MITSloan Management Review

DIGITAL RESILIENCE

Develop Your Cyber Resilience Plan

A four-part framework can help you create an effective cyber resilience plan to minimize damage and sustain operations through a cyberattack.

Chon Abraham, Ronald R. Sims, and Tracy Gregorio • June 02, 2020

READING TIME: 11 MIN

Imagine rushing through a crowded airport with your locked suitcase. Before you can get to your closing gate, someone steps in front of you, blocking your way. Your belongings are safe in your suitcase, but you can't proceed with your travel plans. In this analogy, your suitcase functions like cybersecurity — protecting against the attacks you can anticipate. However, because you're lacking cyber resilience — the ability to

withstand unanticipated disruption — your travel plans are foiled nevertheless.

Cybersecurity and cyber resilience are distinct concerns, and understanding the difference is key to preparing an effective response to cyberthreats. The misconception that a cybersecurity program can substitute for cyber resilience is potentially disastrous. While cybersecurity focuses on keeping attackers out, cyber resilience aims instead to minimize the mayhem caused by attackers who do manage to penetrate networks.

As cyberthreats evolve, cybersecurity ratings are poised to become as important a factor as credit ratings, making failure to implement a professional cyber resilience program more than a reputational risk. A thoughtfully designed cyber resilience program will become not only a competitive advantage but a requirement for sustained growth.

The four-phase cyber resilience framework described here — preparation, detection, response, and recovery — can enhance an organization's capacity to sustain operations through a cyberattack while minimizing both disruption and reputational harm. Stakeholders involved in developing such a plan may include C-level executives such as the CIO and chief information security officer (CISO), along with the security operations center and the incident response team. This article explores each of the four phases and provides examples of the types of challenges companies encounter, as well as opportunities for becoming more cyber resilient.

Phase 1: Preparation

Effective preparation is a collaborative effort of greatest importance and directly proportional to the effectiveness of the resilience plan as a whole. This first phase requires the most organizational support in terms of resources and budget and entails collaboration across the organization. Working together, senior leadership, information security experts, and business continuity managers can prepare a comprehensive plan to sustain critical capabilities and operations through a cyberattack. Necessary preparation steps include the following:

Develop cyber governance policies. Begin by defining the organization's risk tolerance — that is, what you are willing to lose access to for the sake of sustaining operations. IT security leaders can then develop a transparent policy tailored to the organization's risk tolerance. Plan the personnel and technical capabilities needed based on the maximum time, in hours or days, that the organization can last before using backup systems and data sources. Decide how recent backup data must be — hours, days, or weeks old — to support operations. Policies should also cover the timely reporting of suspicious activity and the frequency of monitoring threat intelligence reports, specifying when to seek assistance from private and/or federal cyber authorities when anomalies are detected.

Know your current systems, technologies, and data sources. Determining which systems are actually at risk is an ongoing, repeated process that requires prioritization of the systems and data sources to protect. To identify what's vulnerable and create a plan for securing those high-risk elements, first prioritize critical business functions and associated systems (including data sources and vendor exchanges). Then explore how these critical assets could be affected in various breach scenarios.

Cybersecurity managers should continually update an inventory of the network's necessary data assets and systems

and document the following:

- How any system is identified on the network and its access procedures, such as via application programming interfaces.
- Any technologies that interface with the network, such as internet-of-things devices.
- Data sources used by systems and technologies on the network.
- The individuals and groups that have access to these systems.
- Regular checks that active security controls are functioning properly and "on."

Consistently update and test backups. It's hard to overstate the importance of frequently updated, regularly tested backups. Teams should create documentation for backup storage locations and check regularly to ensure that the backups are occurring as scheduled.

To minimize downtime in case of attack, the IT security and business continuity teams must ensure that any media and resources needed to import the backup are readily accessible. It's important, too, to know how long backup data retrieval and import take, and to account for physically transporting data servers or hardware if necessary. During the 2017 WannaCry ransomware attack that paralyzed organizations worldwide, for example, many companies were hamstrung by their lack of such information: not knowing the kind of media storage used for backups, where backups resided, or who handled backups (internal personnel or outsourced resources); not understanding how to effectively employ their backups; or being unsure of the integrity of backup data.

Establish a due diligence vetting process for vendors. Design vetting procedures to ensure that vendors, particularly cloud

service providers, have a resilience plan for their own business continuity. Some guidelines for vendor diligence include FedRAMP, the Federal Risk and Authorization Management Program, which the U.S. government developed to hold federal vendors to a specific set of standards and can guide an organization in developing standards suited to its needs.

Embrace automation. Using artificial intelligence (AI) and machine learning in cybersecurity platforms for self-defense can significantly insulate the organization from damage, because these technologies are able to learn from what they experience as "normal" and create alerts if they detect abnormal or atypical behavior. For example, AI and machine learning may readily detect unscheduled decreased system performance or downloads of bulk sensitive data at a nonscheduled time; this would trigger a shutdown of possibly infected systems, a snapshot of the activity log, and rerouted transactions (to a backup or mirrored server) to continue operations while diagnosing the threat.

Plan for alternative workspaces. To ensure that the workforce can operate in the event of an ongoing cyberattack, determine your needs for backup mobile devices and alternative workplaces with connectivity and network access that are ready to be used if needed during recovery.

Train, train again, and train one more time. Ongoing training — of the security team, customer-facing personnel, and back-end administrators — is essential for the team to understand what procedures to follow in transitioning to a business continuity plan in the midst of a cyber event. CISOs should run tabletop exercises on stopping the attack and on remaining operational during the attack. They should also encourage departments to role-play their own critical incidents, including reverting to manual processes if technical systems are not

functional. Key organizational stakeholders (departmental managers and operational personnel) and the cybersecurity team need to understand what to do when trouble hits, so the plan itself must be updated and tested at least once a year. It's vital that all stakeholders know who to call and what to do to get the company up and running in a hurry.

Phase 2: Detection

Detection, like preparation, requires collaboration. Depending on the organization's capacity and needs, a centralized unit, such as the security operations center, may be responsible for analyzing, assessing, and triaging cyberattacks, at which point an incident response team is activated. For most companies, this response begins at the C-level, where the CIO or CISO may assess the severity and recommend strategies to mitigate impacts on business objectives. From there, it is a cross-collaborative effort across cyber, information, operations, and business teams to implement monitoring and weigh in on real-time business impacts. The following steps are necessary for robust detection capabilities:

Develop cyberthreat awareness. Global threat intelligence and analysis enables situational awareness of potential threats, actual attacks, and best-practice mitigation techniques. Threat intelligence feeds from governmental agencies and private-sector vendors — such as FireEye, an industry leader in global threat intelligence reporting, and InfraGard, a public-private consortium sponsored by the FBI for threat intelligence sharing — are essential attack detection tools. Organizations should ingest threat information and orchestrate automatic triggers (enabled by AI and machine learning) for automatic data backup and recovery and targeted system isolation responses.

Invest in active monitoring protocols. Security information and event management software gives information security professionals a track record of the activities within their IT environments and provides insight into abnormal network activity, particularly that which could down systems or lose or corrupt data. Investing in such active monitoring protocols can be orchestrated by managed security offerings, through security-as-a-service options, or through cloud services that seek to make organizational data and systems assets undiscoverable by cyberattackers.

Act on threats early. Threat detection is most effective if acted upon fast, so create and enforce threat detection policies for employees and other organizational partners. Federal authorities like the FBI should be regarded not as a last resort but as trusted partners to determine the identity of attackers, reduce the likelihood of repeated attacks, and aid in more effective and timely responses and recovery.

Preserve and share information on attacks. From the earliest point possible in the intrusion or attempted breach, preserve relevant information, such as network web logs that can be forensically analyzed to ascertain cyberattacker techniques, tactics, and procedures. Share this data with a trusted noncommercial threat intelligence partner like the FBI to help foster a robust ecosystem of cyber resilience.

Phase 3: Response

How should the organization react to a threat or attack? Key objectives are to limit damage, improve recovery time, resume operations quickly, and help safeguard the organization from fiscal or reputational harm.

A variety of players may be involved in this step: The incident response team may carry out mitigation strategies, coordinated at the C-level, which in turn updates executive leadership on progress. Executive leadership and operations managers may keep an eye on social media outlets to gauge external stakeholder response and prepare communications related to HR and public relations (PR) for employees, customers, law enforcement, investors, and the press accordingly. Legal team members can help executive leadership determine possible legal implications and decide whether to involve law enforcement.

Response activities will fall into two basic categories:

Technical response activities. Because technical response activities will depend on the specific nature of the attack, it's impossible to cover all possible responses here. Common technical response activities may involve notification, escalation, interaction, or approval for steps to minimize the risk of disruption to operations and prevent the attack from reaching a crisis level. To contain a breach or limit damage, procedures may involve ensuring network segmentation, isolating affected systems, disconnecting all the links from the network, turning off computers to stop the threat from spreading, and employing effective backup systems when primary systems fail.

Business response activities. To ensure that cyber incident response initiatives are carried out promptly and properly, the organization should coordinate internal and external communication, carefully determining if, when, and how the breach will be publicized and communicated to stakeholders such as partners, customers, boards, legal teams, and the media. Other response activities may include ordering audits; overseeing regulatory compliance and data assurance; and

making investments to mitigate technical harm or to protect the brand, such as free credit-monitoring services or funds for customers to offset harm inflicted by a data breach.

Phase 4: Recovery

The recovery phase involves retrieving data, returning to normal operations (using alternative workplaces identified in the preparation step, if necessary), tracking activities and costs resulting from the incident, and fine-tuning future resilience plans based on lessons learned. Essential players include the CIO/CISO, to oversee recovery and forensic activities, report the incident if required, and document incident details for senior leadership. HR or PR personnel may inform internal or external stakeholders about the recovery process, the business impact, and the plan for resuming regular operations. Executive and operational managers may oversee the resumption of business operations, assess postattack business impacts or damage, file needed insurance claims, and offer feedback on the effectiveness of the plan itself. Primary recovery activities involve the following:

Data recovery. Reestablishing business operations may involve backing up, recovering, and restoring data corrupted by an attack. Cloud disaster recovery, primarily an infrastructure-as-a-service solution, backs up designated system data on a remote offsite cloud server. Ready access to cloud-based or offsite data storage is essential. Security experts may need to ascertain whether any data has been damaged or completely destroyed.

Documentation and analysis. Documenting and assessing the entire episode for lessons learned is essential for improving

preparation for subsequent attacks. The organization should analyze its response with questions such as the following:

- What happened and when? Was the incident found in a reasonable amount of time?
- Were the right personnel available to respond? How well did staff members and management perform in dealing with the incident? Were documented procedures followed?
- Did recovery and restoration happen as quickly as expected? Were backup files available and up to date?

Response assessment and adjustment. The organization's risk posture, as defined in the preparation phase, should be revisited — especially after a significant security incident — to determine whether previously established plans and investments provided the desired outcomes during the attack. Questions to consider include the following:

- Were any steps or actions taken that might have inhibited the recovery?
- What will staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

A four-phase cyber resilience plan that identifies clear roles and responsibilities, is carefully crafted to meet organizational needs, and is consistently updated to maintain data security can position an organization to face evolving cyberthreats while minimizing disruption, decreasing damage, and sustaining essential operations. Organizations must remember that cybersecurity is not the same as cyber resilience; should the

first fail, the second must prevail to ensure the organization's survival in an ever-evolving threat landscape.

Topics

Data & Analytics | Digital | Analytics & Strategy | IT Governance & Leadership | IT Strategy | Technology Implementation

Digital Resilience

Today, leaders across all business units must be able to answer a critical question: How secure are we? This series examines how managers can build digital resilience to compete in the new digital economy, where companies need to protect against not only cyberattacks but also technical debt and digital weak points within their infrastructure and teams.

See All Articles in This Series →

ABOUT THE AUTHORS

Chon Abraham is an associate professor of information systems at the College of William & Mary's Raymond A. Mason School of Business and a military reserve cyber officer who teaches and researches cyber resiliency and governance topics. Ronald R. Sims, the Floyd Dewey Gottwald Senior Professor of Business Administration at the Raymond A. Mason School of Business, teaches organizational behavior topics, including human resource management relative to cyber and information security. Tracy Gregorio (@tracygregorio) is president of G2 Ops, a solutions provider for cyber resiliency, cyber risk analysis, and model-based systems and security engineering. She served on the executive committee of the Commonwealth Cyber Initiative, representing industry in coastal Virginia.

TAGS: Cybersecurity, Data Security, Digital Strategy, Hacking, Resilience, Risk Management