Deloitte.

Assessing cyber risk

Critical questions for the board and the C-suite

Cyber Risk

Risk powers performance.

Risk has traditionally been viewed as something to be minimized or avoided, with significant effort spent on protecting value. However, we believe that risk is also a creator of value and, approached in the right way, can play a unique role in driving business performance.

Take the issue of cyber risk. Increased use of technology and globalization are key drivers of cyber risk, but they are also key sources of competitive advantage. Organizations that pull back from these drivers to try and protect value will likely fall behind, while organizations that find better ways to manage cyber risk can power superior performance through increased use of technology and globalization.

A key step on this journey is understanding the current state of your organization's cyber capabilities. This guide and self-assessment tool is designed to help leaders gauge their cyber maturity, build new cyber risk understanding, and answer key questions, including:

- Do we have the right leader and organizational talent?
- Are we focused on, and investing in, the right things?
- How do we evaluate the effectiveness of our organization's cyber risk program?

Today's leading organizations are those that have learned how to protect their value through risk management. Tomorrow's leaders will be those that recognize the opportunity for risk to also create value. Deloitte's Risk Advisory professionals around the world can guide you on that journey and help you transform your organization into a place where risk powers performance.

To learn more, please visit us at www.deloitte.com/risk.

Sam Balaji
Global Risk Advisory Leader

Risk responsibility

Cyber risk is an imperative for everyone within the enterprise—but ultimate responsibility for overseeing risk rests with top leaders.

Many board members and C-suite executives, however, are far removed from the day-to-day challenges of monitoring, detecting, and responding to evolving cyber risks. Those leaders who develop a deeper view into where their organization stands when it comes to cyber risk can gain critical understanding for better managing the business.

Effective cyber risk management starts with awareness at the board and C-suite level. Sharpening your ability to understand risk, manage performance, and move your organization closer to cyber maturity often begins with answering important questions—and should result in becoming a more secure, vigilant, and resilient business. All three traits are critically important today—although cyberthreat management traditionally has focused on "secure" while paying less attention to "vigilant" (comprehensively monitoring the extensive threat landscape) and "resilient" (responding to and recovering from attacks). Here's an in-depth look at 10 must-answer questions that can help top leaders better comprehend where they stand when it comes to "secure, vigilant, resilient."

1. Do we demonstrate due diligence, ownership, and effective management of cyber risk?
2. Do we have the right leader and organizational talent?
3. Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?
4. Are we focused on, and investing in, the right things? And, if so, how do we evaluate and measure the results of our decisions?
5. How do our cyber risk program and capabilities align to industry standards and peer organizations?
6. Do we have a cyber-focused mindset and cyber-conscious culture organization wide?
7. What have we done to protect the organization against third-party cyber risks?
8. Can we rapidly contain damages and mobilize response resources when a cyber incident occurs?
9. How do we evaluate the effectiveness of our organization's cyber risk program?
10. Are we a strong and secure link in the highly connected ecosystems in which we operate?

Boards and C-suite play a critical role in helping their organizations respond to the constantly evolving cyberthreat landscape.

Cyberthreats and attacks continue to grow in number and complexity—all while the business world grows increasingly connected and digital. Amid this new landscape, managing cyberthreats becomes a business and strategic imperative, with the stakes higher than ever. These days, cybercrime involves more than fraud and theft. As the domain of vast criminal networks, foreign government-sponsored hackers, and cyber terrorists, cybercrime extends across the risk spectrum—to involve disruption of services, corruption or destruction of data, and even "ransomware" activities that seek to extort money, access, or corporate secrets from victims.

Today, cyber risk and performance are more tightly intertwined. Tangible costs from cybercrime range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for affected parties. Intangible costs could include loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, and overall damage to an organization's reputation and brand. Beyond the damage to individual organizations, the sheer scope of cyberattacks now has the potential to cause mass-scale infrastructure outages and potentially affect the reliability of entire national financial systems and the well-being of economies.

Top-tier issue

With so much at stake, the board and C-suite increasingly realize that cyber risk must be treated as a top-tier business risk, requiring a level of awareness deeply embedded in the culture of the enterprise. As every aspect of business today touches on some digital component, cyber risk concerns stretch well beyond IT and well beyond the walls of the enterprise—to every partner, to every customer, to every worker, and to every business process.

Realizing that at some point the organization will be breached, leaders should work to understand the most significant threats and how those threats can put mission-critical assets at risk. As boards and the C-suite take a more active role in protecting their organizations, many will struggle to ensure that their efforts are effective. What are their responsibilities? Which competencies should they be cultivating? What are the right questions to ask? Faced with such questions and an evolving threat landscape, preparing for every possibility can prove daunting. So planning for what's probable—not just possible—offers a prudent path forward for leaders.

There's no blanket solution to the challenge, but the board and C-suite leaders can begin developing a custom cybersecurity program or improve an existing one. The 10 key questions that we lay out in the following pages should promote boardroom discussions around management's ongoing cyber strategies, how leaders effectively address evolving challenges, how they mitigate cyber risks, and how they anticipate opportunities.

Assess your maturity level

This list of key cyber risk questions and accompanying range of responses should effectively guide organizations in assessing their cyber posture, challenge information security teams to ask the right questions and provide critical information, and help consistently monitor and improve cyber resilience going forward.

These questions are designed to help you identify specific strengths and weaknesses, as well as paths to improvement. Determine where your organization's responses to the following questions fall on the cyber maturity scale:

Cybersecurity maturity scale

High maturity
We have a strong cyber risk posture within the organization.

Moderate maturity
Cyber risk measures are in place; some work remains.

Low maturity
We are lagging on cyber risk management, with few measures in place and significant work to do.

What it means to be secure, vigilant, and resilient

Secure

Establish and continually maintain foundational security capabilities—by enhancing risk-prioritized controls to protect against known and emerging threats, while also complying with industry cyber standards and regulations.

Vigilant

Detect violations and anomalies through better situational awareness across the environment—within all areas of your ecosystem.

Resilient

Establish the ability to quickly return to normal operations and repair damage to the business following the inevitable cyberattack.

Do we demonstrate due diligence, ownership, and effective management of cyber risk?

1

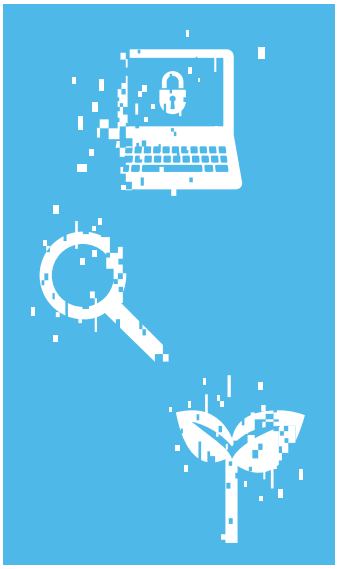
Determining the right degree of accountability at the leadership level is essential. If oversight involves only a 5-minute update on cyber events every now and then, you're probably not doing enough to manage risk effectively.

High maturity

- ☐ Board and C-suite hold a C-level executive accountable for cyberthreat risk management —and are responsible for overseeing development of a cyber risk program as well as confirming its implementation
- ☐ Board and C-suite stay informed about cyberthreats and the potential impact on their organization
- ☐ Board has one or more members—or appropriately leverages strategic advisors—who understand IT and cyber risks
- ☐ An established senior management-level committee, or a hybrid committee consisting of management and board directors, that is dedicated to the issue of cyber risk—or an alternate senior management-level committee has adequate time devoted to the overall cyber program
- ☐ Due diligence is evident in regular updates, budget analysis, and challenging questions to management

Moderate maturity

- ☐ Leadership and board oversight are concerned with cyber issues, but stakeholder communications and oversight of specific structures remain largely high-level
- ☐ Board has a working knowledge of IT and cyber risks
- ☐ Cyber due diligence and the ability to challenge management on cyber issues is lacking
- ☐ Board intermittently assesses the cyber framework and strategic requirements



Low maturity

- ☐ Tone at the top lacks cyber focus and understanding of strategic issues
- ☐ Little engagement by leadership in specific IT security issues
- ☐ Board has no significant experience in IT and cyber risks, and cyber issues are left to those within IT to resolve
- ☐ Oversight of cyber risk and assessment of related budgetary requirements remains at a very high level

Do we have the right leader and organizational talent?

2

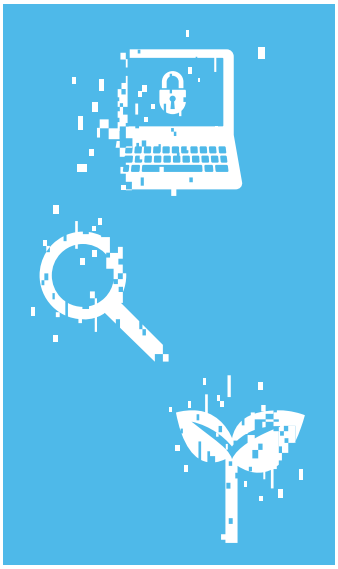
Everyone within an organization holds some responsibility for cyber risk. With everyone responsible and with many leaders busy performing their legacy duties, organizations can fail to designate an appropriate leader—the "right" leader—who will ultimately be accountable for cyber risk.

High maturity

- ☐ Cyber leader has the right mix of technical and business acumen to understand how the organization operates, to engage with the business, and to know where to prioritize efforts
- ☐ Teams of passionate and energized staff stay up-to-date on the latest cyber trends, threats, and implications for their business
- ☐ Cyber risk discussions take place at the board and C-suite level
- ☐ There is a sufficient number of skilled staff with relevant industry experience focused on the right areas
- ☐ Compensation and total reward programs are in-line with industry and risk profile/ importance to the organization

Moderate maturity

- ☐ Cyber leader is in place but is primarily focused on technical risks associated with cybersecurity
- ☐ Cyber leader has a working knowledge of the industry but does not fully understand and appreciate how the organization operates
- ☐ Cyber risk is a significant focus but remains relatively high-level
- ☐ Cyber risk issues often stall at the IT or management level
- ☐ Skilled staff is present in IT and some business areas, but with limited industry-specific threat knowledge



Low maturity

- ☐ Little focus on cyber risk from leadership
- ☐ Cyber knowledge and talent are compartmentalized in the IT function
- ☐ Ad hoc training programs are developed for specific new technologies
- ☐ High turnover of staff due to a lack of investment in talent strategy

Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?

3

Developing meaningful cyber-related messages for the broader organization can help foster the flow of information when there are cyber incidents or concerns. But clearly defining the triggers or threshold events, as well as the actual process for moving information up to management, can make the difference between functional and effective.

High maturity

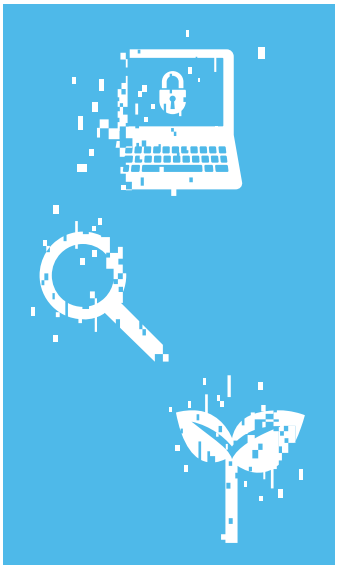
- ☐ Clearly articulated risk appetite and cyber risks are incorporated into existing risk management and governance processes
- ☐ Established enterprise-wide cyber risk policy is approved and challenged, when necessary, by the board
- ☐ Clearly described and operationalized roles and responsibilities across the cyber risk program
- ☐ Key risk and performance indicators exist, and processes are in place to escalate breaches of limits and thresholds to senior management for significant or critical cyber incidents
- ☐ Incident management framework includes escalation criteria aligned with the cyber risk program
- ☐ Evaluation and monitoring of the value of cyber insurance is in place

Moderate maturity

- ☐ Established cyber risk policy is not fully implemented outside IT
- ☐ Cyber risks are addressed only generally in overall risk management and governance processes
- ☐ Risk appetite is not integrated into cyber risk framework
- ☐ Cyber risk response tends to be reactive rather than proactive
- ☐ An alternative senior management committee has adequate time devoted to the discussion of the implementation of the cyber framework

Low maturity

- ☐ No formalized cyber framework is in place
- ☐ Any risk escalation is ad hoc and only in response to incidents



Are we focused on, and investing in, the right things? And how do we evaluate and measure the results of our decisions?

4

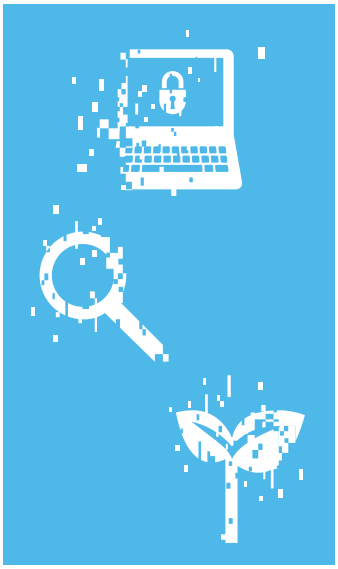
With risk and performance tightly linked, leaders should know what they're expending on resources—and they should know that they're bringing the right resources to bear on cyber challenges. Failing to develop a people strategy, overpaying for services, and other drags on operating costs are all very real risks.

High maturity

- ☐ Cyber risk is considered in all activities—from strategic planning to day-to-day operations—in every part of the organization
- ☐ Investments are focused on baseline security controls to address the majority of threats, and strategically targeted funds are used to manage risks against the organization's most critical processes and information
- ☐ Organization has made an effort to identify their "black swan" risks and has a program to anticipate and avoid these unlikely, but potentially catastrophic, threats
- ☐ Organization's investments and budgets align to risk (clear business cases for investments exist) and are reflected within the cyber strategy
- ☐ Senior management provides adequate funding and sufficient resources to support the implementation of the organization's cyber framework
- ☐ A mechanism for credible challenge exists

Moderate maturity

- ☐ Cyber framework is internally focused without added industry-based processes
- ☐ Cyber strategy and investments are neither aligned nor supportive of one another
- ☐ Imbalance of security investment across baseline security controls and those required for highly sophisticated attacks
- ☐ Strong threat awareness is focused on enterprise-wide infrastructure and application protection
- ☐ Implementation of identity-aware information protection
- ☐ Automated IT asset vulnerability monitoring is in place
- ☐ No significant mechanism for anticipating "black swan" risks



Low maturity

- ☐ Lack of cyber strategy, initiatives, and investment plan
- ☐ Only basic network protection/traditional signature-based security controls exist, with minimal concern for new technologies and methodologies
- ☐ Occasional IT asset vulnerability assessments are performed
- ☐ Business case for cyber investment is rarely made

How do our cyber risk program and capabilities align to industry standards and peer organizations?

5

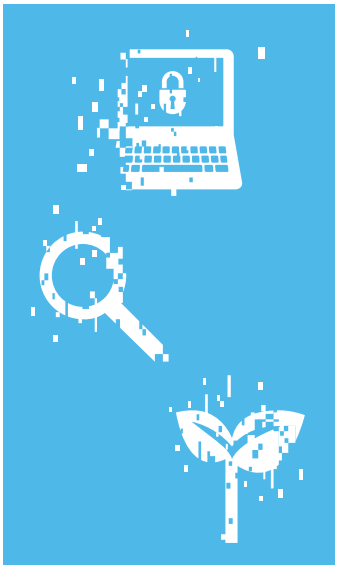
It's important to know if your organization is lagging—to know how you stand against businesses that are effectively addressing cyber risk. But what do you do if you discover you are lagging? If the board and the C-suite aren't actively in charge of the challenge, who is?

High maturity

- ☐ Comprehensive cyber program leverages industry standards and best practices to protect and detect against existing threats, remain informed of emerging threats, and enable timely response and recovery
- ☐ Adoption of an industry framework to establish, operate, maintain, and improve/adapt cyber programs
- ☐ Organization has conducted an external benchmarking review of its cyber program
- ☐ Organization periodically verifies internal compliance with policies, industry standards, and regulations
- ☐ Organization has formally certified critical and applicable areas of their business (e.g., ISO 27001:2013 certification)

Moderate maturity

- ☐ Cyber program implements a number of industry best practices and capabilities, including basic online brand monitoring, automated malware forensics, manual e-discovery, criminal/hacker surveillance, workforce/customer behavior profiling, and targeted cross-platform monitoring for internal users
- ☐ Compliance and other internal program reviews may be undertaken occasionally but not consistently



Low maturity

- ☐ Cyber measures are ad hoc, with little reference to industry standards and best practices
- ☐ May conduct intermittent high-level reviews in support of compliance and regulatory requirements

Do we have a cyber-focused mindset and cyber-conscious culture organization wide?

6

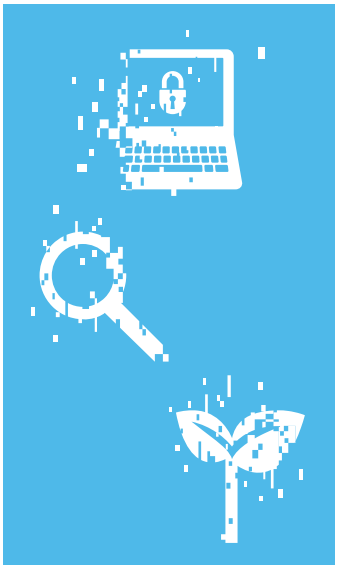
As they try to strengthen their posture to become more secure, vigilant, and resilient, many businesses focus on education and awareness. But the need runs deeper. How do you change behavior? Guidance on the answer should come from the board and the C-suite.

High maturity

- ☐ Strong tone at the top; the board and C-suite promote a strong risk culture and sustainable risk/return thinking
- ☐ People's individual interests, values, and ethics are aligned with the organization's cyber risk strategy, appetite, tolerance, and approach
- ☐ Executives are comfortable talking openly and honestly about cyber risk using a common vocabulary that promotes shared understanding
- ☐ Company-wide education and awareness campaign established around cyber risk (all employees, third parties, contractors, etc.)
- ☐ Awareness and training specific to individual job descriptions helps staff understand their cyber responsibilities
- ☐ People take personal responsibility for the management of risk and proactively seek to involve others when needed

Moderate maturity

- ☐ General information security training and awareness is in place
- ☐ Targeted, intelligence-based cyber awareness focused on asset risks and threat types is in place



Low maturity

- ☐ Acceptable usage policy is in place
- ☐ Little emphasis on cyber risk outside of IT
- ☐ Awareness and training issues are reactively addressed, in that training is given only after a breach or noncompliance is discovered, and only to a small subset of individuals

What have we done to protect the organization against third-party cyber risks?

7

The roots of many breaches have their origins with business partners, such as contractors and vendors. Cyber concerns extend far beyond the four walls of your business, requiring you to align with your partners, to understand what they are doing, and to ensure that you're comfortable with the risk factors those relationships present.

High maturity

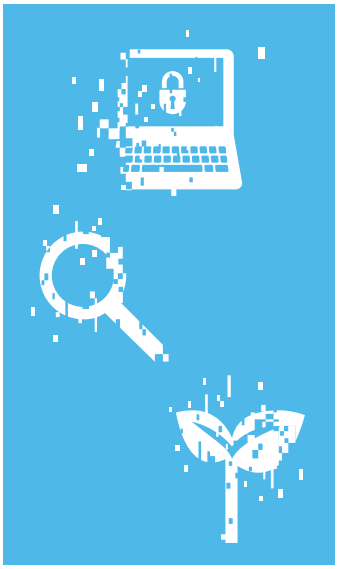
- ☐ Cyber risks are seen as part of the due diligence process for critical outsourcing and subcontracting arrangements
- ☐ All third parties are engaged through a consistent process, and policies and controls are in place (e.g., right to audit), aligned to the organization's expectations and risk tolerance
- ☐ Third parties receive specific training on cyber issues, tailored to relevant needs and risks
- ☐ Risk management program includes profiling and assessing all material third-party relationships and information flows
- ☐ Processes are in place to ensure timely notification of cyber incidents from third parties
- ☐ Steps are taken to mitigate potential cyber risks from outsourcing arrangements based on third-party profiling and risk assessments

Moderate maturity

- ☐ Steps are taken to mitigate potential cyber risks from outsourcing arrangements
- ☐ Due diligence around outsourcing and subcontracting arrangements is encouraged but inconsistently applied
- ☐ Communication from third parties respecting cyber incidents is not contractually embedded
- ☐ Some correlation of external and internal threat intelligence

Low maturity

- ☐ Only basic network protection is in place
- ☐ Third-party due diligence and cyber risk protection measures are nonexistent



Can we rapidly contain damages and mobilize diverse response resources when a cyber incident occurs?

8

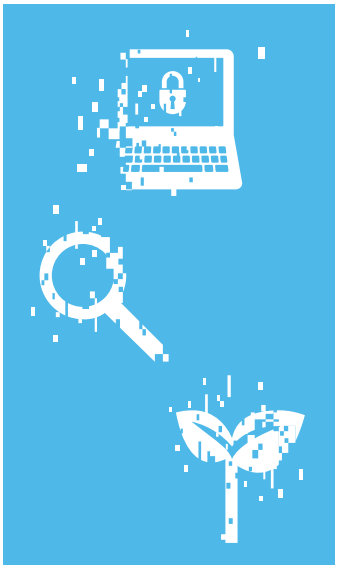
Even among highly secure businesses, it often can take days or weeks to discover a breach. What matters is confidence in your ability to respond—confidence in your processes—once you do detect the active threat. From leadership's perspective, critical incident response capabilities include a clear and current chain of command, a thorough communication plan (including back-up contacts), and a broad view of legal issues, public relations needs, brand implications, and operational impacts.

High maturity

- ☐ Clear reporting and decision paths exist for action and communication in response to a security failure or accident
- ☐ Cyber incident response policies and procedures are integrated with existing business continuity management and disaster recovery plans
- ☐ Crisis management and cyber incident response plans and procedures are documented and rehearsed through wargaming, simulations, and team interaction
- ☐ External and internal communications plans exist to address cyber incidents for key stakeholders
- ☐ Organization is actively involved in industry simulations and training exercises

Moderate maturity

- ☐ Basic cyber incident response policies and procedures are in place but not effectively integrated with existing business continuity management and disaster recovery plans
- ☐ IT cyberattack simulations are regularly undertaken
- ☐ Cyberattack exercises are implemented intermittently across the business



Low maturity

- ☐ Some IT business continuity and disaster recovery exercises occur
- ☐ Cyber incident policies, response plans, and communications are minimal or nonexistent

How do we evaluate the effectiveness of our organization's cyber risk program?

9

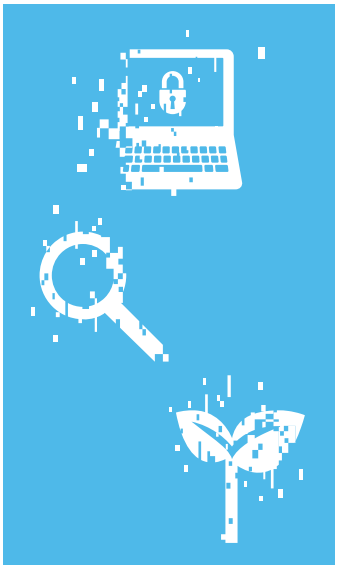
The answer to this question is simple. You evaluate from end to end. Execution is the difficult part. The other challenge: seeing beyond systems—to understand business wide implications and to examine business processes, not just IT, through a critical lens. They're challenges that demand leadership and involvement from the board and the C-suite.

High maturity

- ☐ Board and C-suite ensure that the cybersecurity program is reviewed for effectiveness and that any identified gaps are appropriately managed in line with risk appetite
- ☐ The board, or a committee of the board, is engaged on a regular basis to review and discuss the implementation of the organization's cybersecurity framework and implementation plan, including the adequacy of existing mitigating controls
- ☐ Regular internal and external assessments (health checks, penetration testing, etc.) of vulnerabilities are conducted to identify cybersecurity control gaps appropriate for the industry
- ☐ Oversight activities include regular cybersecurity budget evaluation, service outsourcing, incident reports, assessment results, and policy reviews/approvals
- ☐ Internal audit evaluates cyber risk management effectiveness as part of their quarterly reviews
- ☐ Organization takes time to absorb important lessons and modify the secure and vigilant aspects of the program to emerge stronger than before

Moderate maturity

- ☐ Basic cyber risk assessments take place on a fixed, unvarying schedule and are not industry-specific
- ☐ Internal audit evaluates cyber risk management effectiveness no more than once a year
- ☐ Lessons learned are sometimes, but inconsistently, applied to improve management of cyber risk



Low maturity

- ☐ Cyber assessments and internal audit evaluations are sporadic or nonexistent
- ☐ Cyber measures remain relatively static and any improvements lack an experiential basis

Are we a strong and secure link in the highly connected ecosystems in which we operate?

10

The cyber readiness of your partners influences your cyber posture. But cyber risk is a two-way street when it comes to partners. Are you a weak link? Are you a leader on cyber risk? Are you making a positive impact when it comes to cyber and the broader business landscape? Collaborating with peer organizations and partners to share intelligence on threats is just one example of how business leaders can develop a more relevant, more holistic approach to cyber risk.

High maturity

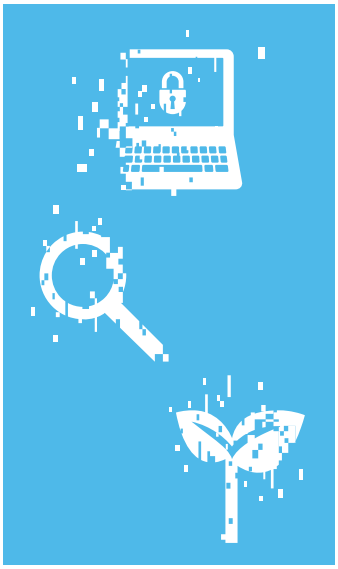
- ☐ Strong relationships are maintained with internal stakeholders, external partners, law enforcement, regulators, etc.
- ☐ Supportive of innovative sharing initiatives that do not compromise information security and privacy
- ☐ Knowledge and information sharing with industry sector, independent analysis centers, government and intelligence agencies, academic institutions, and research firms
- ☐ Expansion of sharing efforts and relationships, to include partners, customers, and end users
- ☐ Preference for vendors that support industry standards and cyber advancements
- ☐ Independently maintain mature programs to avoid being the weakest link

Moderate maturity

- ☐ Ad hoc threat intelligence sharing with peers, or active collaboration with government and private sector on threat intelligence

Low maturity

- ☐ Minimal external relationship development and no information or knowledge sharing with peers, government, or external groups



Setting higher goals, setting strategic goals

Whether you're building or revamping, it's important for organizational risk leaders to set a target state for cyber maturity. Effectively defining that target requires an understanding of the business context and resulting priorities, along with discussions between cyber leaders and decision-makers in the rest of the organization. While not all organizations need to be at the highest level in all areas of cyber maturity, the target state should support the organization in achieving its strategic goals—balanced with the cost and time of achieving it. In many instances, this approach drives the organization toward higher levels of maturity for areas in which cyber risk practices are deemed critical. Developing a mature, advanced cyber risk program is not just about spending money differently. It's about taking a fundamentally different approach—investing in an organization-specific balance of secure, vigilant, and resilient capabilities to develop a program unique to your needs.

Where do you stand?
Based on the results of your assessment, does your current state of maturity support or hinder your strategy and mission? If your maturity index is not aligned with your target state of maturity—or if you have not yet developed appropriate cyber goals—it's time to start enhancing your cyber risk posture.

Of course, it isn't possible for any organization to be 100 percent secure, but it's entirely possible to manage and significantly mitigate the impacts of cyberthreats, including theft, regulatory penalties, legal compensation, and reputational damage. By working collectively, we can minimize the growing potential for broad scale infrastructure outages and business disruption at the national, or even the global, level.

For more information, contact one of our leaders:

Nick Galletto
Global Cyber Risk Services Leader
416-601-6734
ngalletto@deloitte.ca

James Nunn-Price
Asia Pacific Cyber Risk Services Leader
+61 2-9322-7971
jamesnunnprice@deloitte.com.au

Chris Verdonck
EMEA Cyber Risk Services Leader
+32 2-800-24-20
cverdonck@deloitte.com

Ed Powers
US Cyber Risk Services Leader
212-436-5599
epowers@deloitte.com

Deloitte.