Building an Effective Security Incident Response Plan

Presentation for 2019 Resiliency Services Showcase

Scott Owens, CISM, CBCP, PMP

Founder, Managing Director

BluTinuity LLC

Initial Scenario

BluTinuity Experience & Accreditations

Scott Owens, CISM, CBCP, PMP

- Founder & Owner of BluTinuity LLC
- 28+ Years of Experience in Business Continuity, Disaster Recovery, & Incident Response
- 30,000+ Managed Project Team Hours Through >100 Unique Client Projects
- Bachelor of Science Degree from Marquette University
- Professional Certifications:
  - Certified Information Security Manager (CISM) through ISACA
  - Certified Business Continuity Professional (CBCP) through the Disaster Recovery Institute
  - Certified Project Management Professional (PMP) through the Project Management Institute


Security Incidents &
Data Breaches

What is a Security Incident?

NIST Special Publication 800-61r2 (Computer Security Incident Handling Guide): *A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices*.

ISACA: *An incident is any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service*.

What is a Data Breach?

A data breach is a security incident in which information (usually confidential, secret, personal, or otherwise important) is stolen from information systems without authorization or awareness in order to compromise the availability, authenticity, integrity and confidentiality of this data.

Common Targets of Data Breaches

- **Protected Health Information (PHI)**: Patient related health data as defined by the HIPAA Security and Privacy Rules
- **Payment Card Information (PCI)**: Financial card (credit/debit) information as defined by the Payment Card Industry Security Standards Council
- **Personally Identifiable Information (PII)**: Information that can be used to discern an individual's identity
- **Trade Secrets**: Corporate information (strategic, operational, financial, etc.) that may provide a competitive advantage

Why is Security Incident Response Important?

Recent Security Incidents / Data Breaches

May 2017: Wannacry Ransomware;
Exploitation of Unpatched Microsoft O/S
230,000+ Victims in 150 Countries
Photo Source: Security Intelligence

May - July 2017: Equifax Data Breach
Root Cause was Failure to Apply a Security Patch
143 Million Consumers Breached
Name, SSN, Driver License, Credit Card Numbers

February 2017: Amazon Web Services Outage
~4 Hours of Total Downtime Affecting Over 100,000 Websites for
Customers Such as Pinterest, Reddit, Foursquare, Netflix

April 2015: US Office of Personnel Management
Data Breach
21.5 Million Records Breached
Data Included SSN's & Security Clearance Info

2012: Nationwide Insurance Data Breach
Root Cause was Failure to Apply a Security Patch
1.2 Million Records Breached
$5.5M Settlement

January 2015: Anthem Data Breach
78.8 Million Records Breached

November 2013: Target Data Security Breach
40 Million Customers' Credit Card Information Stolen
70 Million Customers' Personal Information Stolen

Other Data Breaches Since 2012

Images displayed are registered trademarks of their respective companies.

Other Real World Security Incident Examples

- Unsuccessful spear phishing attack on healthcare organization in Chicago (attempt to extort $27,000)
- Successful ransomware attack on church
- In the news Jan 21, 2019: Wichita State University employees tricked into providing university ID and password, which was used to access banking information to redirect paychecks to a hacker's bank account

2018 Ponemon Institute Data Breach Study

- Costs include investigations, forensics, determining victims, organizing incident response, communication / public outreach, documentation, compliance, call centers, legal services, audit services, identity protection services, etc.

- The average per capita cost of a data breach in the US is $233
- By Industry: Healthcare $408; Financial $206; Services $181; Pharmaceuticals $174; Technology $170; Energy $167; Education $166

- The average total organizational cost of a data breach in the US is $7.91M

- Malicious attacks account for 48% of data breaches

2018 Ponemon Institute Data Breach Study

The following items reduce the per capita cost of a data breach:

- Incident Response Team $14.0
- Extensive use of encryption $13.1
- Business Continuity Management involvement $9.3
- Employee training $9.3
- Participation in threat sharing $8.2
- Use of security analytics $6.9
- Extensive use of Data Loss Protection (DLP) technology $6.8
- Board level involvement $6.5
- CISO appointed $6.5
- Data classification schema $5.1
- Insurance protection $4.8

Compliance Requirements

- HIPAA * Health Information Portability & Accountability Act (Healthcare)
- FFIEC * Federal Financial Institutions Examination Council (Banking)
- NERC * North American Electric Reliability Corporation (Energy)
- AICPA SOC * American Institute of CPA's Service Organization Control Audits
- State of New York Cyber Security Requirements; Several Other States Have Similar Requirements

Best Practices

- NIST Cybersecurity Framework
- ISO 27002
- HITRUST Cybersecurity Framework
- NIST SP800-61r2 Computer Security Incident Handling Guide
- NIST SP800-184 Guide for Cybersecurity Event Recovery
- Disaster Recovery Institute International (DRII) Professional Practices
- SANS Incident Handlers Handbook

Insurance Requirements

- Most business and cyber insurance policies require the organization to have a mature Incident Response Plan and many of the items listed on the previous Ponemon Institute Data Breach Study slide

Key Aspects of a Security Incident Response Plan

Risk Assessment

- **ISACA**: *A Risk Assessment is the process used to identify and evaluate risk and its potential effects. Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan*.

- Structured Method to Understand Risk – Categorized and Weighted

Risk Assessment Considerations

- Confidentiality of Information
- Availability of Information
- Integrity of Information
- Financial Impact
- Legal Impact
- Regulatory Compliance Impact
- Brand / Reputation Impact
- Operational Performance Impact
- Customer / Client Impact
- Supplier / Vendor Impact

Identification of Potential Scenarios

Think through most likely scenarios and develop Runbooks with specific action steps for those scenarios

- Ransomware
- Malware / Virus Attack
- Network Intrusion
- Data Loss / Breach
- Compromised Credentials / Unauthorized Access
- Loss of Laptop
- Insider Threat
- Social Media Account / Website Compromise
- Physical Security Breach

Security Incident Response Team

Multi-Disciplinary Leadership Team Usually Including These Roles:

- Chief Information Security Officer
- Chief Information Officer
- Privacy Officer
- General Counsel
- Chief Compliance Officer
- Marketing & Communication Officer
- Risk Management Officer
- Facilities & Real Estate Officer
- Human Resources Officer
- Other Leaders and Subject Matter Experts as Needed

Incident Response Team Communication

- Video Conference Bridge
- Group Texting
- Team Contact Email Group
- List of Emergency / Personal Team Phone Numbers
- Intranet Page

External Team of Experts

- Cybersecurity & Data Breach Expert
- External Counsel
- Public Relations
- Cybersecurity & Forensic Investigations
- Network Security
- Data Center
- Technical Solution Vendors
- Insurance Agency
- Call Center / Crisis Hotline
- Credit Monitoring
- Employee Assistance Program
- Real Estate / Alternate Facility
- Portable Power & Communications
- Contractors & Grounds Management
- Alternate Transportation

Law Enforcement & Government

- FBI Cyber Security Investigations
- Local Police & Fire
- County & State Emergency Management
- Ready Wisconsin
- State Dept of Transportation
- FEMA
- National Weather Service

Incident Criteria Definitions

Level	Criteria
Level 1 [Low Severity] Security Event Criteria	* Any technology incident impacting a single development or test environment * Any technology incident impacting the ability to perform routine operations for greater than ½ day * Any direct technology security threat (as opposed to random attempts to hack assets) * System Administrator or designee will respond to the incident within 48 hours to investigate, identify the root cause, suggest a resolution, and close or escalate the incident
Level 2 [Medium Severity] Security Event Criteria	* Any technology incident impacting any hardware, software, or communication component with an expected recovery time of greater than 1 day * Any technology incident impacting a single client production environment or data * Any incident that exposes PHI with the potential to become a HIPAA data breach as defined in these policies * Any facility related incident at any office involving a risk to human safety requiring staff to leave the office for > 1 day * Needs urgent response to diagnose the situation – communication to the SIRT is started; SIRT full engagement is a consideration
Level 3 [High Severity] Security Event Criteria	* Any technology incident with widespread impact involving multiple client production environments and/or a single client environment experiencing a complete system outage * Any facility related incident at any office involving a risk to human safety requiring staff to leave the office for > 1 week * Any person related incident involving intentional misuse of resources or potential sabotage of resources * Any person related incident involving weapons or direct threats to staff or onsite contractors * Any incident that exposes PHI with a high potential to become a HIPAA data breach as defined in these policies * Needs immediate response and containment – SIRT is engaged as a priority

Security Incident Response Procedures

Required

- Actions, Activities, Tasks
- Timing of Activities
- Responsible Roles
- Ability to Track Actual Details

Security Incident Response Procedures

Preparation (Action to take today)

- Risk Assessment
- Develop the SIRP
- Build Relationships with External Experts
- Update Infrastructure Documentation
- Review RTO & RPO for Applications & Systems
- Security Awareness & Training
- Comprehensive Malware Protection & Monitoring Tools
- Encryption
- Implement Information Security Best Practices

Security Incident Response Procedures

Incident Detection & Analysis

- Detection via Monitoring Tools, Help Desk Requests, or Other
- Initial Incident Response
- Document Information About the Incident
- Determine Initial Incident Criteria
- Establish Forensic Chain of Custody
- Incident / Disaster Declaration
- Team & Plan / Runbook Activation
- Communication Strategy & Status Reporting

Security Incident Response Procedures

Incident Containment, Eradication, & Recovery

- Strategies for Containment (Segregation of infrastructure, disable functions, take systems offline, terminate/block access, change access credentials, physical security, etc.)
- Strategies for Eradication (Remote data wipe, removal of malware, patch & mitigate vulnerabilities, etc.)
- Strategies for Recovery (Data recovery, disaster recovery plans, runbook activation, etc.)

Security Incident Response Procedures

Runbooks for Common Scenarios

- Based on Risk Assessment
- Step-by-Step, Specific Technical Plan
- Facilitates Rapid Response, Even if Key Technical Resources are Unavailable

Security Incident Response Procedures

External Notification (*As Appropriate*)

- Legal Counsel
- Law Enforcement
- Insurance Carriers
- State & Federal Agencies
- Customers / Clients
- Vendors / Suppliers / Business Partners

Security Incident Response Procedures

Post Incident Activities

- After Action Review Session
- Investigation Report
- Report to Board of Directors / Managers and Senior Leadership
- Staff Communication
- Mitigation Plan – Technical & Process Oriented
- Breach Notification
- Training & Awareness

Communication Plan

- Pre-defined, Pre-approved Messages
- By Security Incident / Scenario Type
- By Stakeholder Group
- Include Message Initiator
- Include Message Medium

Data Breach Notification

Formal Procedures to Meet Data Breach Notification Compliance and Contractual Requirements, within Specific Timelines

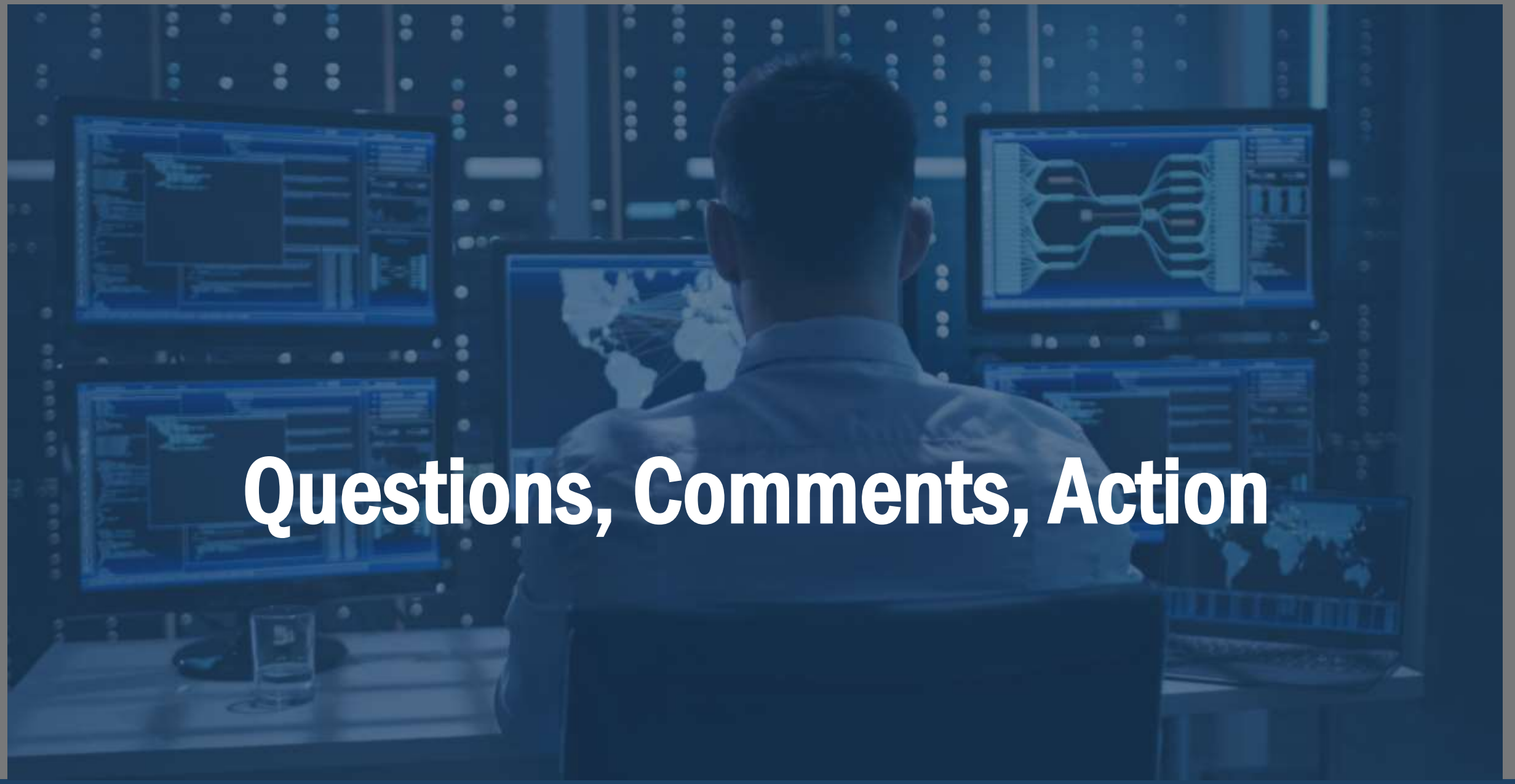
- State & Federal Agencies
- Customers / Clients

After Action Review

- Structured Examination of the Incident and the Team's Response
- Examines the Following:
  - Roles & Responsibilities
  - Key Decisions
  - Timeline of Activities
  - Performance Against Incident Response Procedures
  - Performance Against Schedules
  - Use of Tools
  - Corrective Action Plan to Prevent Similar Incidents, Reduce the Impact of Future Incidents, and Improve Future Incident Response

Tabletop Exercises

Periodic Testing via Tabletop Exercise is the Best Way to Validate Your Security Incident Response Plan



Questions, Comments, Action

Contact Information

Scott Owens, CISM, CBCP, PMP
Founder, Managing Director

BluTinuity LLC
blutinuity.com

414.215.9020
sowens@blutinuity.com
linkedin.com/in/owensscott

Please contact us to see how BluTinuity can make a difference for your business.