Deloitte.

Cyber crisis management: Readiness, response, and recovery

Strategic & Reputation Risk

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.

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.

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

Recovery

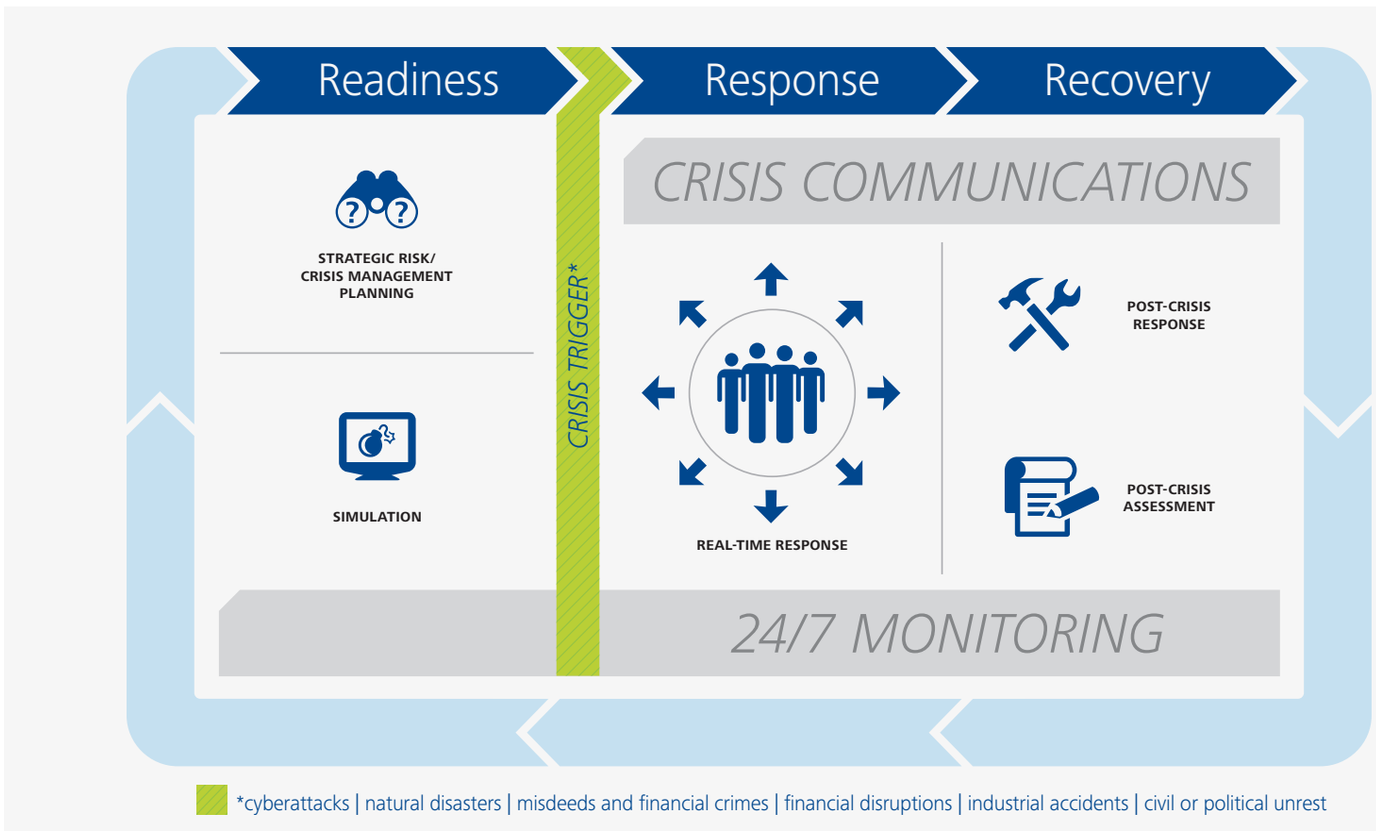
Steps to return to normal operations and limit damage to the organization and its stakeholders continue after the incident or crisis. Post-event steps include assessments of the causes and of the management of the incident or crisis, and promulgation of lessons learned.

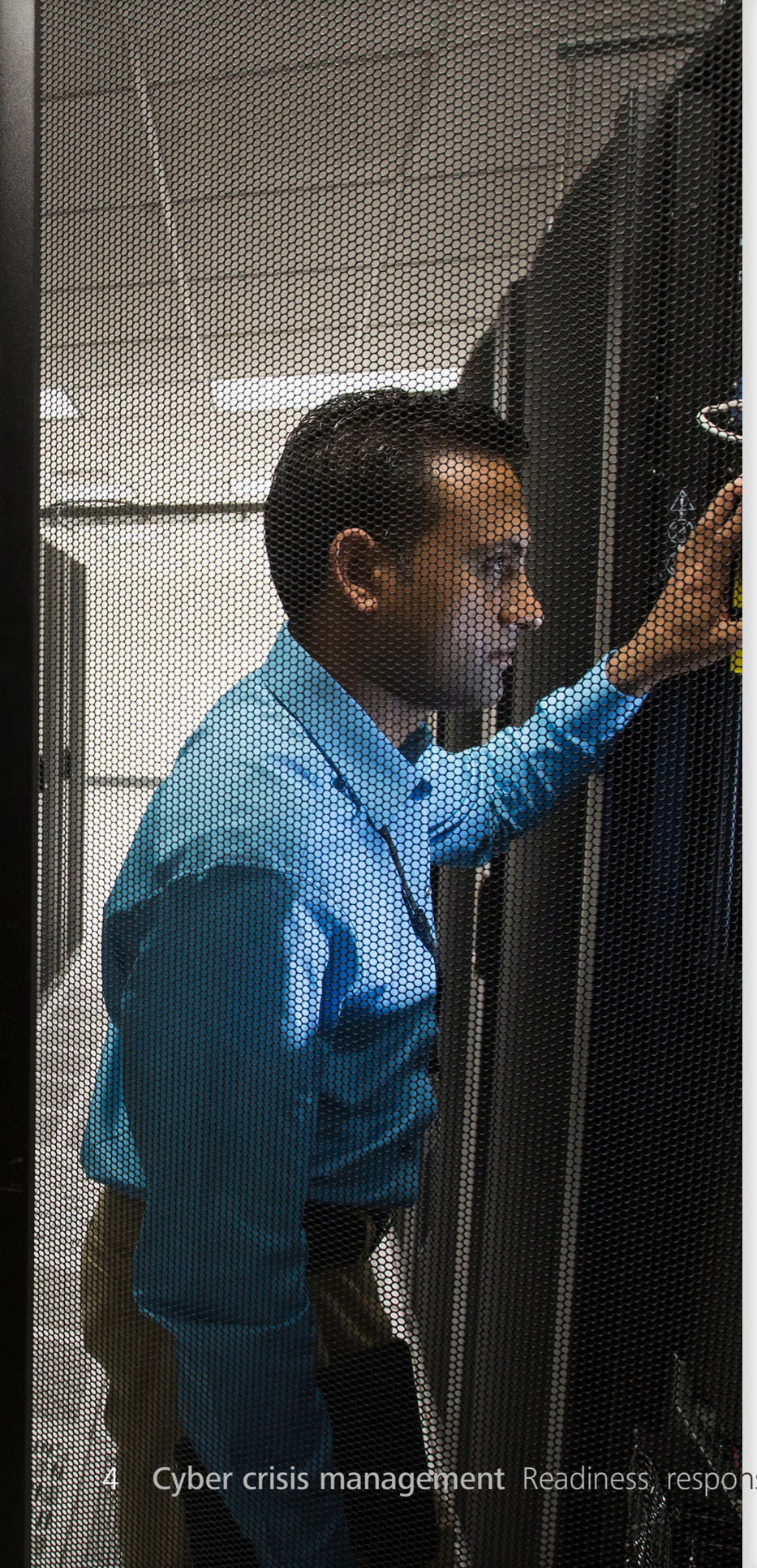
Effective crisis management extends beyond preparing for any specific event to development of broad, flexible capabilities that enable response to a wide range of events along various dimensions. From the standpoint of cybersecurity—the main deterrent to cyber incidents—the goal is to develop a secure,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

Exhibit 1
Deloitte's crisis management lifecycle





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*).

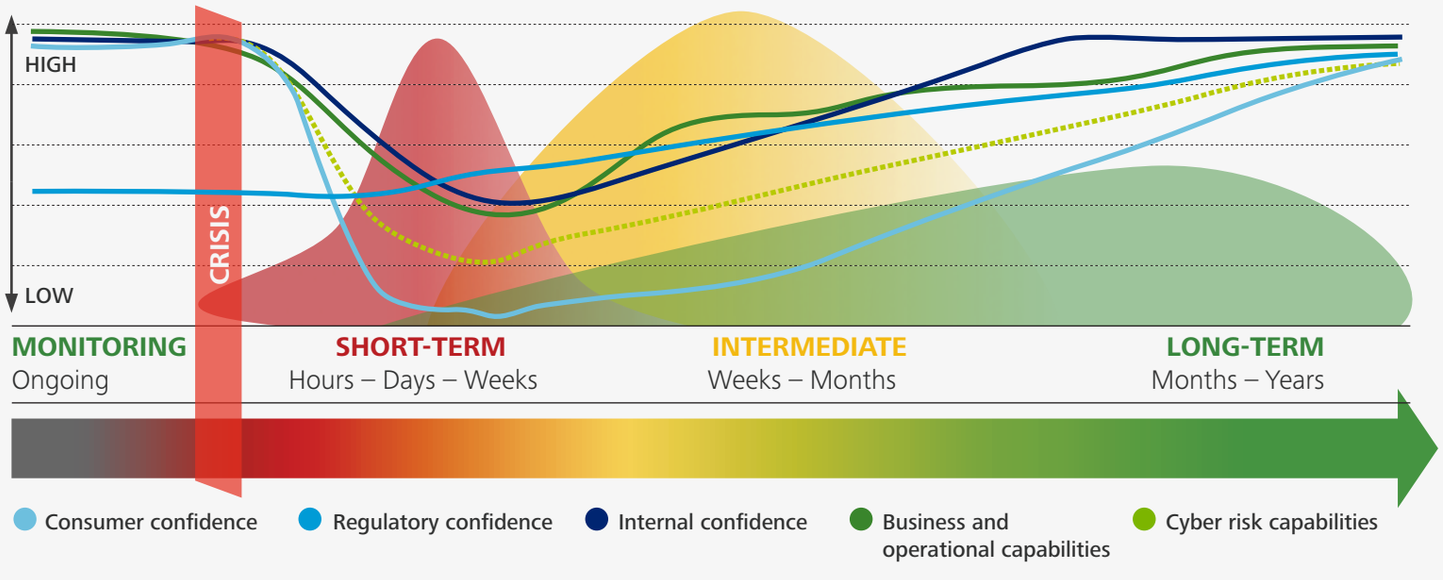
The CIR lifecycle illustrates the interplay between organizational capabilities and stakeholder confidence. Immediately after an incident, affected capabilities must be restored. This usually takes hours or days, but can take weeks or months in severe cases. Also, cybersecurity must be enhanced to secure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

Exhibit 2

Cyber incident response lifecycle



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.

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:

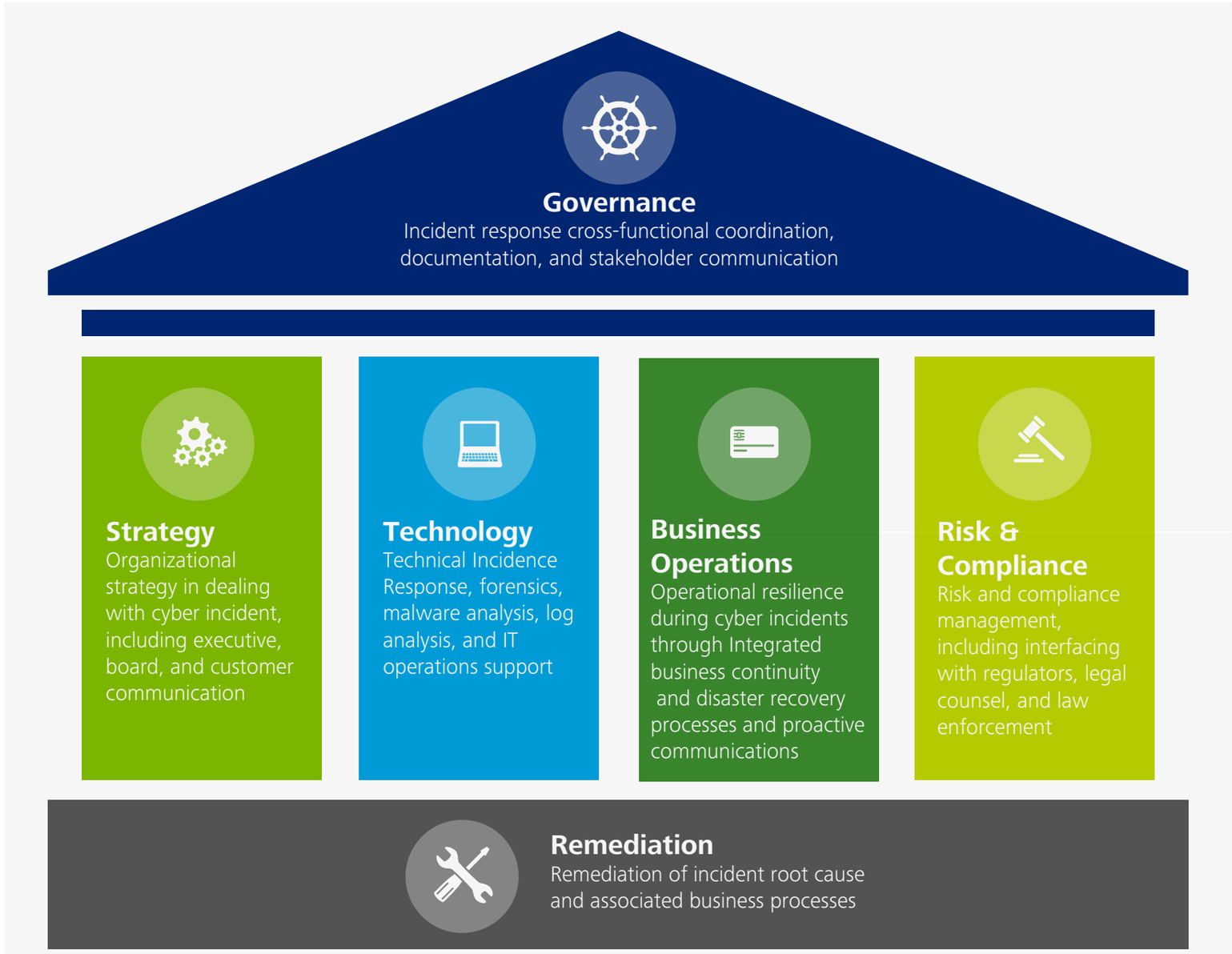
- Segregating duties by establishing an independent investigation team to help determine causes and remediation steps
- Considering the role of legal counsel, who should be on or represented on the response team, which should be led by a business manager (to foster a cross-functional approach to CIR)
- 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 plan and training our staff?
- How are we incorporating lessons learned?

Exhibit 3

Cross-functional capabilities required for effective response



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 sidebar: *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.

Let's talk

For more information, please contact your local crisis management leader
www.deloitte.com/crisiscontacts

Deloitte.