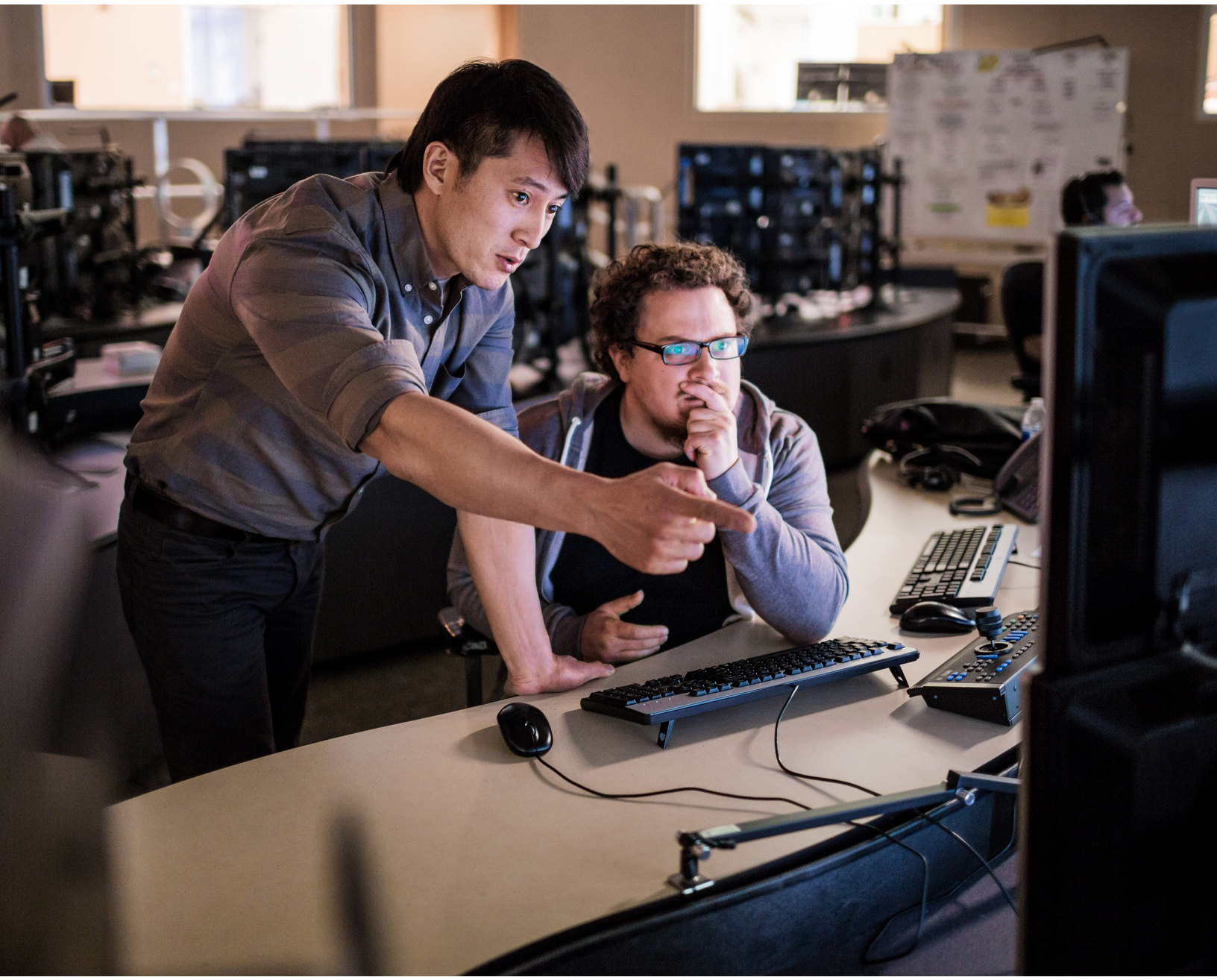
# Data Breaches: Protect Your Organization with an Incident Response Program



## What You Will Learn

The ability to respond effectively to data breaches is critical to every organization. You need to establish a process that will ultimately help you:

- Maintain business continuity
- Protect your reputation and employee morale
- Avoid fines, legal fees, and remediation costs

This white paper is designed to help chief information security officers and other managers quickly establish an incident response program.

## The Need for an Incident Response Team

All organizations depend, at least in part, on their data to carry out day-to-day operations. Governments around the world regulate the handling of various types of data, especially personally identifiable information. Yet new, high-profile data breaches are reported every week, and the costs of those breaches continue to rise.

Here are a few statistics to quantify the impact of security incidents:

- Sixty percent of the time, attackers are able to compromise an organization within minutes.[1]
- The current industry estimate for the time to detection (TTD) of security incidents is 100 to 200 days.[2]
- On average, 3 percent of security incidents result in a confirmed data breach.[3]
- The average global cost of a data breach per lost or stolen record is $154.[4]
- Costs associated with lost business as the result of a breach average $1.57 million.[5]
- Brand value could decline more than 31 percent depending on the type of data breach.[6]
- Even five years ago, the average loss in the value of the brand ranged from $184 million to more than $332 million.[7]

Thankfully, the core elements of an incident response program are straightforward to understand and quick to establish. In this article we'll outline what the critical processes and major roles are within an incident response program.

The language around breaches can be confusing. We use the definitions used by Verizon in its Data Breach Investigations Report.

**Security incident:** Any event that compromises the confidentiality, integrity, or availability of an information asset.

**Data breach:** An incident that results in the confirmed disclosure of data (not just exposure) to an unauthorized party.

1 Verizon's 2015 Data Breach Investigations Report, page 6
2 Cisco's 2016 Annual Security Report, page 6
3 Verizon's 2015 Data Breach Investigations Report, page 3
4 Ponemon's 2015 Cost of Data Breach study, page 2
5 Ibid., page 3
6 Ponemon's 2011 Reputation Impact of a Data Breach report, page 1
7 Ibid., page 1

## Critical Elements of an Incident Response Program

A structured response assures consistent research and action. Responses to security incidents that may involve data loss typically follow a similar workflow, such as the following:

- Research the background details of the incident
- Consult with incident response advisory resources
- Develop and implement a resolution plan
- Follow up to identify improvements

Of course an incident needs to be discovered before anyone is aware a response is needed. Let's start there.

## Detection of Events

New incidents come from multiple sources:

- Internal users
- Internal monitoring tools
- Internal risk-assessment tools
- External customer
- External entities
- Social media

Perhaps the best place to start is to make sure that your organization, and particularly the senior executives, adequately understand what the security risks are and what to look for. Awareness is essential to detection. It's easy to overlook an anomaly when you believe everything is safe.

Automation is your second line of defense. Monitoring tools, including analytics of anomalous traffic or user behavior, can be invaluable.

Finally, keep an eye out on social media. Bad news travels fast. You don't want to be the last to know.

## Triage and Containment

When a security incident occurs, an incident commander assembles a team and leads the efforts to stop, contain, and control the incident and data loss.

The triage process begins as soon as a data incident is detected. The process involves research to understand the situation and to determine which actions need to be taken and when. Information that should be gathered includes answers to the following questions:

- What is the nature of the event?
- Is the event ongoing?
- Is the event known or likely to be known to others outside the organization?
- Which systems, applications, products, or services have been affected?
- Is customer, personal, or other sensitive data actually or potentially exposed or compromised?

Other aspects that should be noted include:

- Interruptions of service for critical or regulated systems
- Legal obligations
- Business continuity issues
- Press or other public statements
- Scope of the compromised data set
- Employee or third-party involvement

"Containment" refers to all efforts to stop, contain, and control the incident and data loss. These efforts need to be taken as soon as practically possible to prevent further data compromise, with measures also taken to prevent the loss of evidence. Major containment steps include:

- **Convening the team:** The initial team should include members of the legal and communications departments, as well as a technology focal point designated by the chief information security officer. Together they will identify other personnel that need to be engaged.
- **Eradicating the cause:** The cause of the incident should be eradicated as soon as reasonably possible without further jeopardizing the security or integrity of systems or data and without destroying important evidence.
- **Conducting computer forensics:** Depending on the nature of the incident and the type of information compromised, you may need to consult an external computer forensics entity to determine the source of the breach and to support your investigations.
- **Preserving the evidence:** Take all necessary steps to preserve evidence related to the incident, including maintaining the chain of custody.

## Response Plans

As soon as the necessary steps have been taken to contain and control an incident, document all the actions taken and produce a set of appropriate response plans. Your plans may include:

- Actions to remediate and recover from harm
- Notifications, if any are required
- Communications, both internal and external
- Customer management

It is important to determine the cause, nature, and scope of the incident before putting the plans together.

After the team has built a comprehensive response plan, it should implement all planned actions with the understanding that the situation may be fluid and that flexibility will be required. You should provide frequent updates to the team and management until all the actions are completed, appropriately managing expectations as clarity increases and conditions evolve.

## Remediation

After completing the main activities outlined in the response plan, review the status of the incident and summarize the lessons learned so that postincident actions can improve future data security practices.

It makes sense to intentionally select a risk posture when it comes to postincident action. In some cases, many actions will need to be undertaken, not all of which will provide the same levels of improvement, equivalent increases in security, or relative returns on investment. We'll cover risk postures and how to select them in a future paper.

## Major Roles within an Incident Response Program

The central role in any incident response program is the incident commander, who leads the virtual response team through the organization's response to data incidents.
The incident commander's responsibilities include:

- Overseeing response efforts for all critical incidents
- Reviewing and assessing the incident priority, status, and exit criteria
- Assembling and leading the incident response team through the response process
- Ensuring that the correct resources are engaged and incidents are receiving the appropriate level of commitment
- Serving as the escalation and communication liaison between the incident response team and the Data Protection Program(DPP) director, as well as other relevant stakeholders
- Defining the documentation to be developed or provided through an incident's life cycle (not only what, but also why)
- Conducting postincident reviews for lessons learned
- Developing recommendations to prevent or limit the occurrence of future incidents
- Overseeing and providing guidance and direction to the incident response program

## DPP Incident Response Team

At Cisco, our Incident Response Team consists of personnel from multiple departments. Members provide guidance and accept resolution responsibilities based on their business function.

The engagement of specific response teams by the incident commander varies depending on the data incident. However, all Incident Response Teams are included in incident communications.

Incident Response Team member organizations and their functions include:

- Business Continuity: strategic guidance and cyberinsurance
- Business-Critical Communications: internal and external messaging strategy and content
- Network Security Incident Response
- Government Affairs: international government interaction
- Human Resources (HR): responsibility for Cisco employees
- InfoSec: data analysis
- IT: Cisco tool and application oversight
- Legal: regulatory and strategy guidance
- Sales: relationship management with customers
- Services: support services for customers

Department executives are expected to be responsible for:

- Providing oversight for the incident program to help ensure overall preparedness to address incidents
- Assigning dedicated resources to assist in the planning and resolution
- Monitoring and reporting the impact of incidents on their functions

## Setting Up an Incident Response Program

The following steps will guide you through quickly establishing an incident response program:

1. Identify an incident response leader who has good knowledge of your business and who is an effective and responsible problem solver.
2. Assemble and empower a team of concerned individuals, with clearly defined roles and responsibilities representing the major roles listed above.
3. Draft your incident response process. There's no need to be fancy or to reinvent the wheel. Just make sure it works for your organization's culture.
4. Connect people and tools with the needed capabilities from around your organization. Chances are, much of what you need is already around somewhere. Suggest what to look for and where to look.
5. Understand the most significant capability gaps relative to your draft incident response process and build a plan to address those gaps. Start with a minimum viable process, and then enhance it over time.

Read the blog

## Conclusion

The operation of your organization depends, at least in part, on its data.

You can avoid fines and remediation costs, protect your organization's reputation and employee morale, and maintain business continuity by building a capability to detect and respond to incidents effectively.

The simplicity of the incident response process can be misleading. We recommend tabletop exercises as an important step in pressure-testing your program.

## For More Information

To learn more, see:

- Cisco incident response infographic
- Cisco 2016 Annual Security Report
- Ponemon's 2011 Reputation Impact of a Data Breach report
- Ponemon's 2015 Cost of Data Breach study
- Verizon's 2015 Data Breach Investigations Report



C11-737237-00 06/16