Are You Ready? A Planning Tool for Managing Sensitive Data Incidents

Kimberly A. Milford, Indiana University
Shirley C. Payne, University of Virginia

May 16th, 2012
Copyright: Kimberly A. Milford and Shirley C. Payne; 2012

This work is the intellectual property of the authors. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the authors.
TODAY’S FOCUS
Agenda

- The world as we know it
- Organizing for incident response
- Checklist overview
- Scenarios
10 SECURITY TRENDS TO WATCH IN 2012


1. Breaches now inevitable
2. Cyber espionage continues
3. Mobile malware continues to increase
4. Mobile devices get anti-theft protection
5. Spear-phishing scourge continues
6. Social engineering attacks hit social networks
7. Botnets keep infiltrating businesses
8. Breach notifications gain greater traction
9. Critical infrastructure rhetoric keeps heating up
10. Code gets externally reviewed
MORE WORRIES

- Everything physical can be digital
- Paper breaches matter too
- Hacktivism
- Clarity of data protection roles for external partners
- Scalability of incident response
- Pressure to swiftly respond to incident reports
LET’S TALK SOLUTIONS
Effective Incident Response

- Forensics Skills
- Tools
- Procedures
- Communications
- Cooperative Relationships
- Policy
Effective Incident Response

- Forensics Skills
- Tools
- Communications
- Cooperative Relationships
- Policy
- Procedures
Effective Incident Response

- Forensics Skills
- Tools
- Procedures
- Communications
- Policy
- Cooperative Relationships
Effective Incident Response

- Forensics Skills
- Tools
- Communications
- Procedures
- Policy
- Cooperative Relationships
PARTIES TO INVOLVE

Core IR Team

- Legal
- Law Enforcement
- Risk Management
- Public Relations
- High Level Management
- Audit
- IT Operations

PARTIES TO INVOLVE

Core IR Team

- Legal
- Law Enforcement
- Risk Management
- Public Relations
- High Level Management
- Audit
- IT Operations
Effective Incident Response

- Forensics Skills
- Tools
- Procedures
- Communication Plan
- Policy
- Cooperative Relationships
Essential: A coordinated, repeatable checklist for incident response
EDUCAUSE
Sensitive Data Exposure Incident Checklist

IDENTIFICATION
CONTAINMENT AND ASSESSMENT
ERADICATION AND RECOVERY
NOTIFICATION
FOLLOW UP
CHECKLIST PROVIDES:

✓ Tasks associated with each major step
✓ Owner for each task
✓ Guidance
✓ Examples
✓ Additional Resources
CHECKLIST COMPLEMENTS:

- [Incident Security Incident Management](#) chapter of EDUCAUSE Information Security Guide
- [EDUCAUSE Data Incident Notification Toolkit](#) that provides templates for:
  - Building a press release
  - Notification letter components
  - Incident-specific web site
  - Incident response FAQ
  - Generic identity theft web site
HOW TO USE CHECKLIST

- Download and customize
- Leverage for all security incidents types, e.g.,
  - Exposure of PII or other sensitive data
  - Public website defacements
  - Loss of paper records
- Utilize to practice IR readiness
- Multi-task steps and sub-steps where feasible
Eradicate and mitigate system vulnerabilities

Return evidentiary equipment and systems to service once they are secured

Identification

Contact Security Office
- Contact law enforcement if lost/stolen physical asset or possible criminal activity
- Conduct preliminary assessment

Containment and Assessment

Assemble team and review responsibilities
- Collect and preserve evidence, with appropriate chain of custody
- Perform Forensics
- Complete final assessment of type and scope of exposure

Eradication and Recovery

Eradicate and mitigate system vulnerabilities

Follow Up and Conclusion

Notify affected individuals, state offices, federal offices, granting agencies, third parties, credit card processors, and credit bureaus

Obtain credit monitoring services

Collect and record staff time and expenses

Implement additional remediation as needed

Securely archive, file and destroy incident records and artifacts

Determine notification requirements
- Collect contact information
- Establish phone, email and web support for affected individuals
- Prepare press and media handling plans, notification letter, and mailing
- Obtain credit monitoring services

Notification

Steps are shown in relative order and indicate approximate start/finish times. Depending upon the nature of the incident and size of the response team, some steps may be performed in parallel, as shown here.
A FEW CAVEATS

- Breach notification requirements must be guided by current laws, industry standards, and contractual obligations.

- Who assumes responsibility for checklist steps may vary when external parties (e.g., vendors, research grant partners, etc.) involved.
Identification
Dude! What just happened?
Identification

1. Limit the damage
2. Alert the Security Office immediately
3. Conduct preliminary assessment
4. Notify others

Tip: Documentation
Tip: The exceptions rule
1. Limit the damage
   - Devices
     - Turn it off (yeah, it’s that easy)
   - Sites
     - Ensure that at-risk data input forms are inaccessible
     - Shut down all unnecessary services
   - Notice
   - Applications
     - Shut down or segregate at-risk services
2. Alert the Security Office immediately
3. Notify the appropriate people

Law enforcement agencies
Counsel
Other campus officials

Tip: When in doubt, notify … and remember to keep them informed
4. Conduct preliminary assessment

- What happened?
- What sensitive data is at risk?
- Who does it belong to?
- How many people could possibly be impacted?
- How likely is it that the sensitive data would be discovered and used by unauthorized individuals?
WHAT WOULD CHUCK NORRIS DO?

A. Unplug the computer  
B. Call the FBI  
C. A roundhouse kick to the head
Containment and Assessment
1. Assemble the Incident Response Team
2. Review the process and responsibilities
3. Collect and preserve evidence
   • Chain of custody
4. Limit scope and magnitude where possible
5. Forensics
6. Complete final assessment and documentation
1. Assemble the Incident Response Team
   - Appoint a team leader
   - Review process and responsibilities
3. Collect and preserve evidence
Containment and Assessment
1. Local IT Support makes an image of the hard drive and gives it to Information Security Office (Incident Response).

2. Information Security Office analyzes the evidence on the hard drive.

3. Information Security Office provides the evidence to Legal Counsel.

4. Legal Counsel works with Law Enforcement to present evidence.
# Containment and Assessment

## Hard Drive/Computer Details

<table>
<thead>
<tr>
<th>Description:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Manufacturer:</th>
<th>Model #:</th>
<th>Serial #:</th>
</tr>
</thead>
</table>

## Chain of Custody

<table>
<thead>
<tr>
<th>Date/Time:</th>
<th>From:</th>
<th>To:</th>
<th>Reason:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>Name/Organization:</td>
<td>Name/Organization:</td>
<td></td>
</tr>
<tr>
<td>Time:</td>
<td>Signature:</td>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td>Name/Organization:</td>
<td>Name/Organization:</td>
<td></td>
</tr>
<tr>
<td>Time:</td>
<td>Signature:</td>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td>Name/Organization:</td>
<td>Name/Organization:</td>
<td></td>
</tr>
<tr>
<td>Time:</td>
<td>Signature:</td>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td>Name/Organization:</td>
<td>Name/Organization:</td>
<td></td>
</tr>
<tr>
<td>Time:</td>
<td>Signature:</td>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td>Name/Organization:</td>
<td>Name/Organization:</td>
<td></td>
</tr>
<tr>
<td>Time:</td>
<td>Signature:</td>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td>Name/Organization:</td>
<td>Name/Organization:</td>
<td></td>
</tr>
<tr>
<td>Time:</td>
<td>Signature:</td>
<td>Signature:</td>
<td></td>
</tr>
</tbody>
</table>
4. Limit scope and magnitude where possible
   - Remove active and cached content on web sites
   - Change passwords
   - Shut down operations of compromised servers
5. Perform forensics and document findings

**Tip:** Preserve the original of the evidence and work with a copy or image.

**Tip:** Try to minimize disruption to units, systems and the original evidence.

**Tip:** Work towards repeatable results.
Case Report # 20120516.22

A concerned citizen contacted the police department regarding possible stolen property. He told police that while he was searching the Internet, hoping to find a motorcycle for a reasonable price, he found an ad that met his requirements. This ad listed a Honda motorcycle for a low price, so he contacted the seller. Upon meeting the seller he became suspicious that the motorcycle was stolen. After hearing this information, police alerted the Auto Theft Unit. The Auto Theft Unit conducted a sting operation to purchase the motorcycle. Undercover officers met with the suspect, who, after receiving payment, provided them with the vehicle, a vehicle title, registration card, and insurance card. The suspect was arrested and the vehicle he was driving was searched incident to his arrest. During the search, a notebook computer was seized. Although the documents provided by the suspect looked authentic, document examiners determined that the documents were counterfeit. The auto theft investigator contacted the computer forensic laboratory for assistance in examining the seized computer. The investigator obtained a search warrant to analyze the computer and search for materials used in making counterfeit documents and other evidence related to the auto theft charges. The laptop computer was submitted to the computer forensic laboratory for analysis.

Objective: Determine if the suspect used the laptop computer as an instrument of the crimes of Auto Theft, Fraud, Forgery, Uttering False Documents, and Possession of Counterfeit Vehicle Titles and/or as a repository of data related to those crimes.

Offenses: Auto Theft, Fraud, Forgery, Uttering False Documents, and Possession of Counterfeit Vehicle Titles.

Case agent: Auto Theft Unit Investigator

Tools used: Guidance Software™, EnCase®, DiGit®, Jasc Software™ Quick View Plus®, and AccessData™ Password Recovery Tool Kit™
WHAT WOULD CHUCK NORRIS DO?

A. Assemble the football team  
B. Establish chain of custody  
C. A roundhouse kick to the head
Eradication and Recovery
1. Revisit 2.5 and look for additional ways to limit exposure
2. Eradicate and mitigate system vulnerabilities, review access privileges, and remediate risks to sensitive data stores
3. Return evidentiary equipment and systems to service once they are secured.
Eradication and Recovery

REACTIVE → PROACTIVE

EXTERNAL

INTERNAL
WHAT WOULD CHUCK NORRIS DO?

A. Run Identify Finder on impacted systems
B. Write a script to find all local stores of kung-fu movies
C. A roundhouse kick to the head
1. Determine need to issue notifications and how
2. Locate contact information for people affected by breach
3. Activate all appropriate notification & assistance services
4. Inform appropriate external entities
1. Determine need to issue notifications and how

- Relevant laws, regulations, contractual obligations may dictate
- If not, be guided by past decisions and lessons learned

**Tip:** Check out “Determining Notification in Event of Breach”
1. Determine need to issue notifications

If no, go to Step 5: Follow-up
2. Locate contact information for people affected by breach

Some breach notification laws allow alternative means of notification depending on

- # of people to be notified
- Absence of contact information
- Cost
3. Activate all appropriate notification & assistance services

- Notification method? U.S. postal, email, incident website
- Free credit monitoring offered?
- Help desk?

Tip: The EDUCAUSE Data Incident Notification Toolkit is your friend
4. Inform appropriate external entities

- State agencies
- The Feds
- Research sponsors/partners
- 3rd party service providers
- Credit card processors
- Credit bureaus
- The Press

Tip: Coordination is key
WHAT WOULD CHUCK NORRIS DO?

A. Handle the truth
B. Be ready and mobilize fast
C. Coordinate
D. A roundhouse kick to the head
Follow Up
Follow Up

1. Collect staff time and record in incident documentation
2. Schedule a debrief meeting
3. Assess remediation needs
4. Initiate plans for remediation
5. Securely files all records, communications, notes and other incident artifacts.
2. Schedule a debrief meeting

AGENDA:

- Any contact from agencies reported to?
- Review contacts from individuals affected. All concerns addressed?
- Were any letters returned? Did you find alternative ways to reach the individual?
- What steps were taken by the department in response to data disclosure and preventing future incidents? What help is still needed to take all appropriate steps?
- How can we improve the process, kit, coordination, etc.?
- Should we collect mail archives (PST files) from response team to preserve our correspondence (when possible legal action is suspected)?
3. Assess remediation needs
4. Initiate plans
5. Securely files all records, communications, notes and other incident artifacts.
WHAT WOULD CHUCK NORRIS DO?

A. Develop remediation plans
B. Throw out all records of the incident
C. A roundhouse kick to the head
PICK A SCENARIO

- Arrest of employee for credit card fraud
- Server theft from research lab
- *Insert your favorite here*
EDUCAUSE LINKS

- Sensitive Data Exposure Incident Checklist
  - https://wiki.internet2.edu/confluence/display/itsg2/Incident+Checklist

- Information Security Guide: Incident Management chapter
  - https://wiki.internet2.edu/confluence/display/itsg2

- Data Incident Notification Toolkit
  - https://wiki.internet2.edu/confluence/display/itsg2/Data+Incident+Notification+Toolkit

- Incident Handling and Response Resources
  - http://www.educause.edu/resources

- Forensics Resources
  - http://www.educause.edu/resources

- Data Breach Resources
  - http://www.educause.edu/resources
OTHER USEFUL LINKS

- HIPAA Breach Notification Rule

- FERPA Information Release Rule

- VISA Breach Notification Requirements

- Determining Notification in Event of Breach
  - http://www.ucop.edu/irc/itsec/securitybreach.html
THANK YOU