Incident Response

Proactive Incident Management

Sean Curran
Director

Powerful Insights. Proven Delivery.
Agenda

Incident Response Overview  3
Drivers for Incident Response  5
Incident Response Approach  11
Proactive Incident Response  17
Incident Response Overview

An incident is a real or suspected adverse event that could or did effect the confidentiality, integrity or availability of an organization's information assets and/or violates the organization's Information Security policies. The impact of an incident may result in a financial or reputational loss.

Information assets include:

- Corporate sensitive data,
- Personally Identifiable Information (PII),
- Protected Health Information (PHI),
- Payment Card data,
- Computer Security systems,
- Applications,
- Networks.
Incident Triad

The CIA (Confidentiality, Integrity, and Availability) triad of information security is a benchmark model used to evaluate the risk of an Incident.

**Confidentiality**
- The component ensures privacy and means that data are only available to the parties that require access to the data or parties that are trusted.
- Ensuring confidentiality means that information is organized in terms of who ought to have access as well as its sensitivity.
- A breach of confidentiality may take place through different means, for instance hacking or social engineering.

**Integrity**
- Data integrity refers to the certainty that the data are not tampered with during or after submission.
- It is the certainty that the data will not be modified or destroyed by unauthorized parties.
- This means there are two points during the transmission process during which the integrity could be compromised: during the upload or transmission of data; during the storage of the document in the database or collection.

**Availability**
- This means that the information is available when it is needed.
- In order for a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels.
- The most available systems are accessible at all times and have safeguards against power outages, natural disasters, hardware failures and systems upgrades.
Drivers for Incident Response
Drivers for Incident Response

Incidents are organizational specific. The organization needs to define what they consider an incident. Examples include:

- An unexpected system outage
- A virus infects hundreds of workstations and effectively shuts down the network;
- An attacker who gains remote administrator-level access to an e-mail server;
- A user who downloads content from the web that is in breach of the Information Security policy;
- A user who defaces another organization's public web site;
- Unauthorized access is gained to a critical information system;
- Unauthorized network access from the Internet;
- A distributed denial of service attack against an organization's public web server;
- Unauthorized access using dial-in or wireless remote access;
- Unauthorized changes to live systems.
Large Data Breaches of the Decade

CardSystems Solutions: 40 million credit card accounts exposed. CSS, one of the top payment processors for Visa, MasterCard, American Express is ultimately forced into acquisition.

AOL: Data on more than 20 million web inquiries, from more than 650,000 users, including shopping and banking data were posted publicly on a web site.

Monster.com: Confidential information of 1.3 million job seekers stolen and used in a phishing scam.

Wyndham Hotels: were sued by the US Federal Government after sensitive customer data, including credit card numbers and personal information, allegedly were stolen three times in less than two years.

2005

2006

2007

2008

“Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated.”

— The IIA Research Foundation

2009

2010

2011

2013

Target and Neiman Marcus Credit and Debit Card data breach!!

Sony’s PlayStation Network: 77 million PlayStation Network accounts hacked; Sony is said to have lost millions while the site was down for a month.

VeriSign: Undisclosed information stolen

Google/other Silicon Valley companies: Stolen intellectual property

Source: CNN, NBC, CSO Online
Data Breaches Statistics

**Number of Breaches in 2013**

219

**Number of Identities Exposed in 2013**

501,516,310

**Overview:**

- Targeted attacks increased in January, 2014 reaching their highest levels since August, 2013.
- Small companies of 250 employees or less were targeted in 39% of attacks through organizations with 2500+ employees were targeted more often, based on first attacks.
- The `.exe file` type was the most common attachment, making up 24.7% of email-based targeted attacks that included file attachments.

**Source:** Symantec
Data Breach Statistics (cont…)

Who’s Perpetrating Breaches?

- 92% Perpetrated by outsiders
- 14% Committed by insiders
- 1% Implicated business partners
- 7% Involved multiple parties
- 19% Attributed to state-affiliated actors

How Do Breaches Occur?

- 52% Hacking
- 76% Network intrusions
- 40% Malware
- 35% Physical attacks
- 29% Social tactics
- 13% Privilege misuse and abuse

The largest data breach that was reported in January, 2014 resulted in the exposure of 105.8 million identities.

In the last 12 months (February, 2013 – January, 2014), more than 500 million identities have been exposed.

A data breach in November, 2013 is now estimated to have exposed 110 million identities.

Source: Symantec, Verizon 2013 Report
The attack can be disrupted at any point in the kill chain. Ideally, a company will have controls at each point to create a defense in depth strategy. “Cyber kill chain” model shows, cyber attacks can and do incorporate a broad range of malevolent actions, from spear phishing and espionage to malware and data exfiltration that may persist undetected for an indefinite period.
Incident Response Approach
Incident Response Approach

In general a Incident Response approach:

- Provides a single point of contact for reporting problems.
- Identifies and analyses what has happened including the impact and the threat.
- Researches solutions and mitigation strategies.
- Shares response options, information, and lessons learnt.

An Incident Response goal is to:

- Minimise the impact of an incident to a company and allow it to get back to work as quickly as possible.
- Be a focal point for preventing, receiving and responding to incidents.

“To ensure successful operation, an Incident Management approach must have the ability to adapt to changing needs of the environment and exhibit the flexibility to deal with the unexpected. In addition, a Incident Management approach must simultaneously address funding issues and organisational changes that can affect its ability to either adapt to the needs or provide the service itself.”
# The First 24 Hours Checklist

- **Record the date and time** when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.

- **Alert and activate everyone** on the response team, including external resources, to begin executing your preparedness plan.

- **Secure the premises** around the area where the data breach occurred to help preserve evidence.

- **Stop additional data loss**. Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.

- **Document everything** known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.

- **Interview those involved** in discovering the breach and anyone else who may know about it. Document your investigation.

- **Review protocols** regarding disseminating information about the breach for everyone involved in this early stage.

- **Assess priorities and risks** based on what you know about the breach.

- **Bring in your forensics firm** to begin an in-depth investigation.

- **Notify law enforcement**, if needed, after consulting with legal counsel and upper management.
Data Breach Incident Response

1. Fix the Issue that Caused the Breach
   - Rely on your forensics team to delete hacker tools.
   - Determine if you have other security gaps or risks and address them.
   - Put clean machines online in place of affected ones.
   - Ensure the same type of breach cannot happen again.
   - Document when and how the breach was contained.

2. Continue Working with Forensics
   - Determine if any countermeasures, such as encryption, were enabled when the compromise occurred.
   - Analyze backup, preserved or reconstructed data sources.
   - Ascertain the number of suspected people affected and type of information compromised.
   - Begin to align compromised data with customer names and addresses for notification.
Data Breach Incident Response

3 Identify Legal Obligations

- Revisit state and federal regulations governing your industry and the type of data lost.
- Determine all entities that need to be notified, i.e. customers, employees, the media, government agencies, regulation boards, etc.
- Ensure all notifications occur within any mandated timeframes.

4 Report to Upper Management

- Compile daily breach reports for upper management.
- The first report should include all of the facts about the breach as well as the steps and resources needed to resolve it.
- Create a high-level overview of priorities and progress, as well as problems and risks.

5 Identify Conflicting Initiatives

- Make the response team and executives aware of any upcoming business initiatives that may interfere or clash with response efforts.
- Decide whether to postpone these efforts and for how long in order to focus on the breach.
Data Breach Incident Response

6 Alert Your Data Breach Resolution Vendor

• Contact your pre-selected vendor to choose business services for your company and protection products for individuals affected in the breach.
• Determine how many activation codes you will need for the protection products based on the number of affected individuals.
• Draft and sign a data breach resolution agreement if you do not have a pre-breach agreement in place.
• Engage your vendor to handle notifications (learn more in the next section: Breach Notification) and set up a call center so affected individuals have access to customer service representatives trained on the breach.
• Work closely with your account manager to review incident reporting and metrics.

7 Keep Your Response Efforts on Track

Resolving a data breach requires a coordinated effort between your response team members, executives, external resources, law enforcement, forensic firm and data breach resolution vendor. Staying organized and documenting every step and decision should be a top priority. Act quickly to minimize the damage but don’t lose sight of your priorities or of the needs of affected individuals.
Proactive Incident Response
What Should an Organization Do Today

Six steps that an organization can take, to significantly reduce the risk of a data breach:

1. **Stop Incursion By Targeted Attacks**
   - The top four means of hacker incursion into a company’s network are through exploiting system vulnerabilities, default password violations, SQL injections, and targeted malware attacks.
   - To prevent incursions, it is necessary to shut down each of these avenues into the organization’s information assets.
   - Core systems protection, IT compliance controls assessment automation, and endpoint management, in addition to endpoint, Web, and messaging security solutions, should be combined to stop targeted attacks.

2. **Identify Threats by Correlating Real-time Alerts with Global Intelligence**
   - To help identify and respond to the threat of a targeted attack, security information and event management systems can flag suspicious network activity for investigation.
   - The value of such real-time alerts is much greater when the information they provide can be correlated in real time with current research and analysis of the worldwide threat environment.

Source: Symantec
What Should an Organization Do Today

3 Proactively Protect Information

- In today’s connected world, it is no longer enough to defend the perimeter. The organization must accurately identify and proactively protect its most sensitive information wherever it is stored, sent, or used.
- By enforcing unified data protection policies across servers, networks, and endpoints throughout the enterprise, the organization can progressively reduce the risk of a data breach.

4 Automate Security through IT Compliance Controls

- To prevent a data breach caused by a hacker or a well-meaning or malicious insider, organizations must start by developing and enforcing IT policies across their networks and data protection systems.
- By assessing the effectiveness of the procedural and technical controls in place and automating regular checks on technical controls such as password settings, server and firewall configurations, and patch management, organizations can reduce the risk of exposing sensitive information.

Source: Symantec
What Should an Organization Do Today

5 Prevent Data Exfiltration

• In the event a hacker incursion is successful, it is still possible to prevent a data breach by using network software to detect and block the exfiltration of confidential data.
• Well-meaning insider breaches that are caused by broken business processes can likewise be identified and stopped.
• Data loss prevention and security event management solutions can combine to prevent data breaches during the outbound transmission phase.

6 Integrate Prevention and Response Strategies into Security Operations

• In order to prevent data breaches, it is essential to have a breach prevention and response plan that is integrated into the day-to-day operations of the security team.
• The use of technology to monitor and protect information should enable the security team to continuously improve their strategy and progressively reduce risk, based on a constantly expanding knowledge of threats and vulnerabilities.

Source: Symantec
Sean Curran

Director
Chicago, IL

Phone: +1.312.476.6345
sean.curran@protiviti.com

Powerful Insights. Proven Delivery.™
Powerful Insights.
Proven Delivery.