Automate Response

Congratulations on selecting IncidentResponse.com to retrieve your custom incident response playbook guide. This guide has been created especially for you for use in within your security response team. We hope you find it valuable and ask that you share it with the rest of your organization so you can collectively be successful in managing incidents and reducing risk throughout the business.

Your playbook overview - “Data Theft”

Incident Response: A Top Priority in Security Management Programs

In the April 2014, U.S. Government Accountability Office reported (GAO-14-354) it’s noted that “major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information).” The GAO projects that these agencies did not completely document actions taken in response to detected incidents. While the agencies identified the scope of an incident, they frequently did not demonstrate that they had determined the impact of an incident, nor did they consistently demonstrate how they had handled other key activities, such as whether preventive actions to prevent the reoccurrence of an incident were taken. The GAO notes, “without complete policies, plans, and procedures, along with appropriate oversight of response activities, agencies face reduced assurance that they can effectively respond to cyber incidents.”

Did you know?

1. In 2014, incidents increased by 78% since 2013.
2. 1,023,108,627 records were breached in 2014.
3. 54% of the breaches consisted of Identity Theft.
4. $3.5 million is the average cost of a breach for a company.
5. Companies experience an average of 10 unauthorized access incidents per month.
6. Malicious insiders and criminal attacks are the top causes for breaches.

1. Source: Gemalto - Breach Level Index
2. Source: Ponemon 2014 Cost of a Data Breach
3. Source: GAO-14-354, p.2
What is an incident response playbook? According to NIST Special Publication 800-61, an incident response process contains four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Descriptions for each are included below:

**Prepare**
The initial phase where organizations will perform preparatory measures to ensure that they can respond effectively to incidents if and when they are uncovered.

**Detect & Analyze**
The second phase where organizations should strive to detect and validate incidents rapidly because infections can spread through an organization within a matter of minutes. Early detection can help an organization minimize the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organization sustains as a result of the incident.

**Contain, Eradicate & Recover**
The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organization to decide which methods of containment to employ early in the response. Organizations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organization.

**Post-Incident Handling**
Because the handling of malware incidents can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring.

---

**Data Theft**
You've selected the "Data Theft" playbook. On the pages that follow, you will find your incident response playbook details broken down by the NIST incident handling categories.

To view your playbook online, visit [https://incidentresponse.com/playbooks/data-theft](https://incidentresponse.com/playbooks/data-theft)
Detect - Data Theft

- Emails returned as Undeliverable due to size limitations
- Identification or publication of proprietary information outside the organization
- Notification of extortion in order to recover stolen data
- Large data dumps of databases, network shares or other computer systems
- Local disk or network shares that are near full capacity
- Work performed outside of normal business hours
- Reporting of large emails being sent by a single user
- Reports of removable and/or mobile devices being used to copy data
- Standard
  - Define Threat Indicators
  - Categorize Incident
  - Request Packet Capture
  - Conduct Scans
- Custom
  - Custom Indicators
Compliance regulations have been violated
Stolen data damaging to business operations or brand of the organization
External user PII or other protected information has been stolen
Internal user PII or other protected information has been stolen
PII or other protected information has been compromised
Customers are affected by this incident
Products/services are affected by this attack
Customers are affected by this incident
External user PII or other protected information has been stolen
Public or personnel safety affected
Ability to control/record/measure/track any significant amounts of inventory/products/cash/revenue is lost
There is indication of who performed the data theft
There is internal knowledge of this incident
Identify worst-case business impact if unable to mitigate this attack
Identify business operations that may be affected and identify any alternate courses
There is indication of who performed the data theft
Identify additional technical implications of the Data Theft
Identify business implications of the Data Theft
Identify worst-case business impact if unable to mitigate this attack
There is internal knowledge of this incident
Determine risk of the stolen data being released to the public
Determine Patch Methods
Log Collection
Evidence Collection
Data Capture
Analysis
Next Step
Prev Step
Define Risk Factors
Custom Factors
Custom
Standard
ANALYZE - DATA THEFT
Identify the system(s) that have been affected
- Servers
- Desktop
- Laptop
- Mobile
- VM
- LDAP Directory

Identify user credentials compromised or at risk

Identify method used to steal data

Identify systems used to steal data

Identify any source attribution collected

Identify lateral movement of compromised users throughout enterprise

Identify the tools used to detect the attack
- SIEM
- IDS
- Firewall
- Scanners
- Antivirus
- Removable Device Monitors
Triage & Confirm Incident Report

- Request System Patch
- Test Code
- Contain malicious Code Sample

Communications
- Direct Phone Call
- Conference Call
- In-Person Meeting
- Intranet Meeting
- Mobile Messaging
- Internet Meeting

Eradicate Malware
- Add/Change/Remove Affected System/Site/Network
- Perform data forensics
- Determine method of removing data from the organizations enterprise network

Monitor network traffic for ongoing theft
- Create alert signatures for suspected data exfiltration
- Prepare to temporarily scan or block all outbound data more than ___ Mb in size
- Implement device control monitoring and control systems
Recover Systems

1. Reimage
2. IDS/IPS & Firewall Updates
3. Identify ways to mitigate further removal of data

Incident Remediation

1. Wipe & Baseline System
2. Scan host with updated Signature
3. Scan File Share with updated Signature
4. Remove Vulnerabilities & Update Routers
5. Coordinate AV updates to be pushed upon release from AV Vendor
POST-INCIDENT - DATA THEFT

Incident Review
- Electronic Personal Health Information (e PHI) Compromised?
- Sensitive Government Information Compromised?

Lessons Uncovered
- Discovery Meeting
- Policy Updates Defined
- Process Updates Defined
- Configuration Updates Defined

Lessons Applied
- Policies Implemented
- Process Changes Implemented
- Configurations Applied

Response Workflow Updated

END
Proactive Response
An automated playbook helps security teams optimize for efficiency and productivity. Your security team has the ability to analyze, detect and prioritize when all pertinent data and multiple security tools are integrated into one system. With one-screen visibility you can identify anomalies, assign tasks, access reporting and communicate across multiple departments effectively for quick responses.

Quick Containment
Time and speed are crucial in assessing the environment and risk in the context of your business. Playbooks give a complete view of the necessary tasks to capture the data needed to support proper recovery and forensics. The efficiency a playbook brings to a security team allows for quick responses to finding the source of the attack, following lateral movement across the organization and taking the proper steps mitigate damage.

Effective Remediation
Organization and automation are key benefits that result in effective remediation. Automated playbooks help to organize security processes, mitigation plans and smooth communication between multiple departments. By optimizing data collection, analysis, and communications you improve the odds for effective eradication, recovery with integrity and forensic-quality reporting.

Security Management Benefits
- Be prepared to handle any incident your team faces
- Control the situation, minimizing the impact to the business
- Efficiently manage your response across multiple departments

Useful Links:
NIST Incident Handling Guide
SANS Incident Handler’s Handbook

Risk Management Benefits
- Communicate effectively to ensure risk mitigation methods are applied
- Prioritize resources and activities where they matter most
- Report and tune based on response learning, reducing risk moving forward

Useful Links:
NIST Risk Management Framework Guide
Sample Policies and Plans

Action Plan
Having a view into what is possible is the first step in taking action. The next step is to bring your team together to drive it toward reality. Email this guide to your peers and managers to begin sharing your playbook with them.

With this playbook, you will be better prepared to handle the response. To help with the management and automation of this incident response playbook, consider working with CyberSponse and their partners. Come take a look at what they do.

For additional incident response playbook examples, visit https://www.incidentresponse.com/playbooks