Deloitte.

# Cyber security: everybody’s imperative

A guide for the C-suite and boards
on guarding against cyber risks

### Secure

Enhance risk-prioritized controls to protect against known and emerging threats, and comply with industry cyber security standards and regulations.

### Vigilant

Detect violations and anomalies through better situational awareness across the environment.

### Resilient

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

*The following FAQ, presenting 10 questions boards should ask and answer around cyber security and resiliency, is designed as a guide to help rank an organization's cyber posture and capabilities as "high," "moderate" or "low." From the cyber "character" of the board and C-suite, to the strength of the organization's cyber culture, to the organization's role as a global guardian of digital commerce, the questions look through the triple lens of security, vigilance and resilience to help pinpoint critical gaps and potential improvement areas. Traditionally, cyber threat management has focused on the "security" component while paying less attention to "vigilance" and "resilience." Our questions and maturity grading scale are designed to remedy this imbalance and present a full picture of the cyber-protected enterprise.*

## Boards and C-suite have an important role to play in helping organizations determine how to respond to the new cyber threat landscape.

Cyber threats and attacks are growing in both number and complexity. In our digital, information-driven world, that means cyber threat management is a business and strategic imperative. Indeed, the stakes are higher than ever. Cyber crime is more than fraud and theft. It is now the domain of vast criminal networks, foreign government-sponsored hackers and cyber terrorists.

Tangible costs from cyber crime 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 cyber attacks 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.

Effective cyber security starts with awareness at the board and C-suite level – the recognition that at some point your organization will be attacked. You need to understand the biggest threats and learn how they can put the assets at the heart of your organization's mission at risk. As boards and the C-suite take a more active role in protecting their organizations, many grapple with how to make the role effective (what are their responsibilities, which competencies should they be cultivating, what are the right questions to ask, etc.).

As every industry and organization is different, the purpose of this FAQ is not to provide blanket solutions to the issues discussed, but to help organizations identify their most critical issues so they can begin developing a custom cyber security program or improve their existing one. We also hope to promote boardroom discussions around management's ongoing cyber strategies and how effectively they address current and future challenges, mitigate risks and anticipate opportunities.

# Assess your maturity level

This cyber security FAQ and accompanying range of responses should effectively **guide** organizations in assessing their cyber posture; appropriately **challenge** information security teams to up their cyber security game by asking key questions and providing critical information; and help them consistently **monitor** and improve their cyber resilience going forward.

The FAQ is designed to help identify specific strengths and weaknesses and paths to improvement. Determine where your organization's responses to the following questions fall on the cyber security maturity scale:

## Cyber security maturity scale

**High maturity**
We have a strong cyber security posture across the board.

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

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

Question

1

# Do the board and C-suite demonstrate due diligence, ownership and effective management of cyber risk?

## High maturity

□ Board and C-suite hold a C-level executive accountable for cyber threat risk management and are responsible for overseeing the development and confirming the implementation of a cyber security program

□ Board and C-suite stay informed about cyber threats and the potential impact on their organization

□ Board has one or more members – or appropriately leverages strategic advisors – that understand IT and cyber risks

□ A senior management committee has been established that is dedicated to the issue of cyber risk or an alternative senior management committee has adequate time devoted to the discussion of the implementation of the cyber security framework

□ Due diligence is evident in regular updates, budget analysis and challenging questions to management

## Moderate maturity

□ Leadership and board oversight are concerned with cyber security 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 security issues is lacking

□ Board intermittently assesses the cyber security framework and strategic requirements

## Low maturity

□ Tone at the top lacks cyber security focus and understanding of strategic issues

□ Little engagement by leadership in specific IT security issues

□ Board features no significant experience in IT and cyber risks, and cyber security is left to those within IT to resolve

□ Oversight of cyber security and assessment of related budgetary requirements remains at a very high level

Question

2

# Do we have the right leader and organizational talent?

## High maturity

□ Cyber security leader has the right mix of technical and business acumen to understand how the organization operates, engage with the business and know where to prioritize efforts

□ Teams of passionate and energized staff keep up-to-date on the latest cyber security trends, threats and implications for their business

□ Cyber risk discussions are elevated to 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 security leader is in place but is primarily focused on technical risks associated with cyber security

□ Cyber security leader has a working knowledge of the industry but does not fully understand and appreciate how the organization operates

□ Cyber security is a significant focus but remains relatively high level

□ Cyber risk issues often stall at the IT or management level

□ Skilled cyber security staff are present in IT and some business areas but have only occasional industry-specific threat knowledge

## Low maturity

□ Little focus on cyber security from leadership

□ Cyber security knowledge and talent are compartmentalized in the IT function

□ Ad-hoc training programs are developed for specific new technologies

□ High turnover of cyber security staff due to a lack of investment in talent strategy

Question

3

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

## High maturity

- □ Clearly articulated risk appetite and cyber risks are incorporated into existing risk management and governance processes
- □ Established enterprise-wide cyber security policy approved by the board
- □ Clearly described and operationalized roles and responsibilities for each of the three lines of defense
- □ 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 security incidents
- □ Incident management framework includes escalation criteria aligned with the cyber security program
- □ Evaluation and monitoring of the value of cyber insurance is in place

## Moderate maturity

- □ Established cyber security 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 security framework

## Low maturity

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

Question

4

# Are we focused on, and investing in, the right things?

## 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 taken 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 cyber security investments exist) and are reflected within the cyber security strategy
- □ Senior management provides adequate funding and sufficient resources to support the implementation of the organization’s cyber security framework
- □ People are comfortable challenging others, including authority figures, without fear of retribution; those who are challenged respond positively

## Moderate maturity

- □ Cyber security framework is internally focused without added industry-based processes
- □ Cyber security 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 security 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 done
- □ Business case for cyber security investment is rarely made

Question

5

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

### High maturity

- □ Comprehensive cyber security 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 security program
- □ Organization periodically internally verifies its 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 security program implements a number of industry best practices and capabilities, including basic online brand monitoring, automated malware forensics and manual e-discovery, criminal/hacker surveillance, workforce/customer behaviour profiling, and targeted cross-platform monitoring for internal users
- □ Compliance and other internal program reviews may be occasionally, but are not consistently, undertaken

### Low maturity

- □ Cyber security 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

Question

6

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

## 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 cyber risk vocabulary that promotes shared understanding

□ Company-wide education and awareness campaign established around cyber security (all employees, third parties, contractors, etc.)

□ Awareness and training specific to individual job descriptions helps staff understand their cyber security responsibilities

□ People take personal responsibility for the management of risk and proactively seek to involve others when that is the better approach

## Moderate maturity

□ General information security training and awareness is in place

□ Targeted, intelligence-based cyber security awareness focused on asset risks and threat types is in place

## Low maturity

□ Acceptable usage policy is in place

□ Little emphasis on cyber security outside of IT

□ Awareness and training issues are reactively addressed in that training is given only after a breach or non-compliance is discovered, and only to a small subset of individuals

Question
7

## What has management done to protect the organization against third-party cyber risks?

### High maturity

□ Cyber security risks are seen as part of the due diligence process for critical outsourcing and sub-contracting arrangements

□ All third parties are engaged through a consistent process, and policies and controls are in place (e.g., right to audit) that align to the organization’s expectations and risk tolerance

□ Third parties receive specific training on cyber security 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 security 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 sub-contracting arrangements is encouraged but inconsistently applied

□ Communication from third parties respecting cyber security 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 non-existent

Question

8

## Can we rapidly contain damages and mobilize diverse response resources should a cyber-incident occur?

### 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 security incident response plans and procedures are documented and rehearsed through war gaming, simulations and team interaction

□ External communications plan exists to address cyber security 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 cyber attack simulations are regularly undertaken

□ Cyber attack 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 non-existent

> “While cyber security posture must be flexible depending on an organization’s size and maturity level, the key is to develop a security level that lets you anticipate, defend and recover from your industry’s most common and emerging threats.
>
> Adel Melek, Managing Director, Global Enterprise Risk Services

Question

9

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

## High maturity

□ Board and C-suite ensure that the cyber security 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 cyber security 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 cyber security control gaps appropriate for the industry

□ Oversight activities include regular cyber security 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 security 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

□ Learnings are sometimes but inconsistently applied to improve cyber security

## Low maturity

□ Cyber security assessments and internal audit evaluations are sporadic or non-existent

□ Cyber security measures remain relatively static and any improvements lack an experiential basis

Question

10

## Are we helping to protect our industry, the nation and the world against cyber risks by taking a holistic approach to knowledge and information sharing?

### High maturity

□ Strong relationships with internal stakeholders, external partners, law enforcement, regulators, etc.

□ Support innovative sharing initiatives that do not compromise information security and privacy

□ Knowledge and information sharing with sector, independent analysis centres, government and intelligence agencies, academic institutions and research firms

□ Expansion of sharing efforts and relationships that includes partners, customers and end users

□ Preference for vendors that support industry standards and cyber security advancements

□ Maintain mature programs ourselves to avoid being the weakest link

### Moderate maturity

□ Ad-hoc threat intelligence sharing with peers or active collaboration with government and sector on threat intelligence

### Low maturity

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

> “As private and public sector actors take steps towards greater accountability and capabilities, discussions on collaboration across sectors and regions can be undertaken with greater trust, confidence and experience.

The World Economic Forum in collaboration with Deloitte. *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience.* (June 2012)

# Everyone needs to up their game

Whether you're building or revamping, it's important for organizational risk leaders to set a target state of maturity for cyber security. The target state for maturity is best defined through an understanding of the business context and resulting priorities along with discussions between cyber security 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 security maturity, the target state needs to support the organization in achieving its strategic goals balanced with the cost and time of achieving it. In many instances, this results in the organization striving for higher levels of maturity where cyber security 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 security goals – it's time to start enhancing your cyber security posture. With defence strategies moving rapidly from incident response solutions to the concept of zero day vulnerability, where vigilant organizations anticipate breaches and prevent them before they happen, prudent, responsible companies cannot afford to lag behind.

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 cyber threats, 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**
National Leader
Cyber Risk Services
416-601-6734
ngalletto@deloitte.ca

**Marc MacKinnon**
National Leader
Security, Privacy and Resiliency
416-601-5993
mmackinnon@deloitte.ca

**Adel Melek**
Managing Director
Global Enterprise Risk Services
416-601-6524
amelek@deloitte.ca

## In collaboration with

**Paul D. Milkman**
Head of Technology Risk Management
and Information Security
TD Bank Group
paul.milkman@td.com

Cyber Intelligence Centre

www.deloitte.ca/cyber

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Designed and produced by National Design Studio, Canada 14-2514T