DECEMBER 2013

How good is your cyberincident-response plan?

Many organizations must face a troubling fact: defending their digital perimeter is not enough. They should assume that successful cyberattacks will occur—and develop an effective plan to mitigate the impact.

Tucker Bailey, Josh Brandley, and James Kaplan

Cybercriminals are successfully targeting organizations of all sizes across all industry sectors. Recent analyst and media reports make clear that attacks are becoming increasingly sophisticated, more frequent, and their consequences more dire. One global company that suffered a large breach spent over $100 million on investigating the incident and on other direct remediation activities. But those costs were small compared with the subsequent multibillion-dollar loss in market capitalization, which was largely attributed to investors' loss of confidence in the company's ability to respond.

That's why it's not enough to focus, as many enterprises do, on defending the digital perimeter with cybertechnologies such as intrusion detection and data-loss prevention. When determined adversaries such as hacktivists and organized criminal syndicates set their minds on finding a way inside, every organization with valuable digitized information is at risk of having its perimeter breached and its critical assets compromised.

Indeed, most organizations today would do well to expand their efforts to mitigate the consequences of inevitable breaches, which likely affect infrastructure systems and compromise key data such as personally identifiable information. An incident-response (IR) plan guides the response to such breaches. The primary objective of an IR plan is to manage a cybersecurity event or incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs. For example, the US Department of Defense, which spends upward of $3 billion a year on cybersecurity, operates

under the assumption that its unclassified networks may be penetrated and therefore concentrates on maintaining operations and minimizing damages from a breach.

Shortfalls of most incident-response plans

The common focus on defending the digital perimeter and assuming the walls will hold doesn't mean that large organizations don't have an IR plan. Most do have one, and some leading organizations invest serious time, money, and effort in these plans.

However, our experience suggests that most organizations don't truly operationalize their IR plans, which are ineffective due to poor design or implementation, or both. We've observed several critical shortfalls.

First, the documentation of how to act in the event of a breach may be out of date. The documentation is often also generic and not useful for guiding specific activities during a crisis.

A second problem is that plans, especially in global organizations, are not integrated across business units. Individual units create locally optimized response plans, which can be useful for dealing with targeted attacks but are not effective for managing an incident across the whole business. Developing individual plans in silos also inhibits sharing relevant knowledge and best practices.

Third, decision making in a response scenario is often based on tribal knowledge and existing relationships. This is due to poorly codified plans and responses that are not thought through. When asked about incident response, many organizations will identify one or two "go to" people who have the institutional knowledge to guide the organization. This may result in a single point of failure when the resident expert is not available or does not have the capacity to identify and manage all the moving parts of a complex breach scenario.

Fortunately, these shortfalls can be addressed by an effective IR plan based on a framework for risk identification, decision making, and escalation paths across the whole business.

Benefits of effective incident-response plans

In our experience working with global institutions, an effective incident-response plan offers five important advantages that can significantly mitigate the downside of a breach.

Improved decision making. By establishing who will have decision rights if and when an incident occurs, an organization can quickly respond to a breach at the appropriate scale or escalation level based on the value at stake. After the security team at a major insurance company confirmed that malicious code had infected a core application, management quickly decided to shut down complete network access. Managers understood that the risk of continued data loss from this specific application outweighed the associated loss of revenue resulting from downtime. Furthermore, having developed standard procedures for isolating strategic segments of their network, the technology teams followed step-by-step instructions to efficiently quarantine the application.

The type of data being compromised will determine response efforts . . . clearly defining the actions to be taken for each type of data that has been compromised will largely determine the success of the overall response.

Internal coordination. While incident response has historically been viewed as an IT department issue, effective planning must incorporate coordination across all business functions, for example, corporate communications, regulatory affairs, legal, compliance and audit, and business operations. Coordination, combined with easily accessible documentation of IR plans, ensures that all levels of an organization can react with greater agility during an incident. In the early stages of a crisis at a large retail bank, representatives in the customer-service call center worked from preapproved scripts to handle calls from customers inquiring about the nature of a data breach. At the same time, executives and security teams were able to focus on investigating the extent of data loss without the distraction of developing communications in real time.

External coordination. Effective IR plans should help maintain relationships with important third parties, such as law-enforcement agencies and breach-remediation and forensics experts.[1] Failure to maintain these relationships can have catastrophic consequences. During a recent war-game exercise, the security team at an insurance company attempted to engage a third-party cyberincident-remediation firm for emergency assistance only to discover that the service agreement with the firm had expired. As a result, the remediation firm could only commit to providing services within 72 hours. Had this been a real-life incident, the institution would have been without critical remediation services for more than three days.

Unity of effort. Efficient IR plans establish clear roles and responsibilities across the organization. One institution learned how important this is the hard way when it delayed releasing an important statement to the media while executives debated the desired messaging. The delay was due to unclear responsibilities that slowed down the executive group as its members defined a list of external stakeholders, tried to assemble a meeting with internal stakeholders, and debated numerous issues. Many of these issues could have been resolved in advance, for instance, assessing the regulatory impact of the loss of specific data.

Damage limitation. Strong response plans also help ensure that minor events do not escalate into major incidents. One individual on an organization's security team was following event-response instructions, which called for routinely monitoring any malware that falls below typical incident thresholds, when he noticed that malicious code was attempting to access highly strategic data assets. In this case, the company averted an incident altogether.

[1]Third-party cybersecurity forensic and remediation experts are often engaged directly after a major incident occurs to provide critical assistance—for example, expediting breach containment to mitigate exposure, obtaining evidence for legal requirements, analyzing attack patterns to understand vulnerabilities and identify potential adversaries, and restoring services.

Components of an incident-response plan

An incident-response plan usually has six major parts.

Incident taxonomy. Organizations typically follow the incident topology defined by the National Institute of Standards and Technology, which defines incident categories broadly as unauthorized access, malicious code, denial of service, and inappropriate usage. Adopting this common taxonomy enables institutions to more easily share security intelligence with one another as well as standardize their own internal communications.

Data-classification frameworks. Leading institutions develop their own response categories based on the value of the various types of data. In other words, the type of data being compromised will determine response efforts and activities. For example, a company might have one set of response processes for confidential customer data and an entirely different set of processes for a loss of critical intellectual property. The stakeholders are different in each case, and the resources a company chooses to allocate to mitigation will vary. Often overlooked, this is the most critical element of an IR plan. The compromise of different types of information results in a wide array of business impacts. Clearly defining the actions to be taken for each type of data that has been compromised will largely determine the success of the overall response.

Performance objectives. IR plans should lay out response objectives for each data type and each incident or event type. For example, the performance objective for responding to a loss of customer data could be to identify the number of customers affected and the extent of data loss within four hours. Within eight hours, the security team should have a good idea of who might be responsible for the theft and an estimate of the business impact.

Definition of response-team operating models. IR plans should specify team structures, individual roles and responsibilities, escalation processes, and war-room protocols (see "The role of the war room"). The operating models tie back to the data-classification framework. For example, it is important to specify exactly when to involve executive leadership in the decision processes, when to activate a war room, and at what threshold executives should take decisive measures, such as isolating sections of the network or shutting down core applications. Operating models also document decision rights, for instance, who authorizes contacting law enforcement.

The role of the war room

The war room is an essential tool in incident response. Borrowed from a military construct, a war room is a physical location with supporting infrastructure where preassigned decision makers gather to share with one another what they know, speed up decision making, and ensure a unity of effort while responding to an incident.

Whether starting anew or building on an existing effort, creating an effective incident-response program requires substantial work. We recommend assigning dedicated project resources and treating the effort as a formal initiative, then taking a four-step approach.

Identification and remediation of failure modes. Continuous improvement of an IR plan is driven by the ongoing identification of potential failure modes—that is, the ways in which the response could break down—and then making the necessary enhancements.

Key tools for use during response. The IR plan is a document that may include as many as eight sections (exhibit). The most useful plans include "artifacts," or procedural guides, such as playbook charters and checklists for containment, eradication, and recovery, as well as guidelines for documenting the response in governance, risk, and compliance applications. For each data type and incident type, the playbook charter outlines the objectives and team operating models. Checklists provide step-by-step instructions and assign roles and responsibilities to specific individuals.

Building an incident-response program

Whether starting anew or building on an existing effort, creating an effective IR program requires substantial work. We recommend assigning dedicated project resources and treating the effort as a formal initiative (see sidebar, "Nine guiding principles for incident response"). The team should follow a four-step approach.

Understand the current environment

First, analyze business-continuity and disaster-recovery plans to understand current response protocols. Use these documents as a framework to develop an incident-response-plan template. Build a baseline understanding by interviewing key individuals, usually 20 to 30, across the organization, including, for example, sales, marketing, operations, IT, security, regulatory affairs, and communications. Use these interviews to identify, document, and categorize information assets, vulnerabilities, and potential threats. The team should also create process flows of current methods to identify incidents, escalate issues, and respond both internally and externally.

Once a basic understanding of the environment is achieved, organizations should assess the effectiveness of previous response efforts. For each previous incident, they should identify any problems that arose with the response, diagnose potential causes for failure, and create an exhaustive list of potential failure modes.

Identify the most critical information assets

Organizations need to identify the information assets most critical to business operations as a

basis for developing the data-specific actions to be taken. These information assets range from customer data to M&A deal terms to critical intellectual property, and identifying them will require input from business owners across the enterprise. For each asset, there should be a clear analysis of the cyberrisks involved, the business impact if the asset is compromised, and the response required.

Create the plan and supporting tools

Early in the development process, companies should involve the people who will own and maintain IR documentation. This will help the program transition from a special IR initiative to business-as-usual practices. It is also important to jointly develop the key components, for example, an incident taxonomy and data-classification frameworks.

Exhibit
An incident-response plan presents the key tools to use after a cyberattack.

Section	Description
1 **Introduction**	• Purpose of response plan, initiation guidelines, and how to use the plan • Plan contents and scope of use
2 **How to use the incident-response plan**	• Explanation of the different levels of incident response and escalation points • Description of how to use the document for each part of the process
3 **Event handling**	• Event types, guidelines for categorization, and suggested actions
4 **Incident topology**	• Incident types • Affected information assets
5 **Incident-response team and war room**	• Team responsible for incident response
6 **Setup of the war room**	• Structure of working groups that are part of the war-room/critical-decision rights and responsibilities
7 **Response plans**	• Plans for each incident type • Plans for each information-asset type • Checklists of key processes, actions, and notifications to be triggered in the event of a cyberattack, categorized by both incident and asset type
8 **Post-incident procedures**	• Post-incident procedures and documentation of post-incident learning and codification: — Documenting incident details and response actions — Collecting lessons learned from incident response — Updating plan to improve future responses

Nine guiding principles for incident response

By working with many large global institutions on this topic, we have developed a list of guiding principles that should be reflected in any incident-response plan:

1. Assign an executive to have ongoing responsibility for the IR plan and for integrating IR efforts across business units and geographies.
2. Develop a taxonomy of risks, expected threats, and potential failure modes and refresh them continually based on changes in the environment.
3. Develop quick-response guides for likely scenarios and make them easily accessible.
4. Establish processes for making major decisions, for instance, when to isolate compromised areas of the network and how to do so quickly.
5. Maintain relationships with key external stakeholders, such as law enforcement (for example, in the United States, the Federal Bureau of Investigation).
6. Maintain service-level agreements and relationships with external breach-remediation providers and experts.
7. Ensure that documentation of IR plans is available to the entire organization and is routinely refreshed.
8. Ensure that all personnel understand their roles and responsibilities in the event of a cyberattack.
9. Identify the individuals who are critical to incident response and ensure that they have backup and that a succession plan is in place.

During the design phase, it's important to share artifacts and frameworks with relevant parties early and often. For example, once the team creates the overall outline and specific structure of the IR documents, it should share the draft work with the security team. This not only solicits valuable feedback from an eventual end user but also generates excitement for the tool.

Integrate planning into business processes

Having a robust incident-response plan on paper is critical, but all too often organizations overlook the fact that developing a real IR capability requires moving the plan from a static document to being embedded in the fabric of the organization.

To successfully implement the IR program, companies should first make sure that the tools are accessible, for example, by publishing IR documentation in print, digital form, and on an internal Web-based platform, and distributing it widely to relevant parts of the organization.

Next, it's crucial that companies carry out a comprehensive change-management, commu-

nications, and training program to increase awareness of the new IR processes.

Finally, successful incident response requires developing "muscle memory" through regular training and practice. Companies should build detailed incident scenarios and incorporate into the annual development plan the opportunity for key decision makers to use the IR plan to navigate simulated breaches in war-game exercises that can be conducted around a table without affecting real systems.

• • •

An effective incident-response plan ultimately relies on executive sponsorship. Given the impact of recent cyberbreaches, we expect IR to move higher on the executive agenda. Putting the development of a robust IR plan on the fast track is imperative for

companies because external stakeholders are losing patience. When a successful cyberattack occurs and the scale and impact of the breach comes to light, the first question customers, shareholders, and regulators will ask is, "What did this institution do to prepare?"

Tucker Bailey is an associate principal in McKinsey's Washington, DC, office, **Josh Brandley** is a consultant in the Toronto office, and **James Kaplan** is a principal in the New York office.