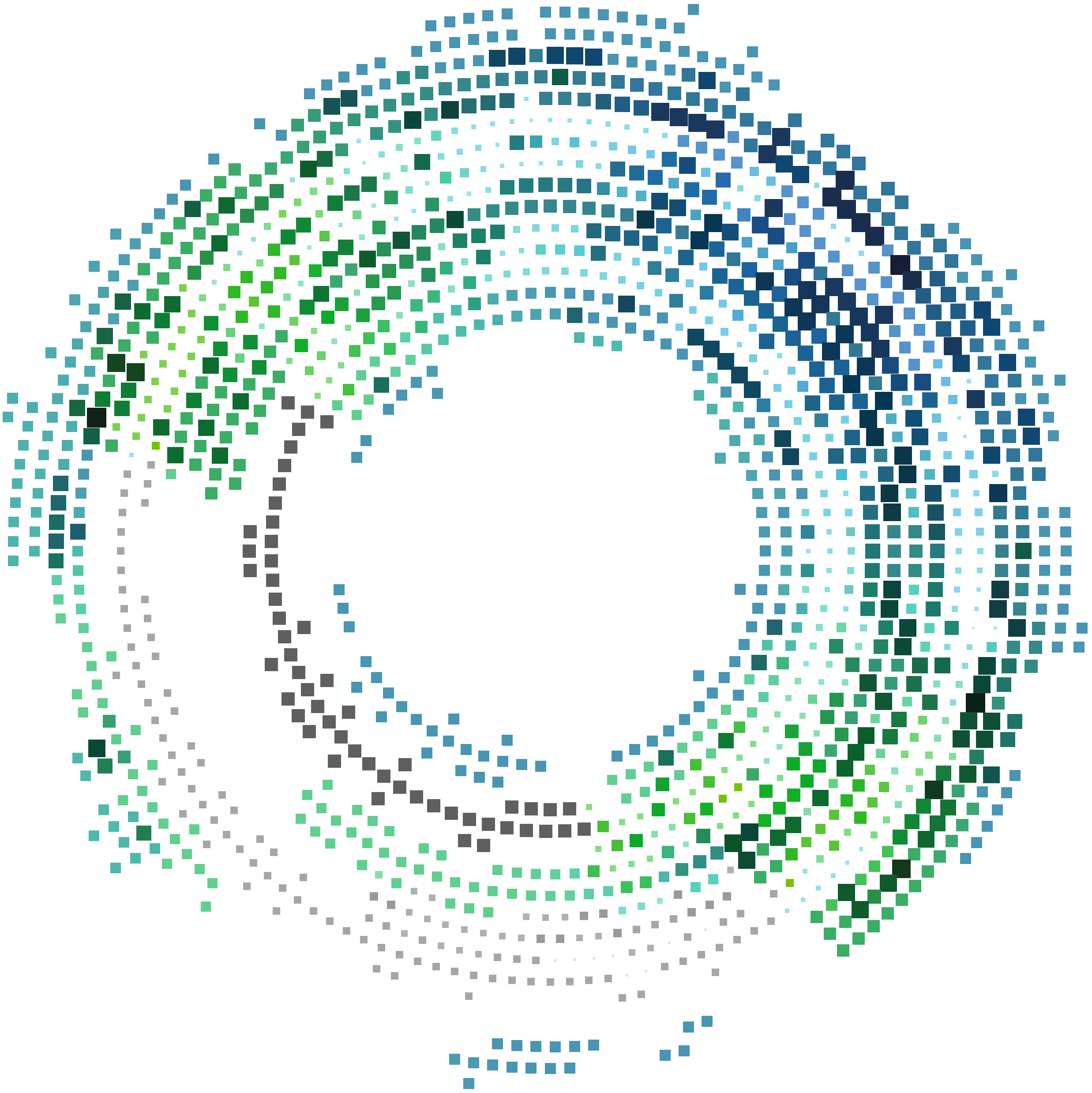
Deloitte.

德勤



Cyber Risk

Risk powers performance

Cyber ●

Assessing cyber risk

Critical questions for the board and the C-suite

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 ffectiveness 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.

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.

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

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

2. Do we have the right leader and organizational talent?

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 ppropriate 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

Cyber crisis management

Readiness, response,and recovery

Readiness, response, and recovery

Hacked devices, crashed websites, breached networks, denials of service, copied emails, stolen credit card data, and other cyber incidents have become commonplace. It's enough to leave one thinking—correctly—that no organization can achieve totally assured cybersecurity.

Most organizations have therefore developed some level of cyber incidence response (CIR) capabilities. Yet those capabilities, which are often weighted toward short-term responses and IT issues, may fail to address all impacts of a cyber incident and keep it from reaching crisis proportions.

Avoiding a cyber crisis often comes down to properly managing a cyber incident before, during, and after it unfolds. This starts with a broad view of cyber crisis management. Executives often see cyber incidents as "an IT issue," when IT is only one domain involved. Forward-thinking management teams recognize that effective crisis planning involves multiple functions and skill sets. They also recognize that these must be highly coordinated if an incident is to be contained or, if an incident does escalate to crisis levels, managed.

The need for crisis planning

CBS.com notes that 1.5 million cyberattacks occur every year, which translates to over 4,000 attacks every day, 170 every hour, or nearly three every minute.[1] While few attacks succeed, the high probability of cyber incidents dictates that every organization needs to be prepared to respond effectively.

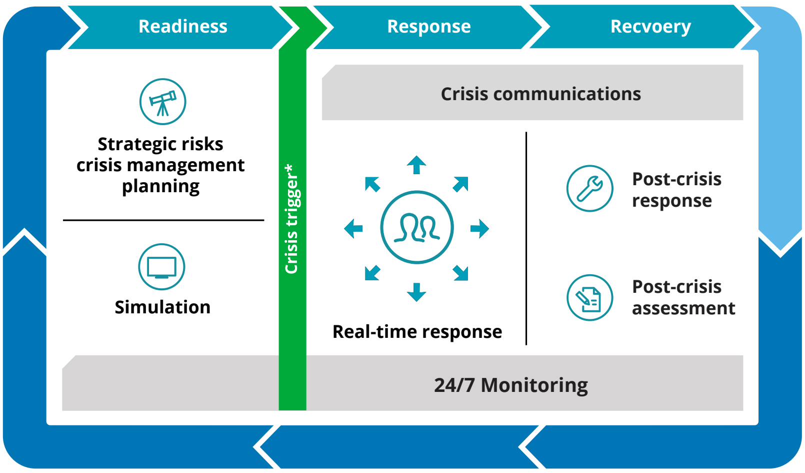
Effective preparation addresses the entire crisis management lifecycle of readiness, response, and recovery (see Exhibit 1).

Each phase of this lifecycle presents opportunities to protect the organization from risks, costs, and damage emanating from an incident—and to strengthen the organization's defenses going forward:

Readiness

Readiness equates not only to vigilance, for example in the form of 24/7 Monitoring, but also to readiness of resources. A well-prepared, multifunctional team must be poised to deal with all aspects of an incident or crisis. In addition, crisis simulation and war-gaming enables management to understand what can happen, which steps to take, and whether the organization is truly prepared.

Exhibit 1: Deloitte's crisis management lifecycle



🟩 *cyberattacks | natural disaster | misdeeds and financial crimes | financial disruptions industrial accidents | civil or political unrest

Response

Management's response can either contain or escalate an incident; indeed, a poor response can even create a crisis. Vigorous, coordinated responses to incidents limit lost time, money, and customers, as well as damage to reputation and the costs of recovery. Management must be prepared to communicate, as needed, across all media, including social media, in ways that assure stakeholders that the organization's response is equal to the situation.

Recovery

Steps to return to normal operations and limit damage to the organization and its stakeholders continue after the incident or crisis. Post-event steps include assessments of the causes and of the management of the incident or crisis, and promulgation of lessons learned.

Effective crisis management extends beyond preparing for any specific event to development of broad, flexible capabilities that enable response to a wide range of events along various dimensions. From the standpoint of cybersecurity—the main deterrent to cyber incidents—the goal is to develop a secure, vigilant, and resilient organization.

IT and digital assets now drive a huge portion of enterprise value. Knowing this and understanding system vulnerabilities, attackers target organizations repeatedly and from various angles. Therefore, the risk that cyber crises pose to reputation, brand, operations, and customer and supplier relationships will continue to increase, as will the associated legal and financial effects.

No board of directors or senior executive team can credibly deny the seriousness or the likelihood of cyberthreats. So, the time to prepare a highly effective cyber crisis management plan is before a cyber incident occurs.

[1] CBS News, These cybercrime statistics will make you think twice about your password: Where's the CSI cyber team when you need them?

Secure, vigilant, and resilient

In pursuing cybersecurity, an organization should strive to become:

Secure

A secure organization prioritizes the value of digital assets, with a focus on what matters most to the organization. All data is not created equal, nor is it practical or possible to provide complete security for all data. By prioritizing the value of digital assets, management can allocate resources according to the value of the assets, with the goal of obtaining a level of security that corresponds to their value.

Vigilant

Vigilance demands that everyone be aware of how they could expose the organization to cyber risk through their devices, social media, and online conduct. A vigilant approach rests on gathering threat-related intelligence and gauging the range of threats that could harm the organization. This information also informs cyberthreat monitoring. In addition, policy development, training, and accountability regarding cyber incidents each play a key role in maintaining vigilance.

Resilient

A resilient organization aims to minimize the impact of an incident on its stakeholders while quickly restoring operations, credibility, and security. Rapid detection of cyber incidents and well-structured recovery plans can usually limit damage. Recovery plans should designate clear roles, responsibilities, and actions to mitigate damage and reduce future risk, remediate the situation, and return to normal operations.

A secure, vigilant, resilient organization has all three phases of cyber risk management covered. Deloitte strives for this state as an organization and has organized cyber risk services to enable clients to do the same.

The cyber incident response lifecycle

While the precise nature, location, and impact of incidents cannot be predicted, the incident response lifecycle follows a predictable path (see Exhibit 2).

The CIR lifecycle illustrates the interplay between organizational capabilities and stakeholder confidence. Immediately after an incident, affected capabilities must be restored. This usually takes hours or days, but can take weeks or months in severe cases. Also, cybersecurity must be enhanced to secure the environment, improve visibility into threats, and reduce the impact of future incidents.

Containing an incident and avoiding a crisis calls for proactively addressing stakeholder concerns. Customers usually express concern regarding loss of personal data and privacy and may develop long-term brand aversion.

Business partners are concerned about near-term cross-contamination of their systems and the longer-term integrity of data and transactions. Employees may be overwhelmed by negative publicity and increased stress. Regulators want assurance regarding consumer protection, and the state of the business and industry. Investors are attuned to short-term financial impacts and longer-term business and brand viability.

Over the course of the response lifecycle, crisis communications stand among the highest priorities.

Specifically, the organization must:

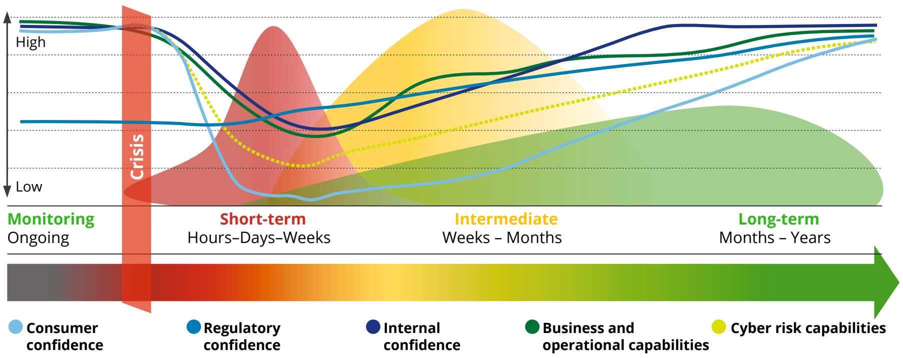
- Respond to a high volume of requests from customers, business partners, vendors, regulators, law enforcement, and the board of directors
- Manage requests from business partners to modify arrangements, processes, and methods of sharing information
- Engage in proactive messaging to the broader base of stakeholders and the public regarding what is known and not known, and what the organization is doing
- Monitor and address traditional, web-based, and social media reactions to the event and to the organization's response and intentions

In addition, management must:

- Address any potential threat of legal or regulatory action, and determine what legal recourse is available to the organization
- Minimize the time between developing and implementing the remediation plan, while also managing the risks generated in that interim.

The more comprehensive and tested the plan, the better management's response to an incident will be. Yet management should understand that the plan does not represent a script that will play out in reality and that responses must be flexible and fluid. You may have to depart from the plan, but the plan will provide a framework and guidance for coordinating the diverse elements involved in the response.

Exhibit 2: Cyber incident response lifecycle



Getting coordinated

Cyber incident response programs require coordination in six key areas: governance, strategy, technology, business operations, risk and compliance, and remediation.

1 Governance

Governance frames the way you organize and manage your response team. It ensures program coordination across functional areas, documentation of all policies, procedures, and incidents, and clear communication roles, responsibilities, and protocols. Governance aligns response strategy with goals and provides mechanisms for cross-functional communication.

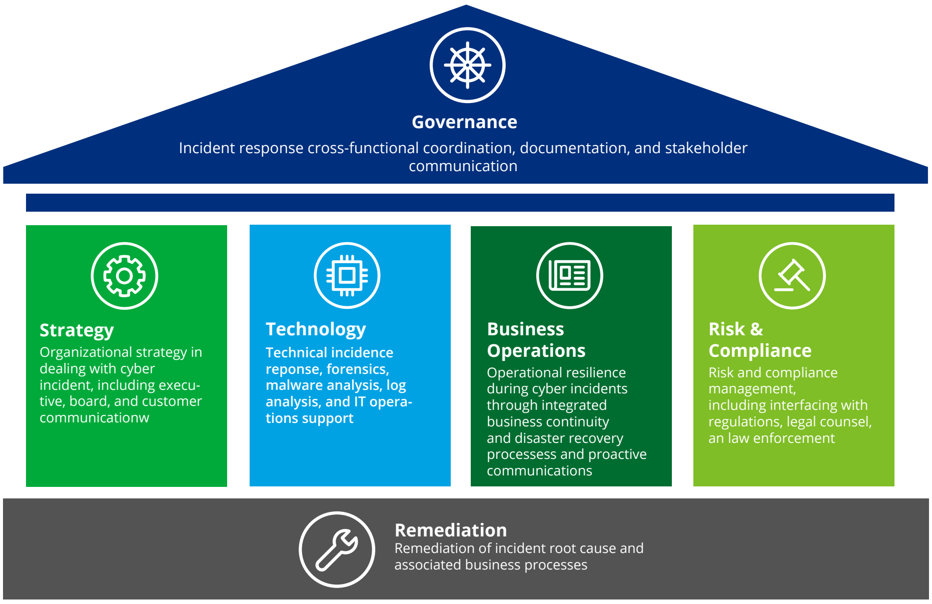
Key steps in establishing governance for response management include:

- Segregating duties by establishing an independent investigation team to help determine causes and remediation steps
- Considering the role of legal counsel, who should be on or represented on the response team, which should be led by a business manager (to foster a cross-functional approach to CIR)
- Defining incident response and recovery lifecycle phases and a decision framework with clear steps and measures of success

Key questions

- Do we have the right team in place?
- What should be reported, to whom, and when?
- Are we periodically testing our planand training our staff?
- How are we incorporating lessons learned?

Exhibit 3: Cross-functional capabilities required for effective response



Governance
Incident response cross-functional coordination, documentation, and stakeholder communication

Strategy
Organizational strategy in dealing with cyber incident, including executive, board, and customer communicationw

Technology
Technical incidence reponse, forensics, malware analysis, log analysis, and IT operations support

Business Operations
Operational resilience during cyber incidents through integrated business continuity and disaster recovery processess and proactive communications

Risk & Compliance
Risk and compliance management, including interfacing with regulations, legal counsel, an law enforcement

Remediation
Remediation of incident root cause and associated business processes

2 Strategy

Response strategy defines how you lead, prioritize, and communicate during incident response and crisis management. Organizations should align response strategy with the organization's responsibilities and values. A sound strategy frames a cost-effective, well-resourced, organization-wide approach to addressing cyber incidents. This minimizes "tunnel vision" in response planning and reduces adverse impact to operations and revenue.

Key aspects of response strategy include:

- Defining escalation and prioritization processes to manage and coordinate IT, operational, and business recovery
- Engaging the organization's government affairs team or other government liaison function to inform and work with regulatory agencies and any appropriate officials—an essential step in any regulated industry
- Aligning response efforts with security management and IT engineering initiatives

Key questions

- When should the C-suite and board be informed?
- Does our strategy address internal and external coordination?
- How will we assist affected stakeholders?
- What are the best communication channels?

3 Technology

The IT and cybersecurity teams develop and implement mechanisms for detecting, monitoring, responding to, and recovering from a cyber incident or crisis. IT engineers create the needed architecture, and IT works to maintain systems that are resistant to attacks.

Technical forensic and investigative capabilities are vital to preserving evidence and analyzing control failures, security lapses, and other conditions related to the incident (see pg 24: After an incident: Investigation and response). In addition, organizations should implement both proactive and responsive technology solutions to mitigate future cyber incidents.

Key steps in framing the technology aspects of incident response include:

- Being realistic about IT tools, which enable security and operational capabilities, but do not eliminate risk
- Resolving the tension between immediate needs in the wake of an incident and longer-term remedies
- Accepting that workarounds and throw-away work are often necessary to meet near-term priorities

Key questions

- Which incident and crisis mitigation techniques are we employing?
- What technical capabilities do we have, and what are we missing?
- Do we have access to forensic resources?
- How are we gathering and using threat intelligence?

After an incident: Investigation and response

Think of a digital crime scene as you would a physical crime scene: trampling evidence or cleaning things up can make forensic tasks difficult to impossible. So, the team should start by securing the digital crime scene and preserving evidence.

However, saving the "victim"—a damaged or compromised system required to run a process or business—may also be a priority. That "victim" may require first aid when the recovery strategy calls for restoring the same system as quickly as possible. In such cases, the business needs to balance that decision and associated activities against the need to preserve evidence for analysis.

In general, the following steps to address a cyber incident can assist in identifying causes and remedies, and hasten recovery:

- Document how the incident came to light, who reported it, and how they were alerted; interview IT staff and other relevant parties
- Consider and research the possibility of insider involvement and take steps to minimize this risk going forward
- Identify affected systems and isolate them so no one attempts to fix, patch, or alter the state of the systems
- Gather all available evidence and analyze it to determine cause, severity, and impact of the incident
- Strengthen network security, improve protocols, and increase vigilance as indicated by the analysis
- Enhance monitoring and other measures to mitigate future risk of similar incidents and enhance policies that may increase security
- Document and report the findings to any relevant stakeholders and consider potential requirements to report the incident to a regulatory body

Without an effective investigative response, the causes of the incident may never be understood, and the risk of a repeat incident may actually increase. Speed is essential to limiting damage after an incident. For example, for insurance purposes immediate response can result in more accurate loss measurement and claim quantification, and faster settlement of a claim.

4 Business operations

After an incident, critical business operations must resume as soon as possible to minimize disruptions that generate financial, reputational, regulatory, and stakeholder impacts.

Keys to minimizing business disruption include:

- Implementing out-of-band processes to replace those that are broken or that present too many constraints during incident response or to remediation
- Planning for surge support and allocating resources accordingly
- Understanding existing business limitations, such as the risks associated with using standard payments systems or certain applications

Key questions

- Which business processes and applications are most critical to operations?
- What infrastructure must be given the greatest protection?
- How will we go about returning to full operations?
- How can staff, suppliers, and partners support recovery?

5 Risk and compliance

Risk and compliance functions should assess and manage the regulatory compliance elements of incident and crisis response, including interfacing with legal counsel, regulators, and law enforcement. The keys are to be able to comply with requirements and to demonstrate compliance. For example, after an incident, investigative processes and responses must be documented to demonstrate the adequacy of both.

Keys to successful management of risk and compliance after an incident include:

- Anticipating requests from regulators and law enforcement, which may include requests for access to systems and a review of response activity
- Analyzing the impacts and loss exposures for insurance and other reporting purposes
- Understanding any additional risks brought about by ad hoc processes, technology, and work-arounds required during incident response

Key questions

- What are the breach notification requirements?
- What are the regulatory and third-party obligations?
- When and how do we inform law enforcement?
- How could this particular incident—or a pattern of incidents—impact the organization's compliance posture?

6 Remediation

Remediation begins after critical business operations resume, with short- and long-term efforts to close gaps. The organization must verify that attack vectors are eradicated and take steps to prevent similar attacks in the future. Remediation must eliminate or minimize root causes of incidents and return businesses, functions, IT, and stakeholders to a secure operating environment.

Keys to successful remediation include:

- Balancing the inclination to secure digital assets against the need to do business seamlessly
- Prioritizing the influx of technology project requests and increased IT budgetary needs
- Preparing for increased regulatory scrutiny and a potentially more rigorous regulatory regime

Key questions

- Have the IT and business-process root causes been identified?
- Has a remediation plan been developed?
- Have the root causes been eliminated or minimized?
- What are the lessons learned and how can we apply them?

The response team should include individuals from each of the above six areas to develop a well-resourced, balanced, consistent approach to cyber incidents and cyber crises across the organization.

Five lessons in crisis management

Deloitte's work in crisis management with senior executive teams has yielded the following lessons:

1. **There's no substitute for preparedness.**
   Wargaming, rehearsals, and other structured preparations do much to position the organization to launch a coordinated response.

2. **Every decision counts.**
   In a crisis every decision can affect stakeholder value mainly through heightened reputational risks, which can destroy value faster than operational risks.

3. **Response times should be in minutes.**
   Teams on the ground must respond rapidly, not in hours or days. They must take control, lead with flexibility, act on incomplete information, communicate well, and inspire confidence.

4. **When the crisis has passed, work remains.**
   After breathing a sigh of relief, you must capture data, log decisions, manage finances, handle insurance claims, and meet legal and regulatory requirements.

5. **You can emerge stronger.**
   Almost every crisis creates opportunities for an organization to shine, first, by responding effectively and, second, by searching out opportunities to improve.

Customers, suppliers, employees, and other stakeholders understand that crises will occasionally affect the organization. What they find hard to understand are lack of preparation, inadequate responses, and confusing communications on the part of management.

Are you ready?

Most organizations will lack the resources to develop and maintain all necessary incident and crisis response capabilities in-house. The expertise required, the evolving risk landscape, and the resources of cybercriminals render it impractical for most organizations to go it alone. Thus, an outsourced or co-sourced approach with a provider of managed cybersecurity and response services may be the best option for most organizations.

Leveraging cyberthreat intelligence capabilities, for example via sharing with industry peers or outsourcing to specialists will make sense for many organizations. Many will also benefit from external support in developing and maintaining cyber monitoring and cyber risk management programs. For example, 24/7 Monitoring can provide early warnings of cyberthreats and risk sensing can detect patterns of criminal activity, but would not be economically viable for most organizations to develop on their own. By the same token, objective verification of readiness, response, and recovery plans, by means of crisis simulation, wargaming, and other assessments, can detect gaps and weaknesses in those plans.

When it comes to incident and crisis management, readiness is an evolutionary state. What you were ready for yesterday may be the last thing cybercriminals have in mind today. Indeed, you cannot really know the specific source or target of the next attack. But you can gauge risks based on the value of your digital assets and the impact of their being compromised. You can gauge likelihood. And you can ready the organization for effective response and recovery.

Contacts

Tonny Xue
Partner
Risk Advisory
Tel: +86 10 8520 7315
Email: tonxue@deloitte.com.cn

Steven Feng
Partner
Risk Advisory
Tel: +86 21 6141 1575
Email: stefeng@deloitte.com.cn

Terence Tang
Partner
Risk Advisory
Tel: +86 755 3353 8639
Email: tertang@deloitte.com.cn

Thomas Lee
Partner
Risk Advisory
Tel: +852 2852 1931
Email: thomalee@deloitte.com.hk

Tommy He
Partner
Risk Advisory
Tel: +86 10 8512 5312
Email: the@deloitte.com.cn

Alexander Shi
Partner
Risk Advisory
Tel: +86 21 2316 6953
Email: alexshi@deloitte.com.cn

Eva Kwok
Partner
Risk Advisory
Tel: +852 2852 6304
Email: evakwok@deloitte.com.hk

About Deloitte Global
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 244,400 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte in Greater China
We are one of the leading professional services providers with 24 offices in Beijing, Hong Kong, Shanghai, Taipei, Changsha, Chengdu, Chongqing, Dalian, Guangzhou, Hangzhou, Harbin, Hefei, Hsinchu, Jinan, Kaohsiung, Macau, Nanjing, Shenzhen, Suzhou, Taichung, Tainan, Tianjin, Wuhan and Xiamen in Greater China. We have nearly 13,500 people working on a collaborative basis to serve clients, subject to local applicable laws.

About Deloitte China
The Deloitte brand first came to China in 1917 when a Deloitte office was opened in Shanghai. Now the Deloitte China network of firms, backed by the global Deloitte network, deliver a full range of audit, consulting, financial advisory, risk management and tax services to local, multinational and growth enterprise clients in China. We have considerable experience in China and have been a significant contributor to the development of China's accounting standards, taxation system and local professional accountants. To learn more about how Deloitte makes an impact that matters in the China marketplace, please connect with our Deloitte China social media platforms via www2.deloitte.com/cn/en/social-media.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the "Deloitte Network") is by means of this communication, rendering professional advice or services. None of the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

CQ-059EN-16

This is printed on environmentally friendly paper