Getting Cyber-Prepared:
Incident Response & Business Continuity
November 2018

This SecureTheVillage Webinar brought to you by …

Getting Cyber-Prepared: Incident Response & Business Continuity

- Guide: Stan Stahl, PhD
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guests
  - Brad Maryman (FBI Retired), President, Maryman & Associates Inc.
  - Pat Fraioli, Esq., Managing Director, MRM Capital Holdings.

Getting Cyber-Prepared: Two Themes

Failing to Plan is Planning to Fail.

Barry Boehm
Software Engineer

In preparing for battle I have always found that plans are useless, but planning is indispensable.

Dwight Eisenhower
General, President

Getting Cyber-Prepared: Objectives

- When an incident happens, you have three fundamental objectives:
  - Getting back to work as quickly as possible
  - Determining exactly what happened as thoroughly as necessary
  - Managing Your Legal Exposure
- It is the purpose of planning to accomplish these objectives

Incidents Can Impact Confidentiality / Privacy & Business Continuity

Confidentiality / Privacy	Business Continuity	Incident
✓		Loss of information confidentiality (data theft)
✓	✓	Compromise of information integrity (damage to data or unauthorized modification)
✓	✓	Theft or damage of physical IT assets including computers, printers, etc.
✓	✓	Denial of service attack
✓	✓	Any other hindrance in being able to access the system or data (availability)
✓		Misuse of services, information, or assets
✓	✓	Infection of systems by unauthorized or hostile software
✓		Attempts at unauthorized access
✓	✓	Unauthorized changes to organizational hardware, software, or configuration
✓	✓	Reports of unusual system behavior
✓		Responses to intrusion detection alarms
	✓	Loss of one or more critical servers
	✓	Internal IT network disruption resulting from a downed firewall, router, switch, other network component, etc.
	✓	External IT network disruption due to the lack of availability of an outsourced system, such as a hosted server
	✓	Telecommunications disruption resulting in not being able to communicate externally from a site, including via phones or data network
	✓	Loss of website or other external facing application, either marketing, e-commerce or other
	✓	Loss of access to an Internet service or Software as a Service (SaaS), such as Salesforce, Dropbox, etc.
	✓	Unavailability of a work facility
	✓	Unavailability of key personnel

Role of Forensics & Investigations: Examine Evidence & Determine Facts

- Were we compromised?
- Was the compromise leveraged?
- Was PII or trade secrets exfiltrated?
- Do we have a financial loss?
- Do we have the logs and artifacts to indicate attribution or origin?
- Were things other than the main event transpiring in the background?

Legal Framework

- Fulfill your obligations
- State by State, GDPR
- Notification
- Other Requirements
- Affected Individuals
- Regulators (e.g. 500)
- Who What Where…
- You Must Disclose What You Learn
- Protect the Company
- Time is of the essence (so, checklists)
- Planning indispensable
- Attorney-directed
- Atty-Privilege
- Insurance Issues
- You Decide What to Disclose & To Whom

Incident Response & Business Continuity Touch Every Element of NIST Framework

Identify	Protect	Detect	Respond	Recover
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management	• Identity Management & Access Control • Awareness and Training • Data Security • Information Protection Process and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communication

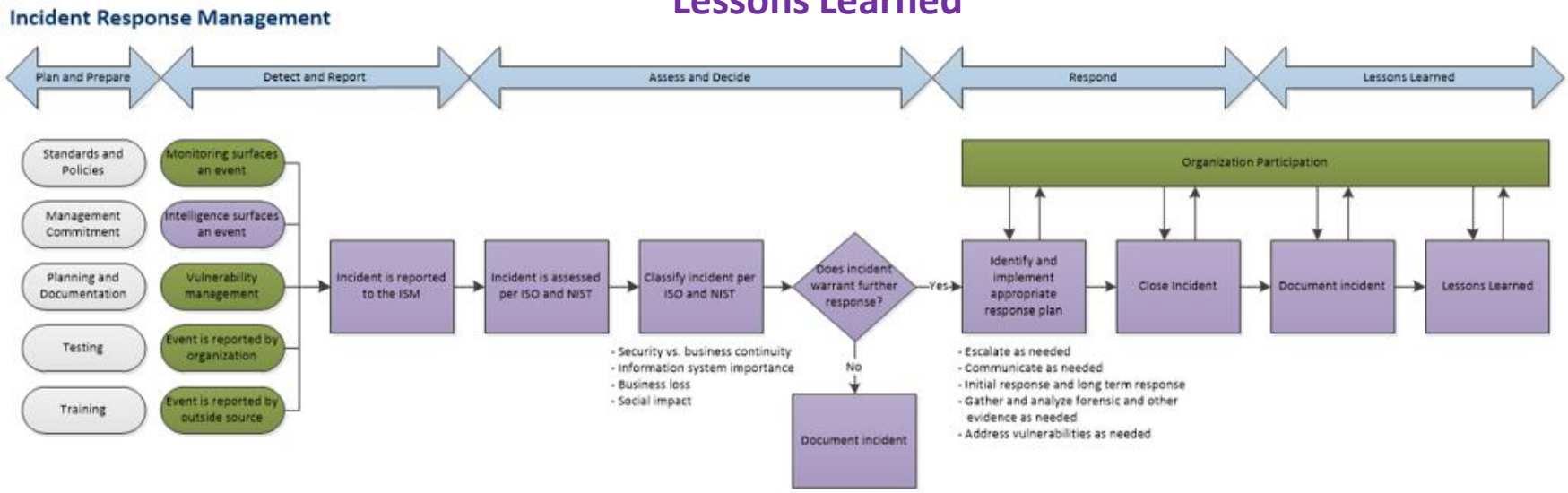
Cybersecurity Framework, v 1.1. NIST, 2018

The Incident Response Team

- Information Security Manager
- Appropriate Executives
  - CEO, COO, CFO, HR
- CIO, IT Director, IT Vendor
- Information Security Subject Matter Expertise
- Computer Forensics / Investigator Subject Matter Expertise
- Legal Counsel
- PR

Five Basic Incident Response & Business Continuity Phases

Plan & Prepare
Detect & Report
Assess & Decide
Respond & Recover
Lessons Learned



References:
ISO 22301: *Business Continuity Management Systems*, 2012
ISO/IEC 27035: *Information Security Incident Management*, 2016
NIST 800-61: *Computer Security Incident Handling Guide*, 2012

Planning & Preparation … Testing

- IT Management
  - Information Backups and Images
  - Computer Logs and Audit information
  - Documentation
  - Disaster Recovery & Restore Procedures
  - Off-Site Preparedness
  - Telecommunications Preparedness
  - Power / HVAC etc
- Organization
  - Business Impact Analysis
  - Staff Resources
  - Incident Handling Communications
    - Legal
    - Public Relations
- Testing the Plan
  - IT Testing
  - Table-Top Exercises

Information to Gather Ahead of Time

- Contact information
  - Attorney
  - Insurer
  - IT Vendors
  - Cloud Vendors
  - Security Vendor
  - Forensics Specialist
  - Local Law Enforcement
  - PR Person
  - Banker
  - Accountant; Payroll
- System Information
  - Network Inventories, Diagrams
  - Server, Router, Firewall Configurations
  - Passwords
- Data Maps
  - Where Are The Crown Jewels?
- Checklists and Procedures

Mistakes to Avoid / Lessons Learned

- In the rush to remediation, remember to preserve the memory captures and logs, etc. needed to perform forensics
- Avoid making assumptions about what happened, let the evidence tell you
- Once the event is addressed and behind you, bring the team back together to assess the plan; what worked and didn't work
- Discuss what preventive steps can be taken to avoid a recurrence

ResourceKit: Getting Cyber-Prepared: Incident Response & Business Continuity

Getting Cyber-Prepared: Incident Response & Business Continuity

ResourceKit Articles

Contacting Law Enforcement - F.B.I. Los Angeles: (310) 477-6565 Secret Service: (213) 894-4830 Los Angeles County District Attorney's Office: (213) 974-3512. Identity Theft Los Angeles County Sheriff's Office: Consumer Guide to Preventing Identity Theft (National Crime Prevention Council) Orange County Sheriff's Department: Scams Orange County Sheriff's Department: Identity Theft FBI Internet Crime Complaint Center (IC3)

Incident Response Objectives - The objectives of incident response are to: Verify that an incident occurred or document that one has not Maintain or restore business continuity while reducing the incident impact Identify the causes of the incident Minimize the impact of future incidents Improve security and the incident response planning function Prosecute illegal activity Keep management, staff and […]

Incident Response Plan Components - The should contain the following information necessary to maintain or resume operations and respond to an information security incident: Names, roles and contact information for the Incident Response Team (IRT), staff, vendors (including vendors needed to respond to an incident), and key clients Regulatory, contractual and compliance requirements An overview of critical business functions, criticality […]

Incident Response Management and the Incident Response Team - Information Security Manager (ISM) The Information Security Manager (ISM) is responsible for maintaining the confidentiality, integrity, and availability of the Organization's business information. As such, the ISM has senior-level responsibility for the incident response plan. If an incident has the potential to compromise or disrupt confidentiality, integrity or availability, the ISM has the authority to […]

Incident Response Phases; Plan & Prepare - The Five Incident Response Phases Plan and Prepare Detect and Report Assess and Decide Respond Lessons Learned Plan and Prepare As part of the planning and preparation process, the Organization needs to maintain documentation on the following. Business Impact Analysis Disaster Recovery and Restore procedures Business Staff Resources Information backups and images Offsite Preparedness Telecommunications […]

Initial Event Detection and Plan Initiation - Initiation of this plan occurs upon the observation of an event that might have information security or business continuity implications. Examples include: A

https://resourcekit.securethevillage.org/resources/getting-cyber-prepared/

Information Security Manager & Leadership Team — Getting Started

- Form Your Incident Response Team
- Have Everyone Watch the Video
- Review the ResourceKit
- Start Planning

Next Webinar: Third-Party Security Management

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- December 6, 10 AM Pacific
- Registration: SecureTheVillage.org

SecureTheVillage Webinar Series

- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable
- SecureTheVillage ResourceKit
- First Thursday of month, 10AM Pacific

Information Security Management Webinar Schedule — 2018

February 1	Information Security Management Overview; The Role of Leadership
March 1	The Information Security Management & Leadership Team
April 5	Online Bank Fraud — How To Avoid Being a Victim
May 3	Basics of Cyber-Law
June 7	Information Security Policies and Standards
June 29	Conducting an Information Security Risk Assessment
August 2	Information Classification and Control
September 6	Securing the Human
October 4	Managing Security of the IT Infrastructure
November 8	Getting Cyber-Prepared: Incident Response & Business Continuity
December 6	Third-Party Security Management
January 2019	Managing Cyber-Risk and Insurance

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Monthly Webinar Series: Provides Practical Real-World Actionable How-To Information Security Management Guidance.

Executive Focus Groups: Designed to assist Chief Executives understand how to turn their organization into Cyber-Guardians and create a cyber resilient culture.

Information Security Management and Leadership ResourceKit: A practical guide for implementing an information security management and leadership program in your organization.

Code of Basic IT Security Management Practices: A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

Community-Based Programs to train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: *SecureTheVillage.org*

For More Information …

Stan Stahl, SecureTheVillage & Citadel Information Group
Stan@SecureTheVillage.org
323-428-0441

Brad Maryman, Maryman & Associates
maryman@maryman.com
805-522-2264

Patrick Fraioli, MRM Capital Holdings
pfraioli@icloud.com
310-866-8595

FREE Citadel *Cybersecurity News of the Week & Weekend Vulnerability and Patch Report*
https://Citadel-Information.com

For Marketing / Sponsorship Opportunities
Email us at info@securethevillage.org. Put *Sponsor Opportunity* in Subject
Visit us at https://securethevillage.org/sponsorship-opportunities/