sizes and types of companies.[7]

[7] Ponemon Institute, "The Third Annual Study on the Cyber Resilient Organization," March 2018.

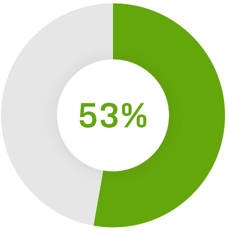
Cyberattacks Are Silent but Ever-Present in the Boardroom

It's easy to believe that the executive suite and boardroom are at least somewhat insulated from the cybersecurity risks hovering over the rest of the organization. After all, executive discussions often take place independent of conventional enterprise tools, applications and systems.

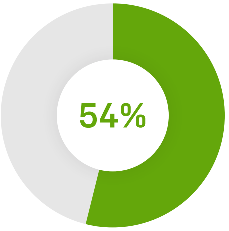
Yet many of the applications and technologies executives and board members use weren't designed with today's cybersecurity risks in mind. This includes: email, text messaging and file-sharing services, along with various applications that store notes and other information in apps or databases. Risks are also magnified when people do not abide by appropriate security precautions.



According to Ponemon Institute,[8] **52%** of executives said their companies experienced a ransomware attack.



In addition, **53%** of these respondents say they had more than two ransomware incidents in the past 12 months.



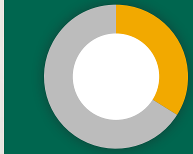
Finally, **54%** said negligent employees, including senior-level executives, were the root cause of a data breach.

Unfortunately, the same risks that apply to the enterprise as a whole apply to leadership teams and the board of directors. Making matters worse, there's the added risk that the information that business leaders exchange is among the most strategic and sensitive.

[8] Ponemon Institute, “2017 State of Cybersecurity in Small and Medium-Sized Businesses,” September 2017.

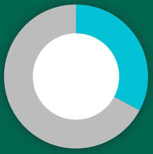
DID YOU KNOW?

When establishing IT security priorities, organizations depend on[9]



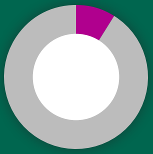
CEO

34%



CIO

33%



Board of Directors

9%

[9] Ponemon Institute, "2017 State of Cybersecurity in Small and Medium-Sized Businesses," September 2017.

5 Ways to Verify Your Governance Model Is Equipped for Today's Cyber Risks

Enterprise and board-level best practices in addressing cyber risk don't happen by accident. Andrea Bonime-Blanc, lead cyber risk governance author and researcher for The Conference Board, points out that five issues are critical to address:[10]

01

A board must tackle cybersecurity in a manner that is appropriate to its industry, footprint, geography, assets and people.

02

A board should have either a committee, cyber expert or both tackling the issue of cybersecurity oversight as part of overall IT oversight. This entity should report to the board at least twice a year.

03

An audit committee should not assume responsibility for cybersecurity oversight. It's best to address the issue through a technology and cybersecurity-based committee approach.

04

Some directors and senior executives must be savvy or knowledgeable about cybersecurity. An inability to ask key questions or understand critical issues is a recipe for problems.

05

Some board members should engage in cybersecurity preparedness education and training.

[10] Harvard Law School Forum on Corporate Governance and Financial Regulation, "A Strategic Cyber-Roadmap for the Board,"January 12, 2017.

The Power of People, Processes and Technology

Strategic insight illuminates the path to progress. It helps an enterprise identify the protections required, how a defense strategy should be designed and what governance framework must exist. Managing risk at the board level revolves around the same set of challenges. **The common denominator is that cybersecurity controls consistently revolve around three key factors: *people, processes and technology.*** Any weak link in this equation leads to vulnerabilities and increased levels of risk.

PEOPLE

The "people" part of the framework involves understanding how senior level executives and others use, manage and exchange documents and data.

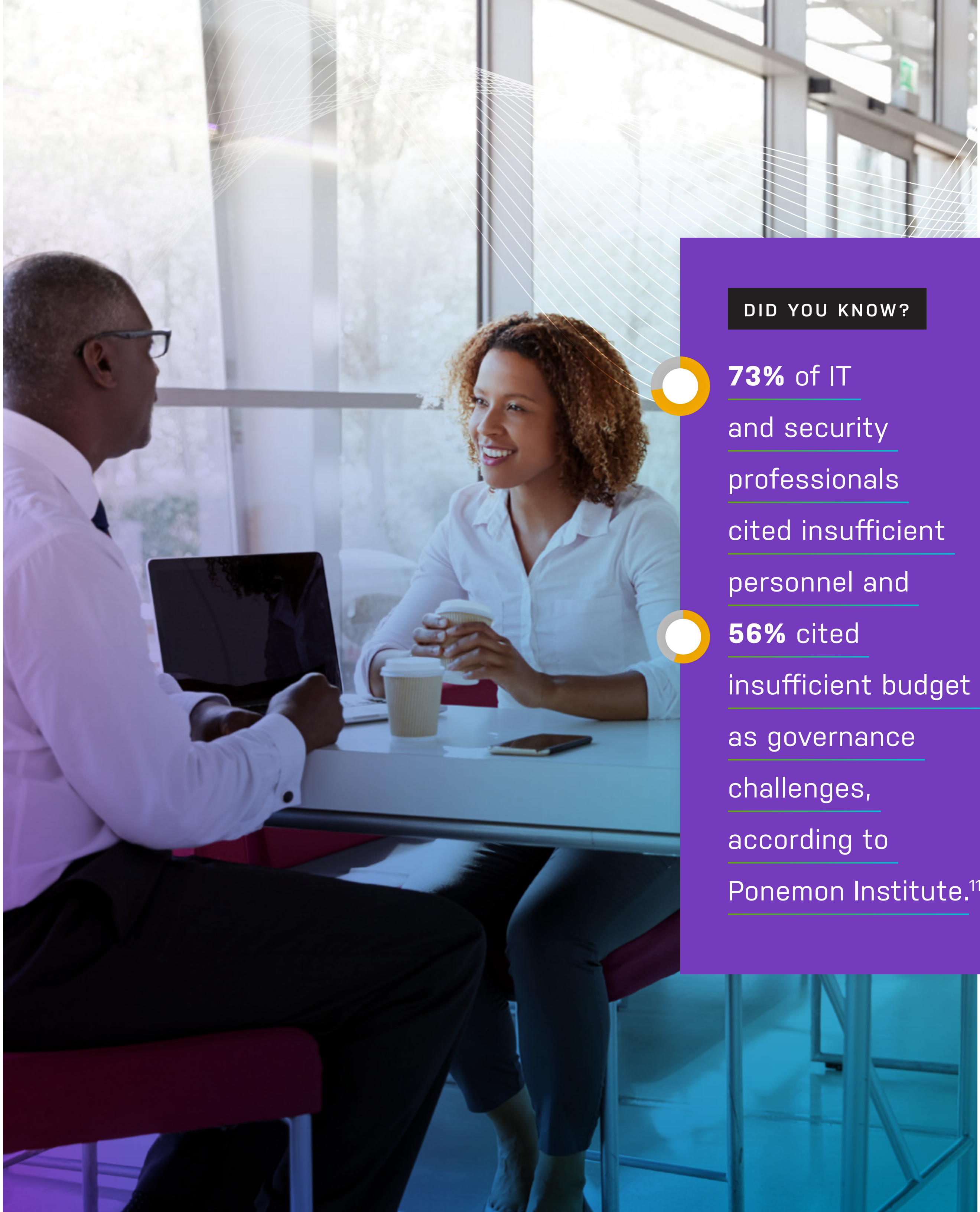
PROCESS

The "process" piece of the puzzle revolves around an understanding of how work takes place and what checks and balances exist for various tasks.

TECHNOLOGY

"Technology" is all about putting systems in place that allow people to complete work without unnecessary burdens — all while determining that the enterprise enforces rules and procedures.

With an appropriate and clearly defined structure around people, processes and technology, an enterprise can hardwire the right set of rules into systems and help ensure that leadership teams — and everyone else inside and outside an organization — are acting in safe and acceptable ways. The enterprise can establish that there's a match between its cyber risk objectives and the way people actually do things. This top-down approach is at the center of moving to a best practice framework.



DID YOU KNOW?

73% of IT and security professionals cited insufficient personnel and **56%** cited insufficient budget as governance challenges, according to Ponemon Institute.[11]

[11] Ponemon Institute, "2017 State of Cybersecurity in Small and Medium-Sized Businesses," September 2017.

4 Keys to Effective Cyber Risk Controls

01

Identify IT and system administrators that could inflict damage without collusion. Establish secondary approvals and other controls so that no single individual has unchecked power.

02

Establish approvals for financial transactions that involve large sums as well as for key changes to IT systems. Use a multi-factor authentication system or a verified approval process that goes beyond an email or phone call before initiating any significant transaction or change.

03

Place cyber oversight within the domain of an audit or risk committee. This group must provide the full board with periodic updates about changes in the threat environment, business continuity plans, necessary changes and any other cyber risk issues.

04

Schedule regular briefings with board members about risk and the current state of controls. This increased transparency and knowledge will aid in prioritizing issues while improving business performance and brand perception.

Future-Proofing Cyber Risk Governance

When an organization deploys the right tools and embeds rules into its governance model, a new era of cybersecurity emerges. It's possible to automate processes, including the enforcement of policies, and create safe and secure methods for enterprise leaders and others to communicate, collaborate and tackle sensitive tasks.

A best practice approach includes:

An enterprise meeting point, such as a dedicated board portal or special project portal.

Controls over which devices and apps are allowed and how, when and where people can use them.

A governance framework that provides the level of flexibility and autonomy that groups require to complete tasks — while plugging into robust security technology, and systems to alert employees, when necessary.

Specific enforceable rules. For instance, this might include a notification that an action — say clicking a link or initiating a wire transfer — represents risk. An application might also prompt for an additional approval before completing a sensitive task.

Tools, such as content management software and mobile device management (MDM) systems, and specialized technologies, such as analytics, artificial intelligence (AI) and next-generation firewalls, can aid in enforcing policies.

Maintain regular communication between the board and key leaders, including the CSO, CISO and CTO. This includes monthly board and senior-level meetings that address key cyber risk issues. The board has a responsibility to push governance models into the organization as a whole.

DID YOU KNOW?

Accenture[12] found that

64%

of CISOs now report directly to the CEO or board, and

29%

of CIOs have budget authorization.

[12] Accenture, "Gaining ground on the cyber attacker," April 10, 2018.

10 Board-Level Cyber Risk Best Practices

01

Ensure that one or two board members have a solid understanding of cyber risk and cybersecurity. Others should have a basic understanding of these issues.

02

Focus on building a robust communication channel between the board and key senior executives, such as the CIO, CISO and CSO.

03

Use dashboards to understand cybersecurity performance and whether an organization is aligning strategy and spending with real-world risks.

04

Boards should ask questions and explore cyber risk topics on a regular basis. Conduct briefings with key security executives and teams.

05

Use an acknowledged cyber framework, such as the one by National Institute of Standards and Technology, to establish, manage and analyze processes.

06

Seek independent assessments and use this information to identify risks and formulate a cyber plan.

07

Establish high-level metrics that pertain to cyber risk and cybersecurity.

08

A board should be informed immediately following any new cyber risk or an actual breach.

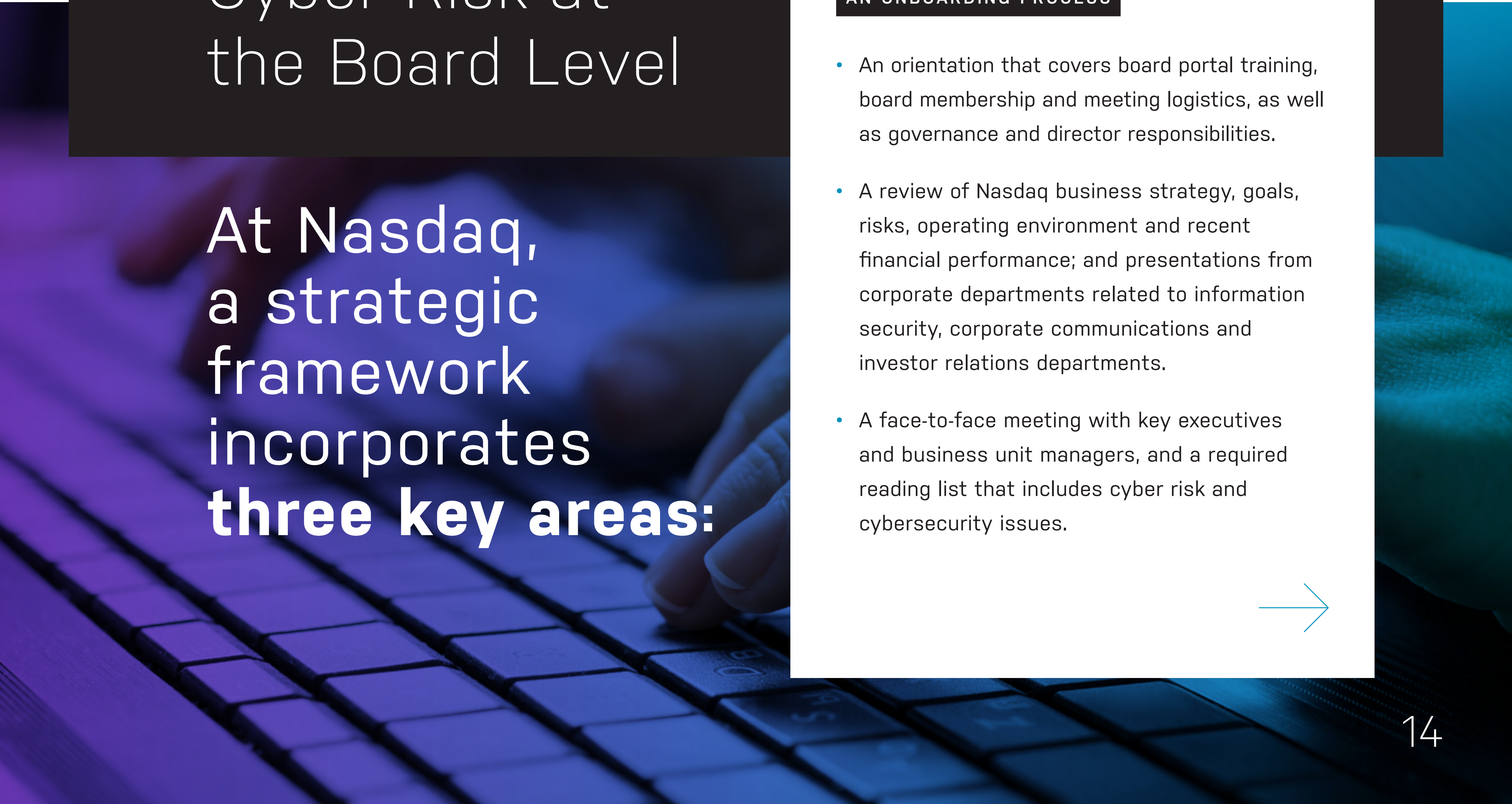
09

Establish a board committee that focuses on cyber risk oversight.

10

Organizations, and their CISOs, should regularly engage with law enforcement, industry peer groups and government.

How Nasdaq Addresses Cyber Risk at the Board Level

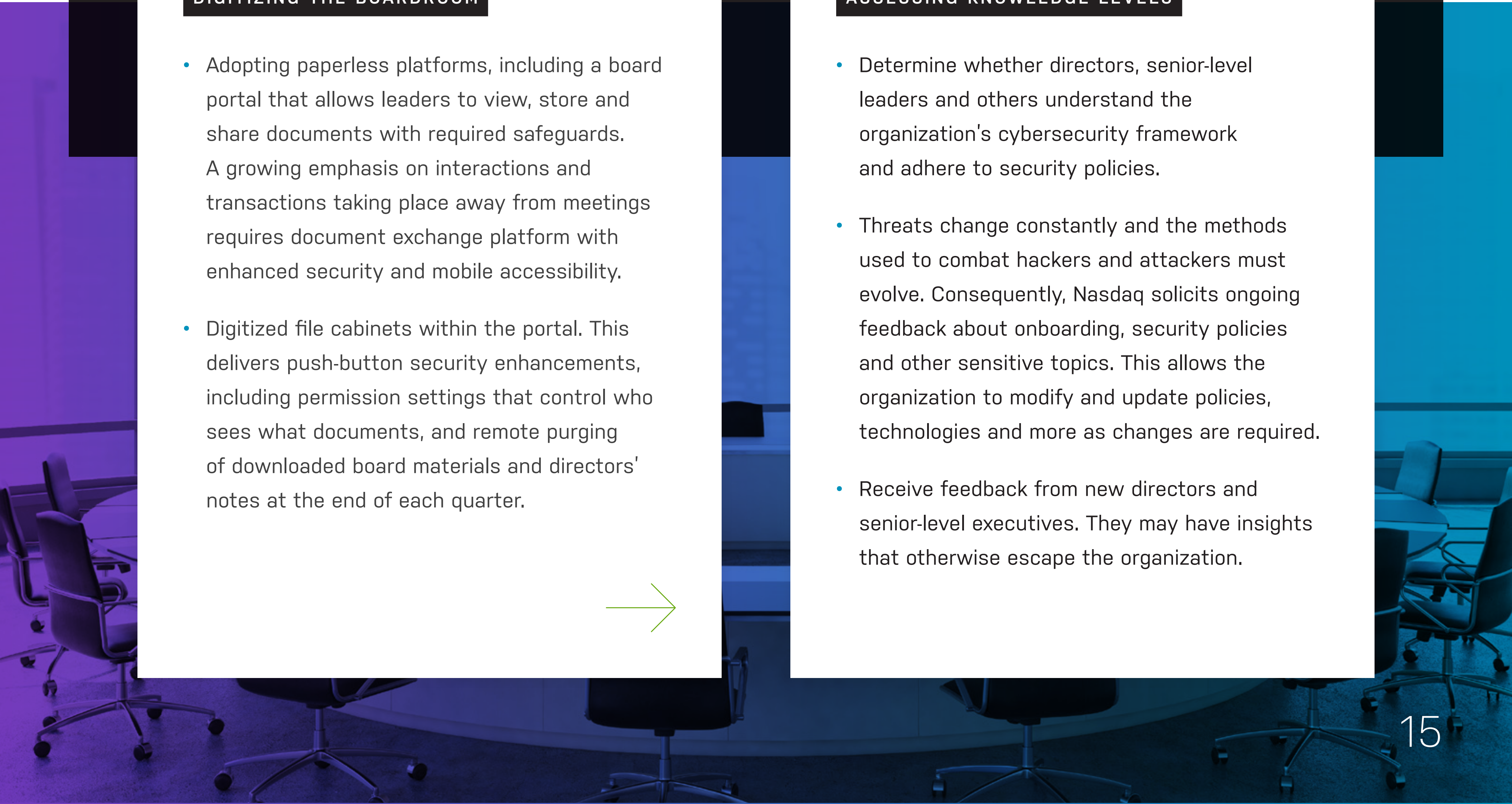


At Nasdaq, a strategic framework incorporates **three key areas:**

01

AN ONBOARDING PROCESS

- An orientation that covers board portal training, board membership and meeting logistics, as well as governance and director responsibilities.
- A review of Nasdaq business strategy, goals, risks, operating environment and recent financial performance; and presentations from corporate departments related to information security, corporate communications and investor relations departments.
- A face-to-face meeting with key executives and business unit managers, and a required reading list that includes cyber risk and cybersecurity issues.



02

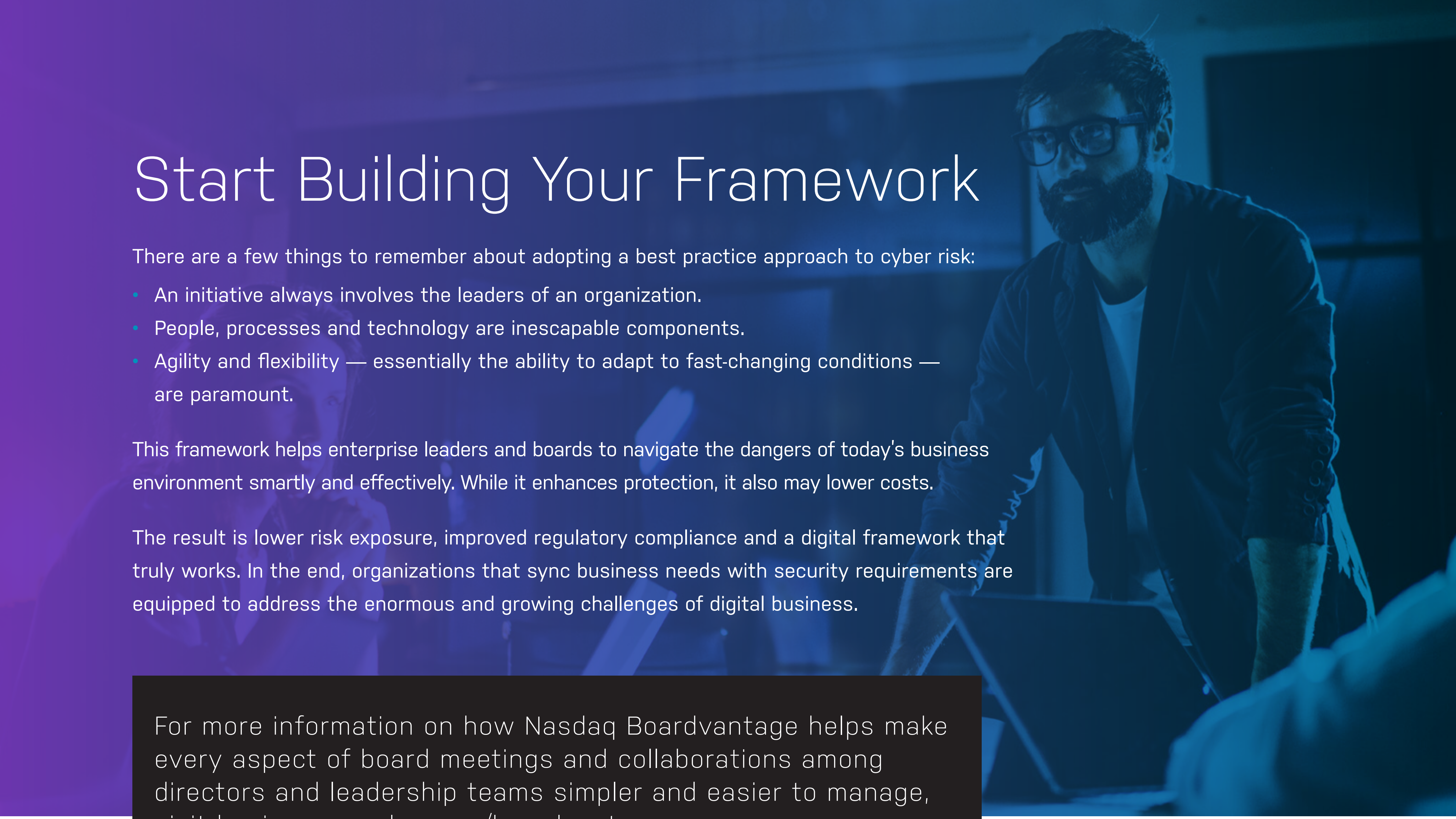
DIGITIZING THE BOARDROOM

- Adopting paperless platforms, including a board portal that allows leaders to view, store and share documents with required safeguards. A growing emphasis on interactions and transactions taking place away from meetings requires document exchange platform with enhanced security and mobile accessibility.
- Digitized file cabinets within the portal. This delivers push-button security enhancements, including permission settings that control who sees what documents, and remote purging of downloaded board materials and directors' notes at the end of each quarter.

03

ASSESSING KNOWLEDGE LEVELS

- Determine whether directors, senior-level leaders and others understand the organization's cybersecurity framework and adhere to security policies.
- Threats change constantly and the methods used to combat hackers and attackers must evolve. Consequently, Nasdaq solicits ongoing feedback about onboarding, security policies and other sensitive topics. This allows the organization to modify and update policies, technologies and more as changes are required.
- Receive feedback from new directors and senior-level executives. They may have insights that otherwise escape the organization.



Start Building Your Framework

There are a few things to remember about adopting a best practice approach to cyber risk:

- An initiative always involves the leaders of an organization.
- People, processes and technology are inescapable components.
- Agility and flexibility — essentially the ability to adapt to fast-changing conditions — are paramount.

This framework helps enterprise leaders and boards to navigate the dangers of today's business environment smartly and effectively. While it enhances protection, it also may lower costs.

The result is lower risk exposure, improved regulatory compliance and a digital framework that truly works. In the end, organizations that sync business needs with security requirements are equipped to address the enormous and growing challenges of digital business.

For more information on how Nasdaq Boardvantage helps make every aspect of board meetings and collaborations among directors and leadership teams simpler and easier to manage, visit business.nasdaq.com/boardvantage.

CONTACT US

North America & South America +1 844-375-2626, Opt. 6
Europe & Africa +44 (0) 20 3734 1514
Middle East +971 5885 76815
Asia Pacific +852 2167 2500
URL business.nasdaq.com/boardvantage