Securing the Network—Lessons Learned From Cyber Investigations

Visibility. Visibility. Visibility.

October 2019

This SecureTheVillage Webinar brought to you by …

I hear and I forget. I see and I remember. I do and I understand. … Confucius

PEPPERDINE | GRAZIADIO BUSINESS SCHOOL

CyRP

CITADEL
INFORMATION GROUP, INC.

Cybersecure SoCal 2019
Cybersecurity is a Team Sport.
Building a Winning Cybersecurity Team

… a joint presentation of SecureTheVillage and Pepperdine Graziadio Business School

Keynote Speaker: Ron Ross
Fellow at National Institute of Standards and Technology

October 17, 2019 … Mark Your Calendars

StaySafeOnline

Powered by: **National Cyber Security Alliance**

Securing the Network—Lessons Learned From Cyber Investigations

- Guide: Stan Stahl, PhD
  - Founder, SecureTheVillage
  - President, Citadel Information Group

- Guest: Joe Greenfield
  - Managing Director and Chief Forensic Examiner, Maryman & Associates
  - Associate Professor of Practice, USC Viterbi School of Engineering

Webinar 10: Getting Cyber-Prepared: Incident Response & Business Continuity, Nov 2018

Getting Cyber-Prepared: Obj

5

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

Incident Response & Business Continuity Touch Every Element of NIST Framework

9

Identify	Protect	Detect	Respond	Reco
• 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	• Recover Planning • Improv • Commu

Cybersecurity Framework, v 1.1. NIST, 2018

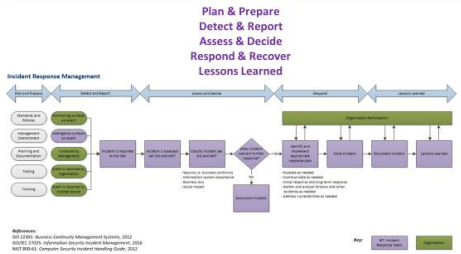
The Incident Response Team

10

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

Five Basic Incident Response & Business Continuity Phases

11



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

Lessons Learned from Cyber Investigations

- Outline
  - Visibility: What it is
  - Case Studies in Visibility: The Good. The Bad. And the Ugly.
  - Getting Visible
  - Testing Your Visibility

Critical Importance of Network Visibility in Response to a Cyber Incident

Security Visibility: What It Is

- Intrusion Detection & Prevention, Etc
- Audit Logs
  - Systems and Servers
  - Network Devices
  - Security Systems
- Surveillance
- Information Sharing & Analysis Organizations (ISAOs)
  - LA Cyber Lab

Visibility is Seen Throughout the 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

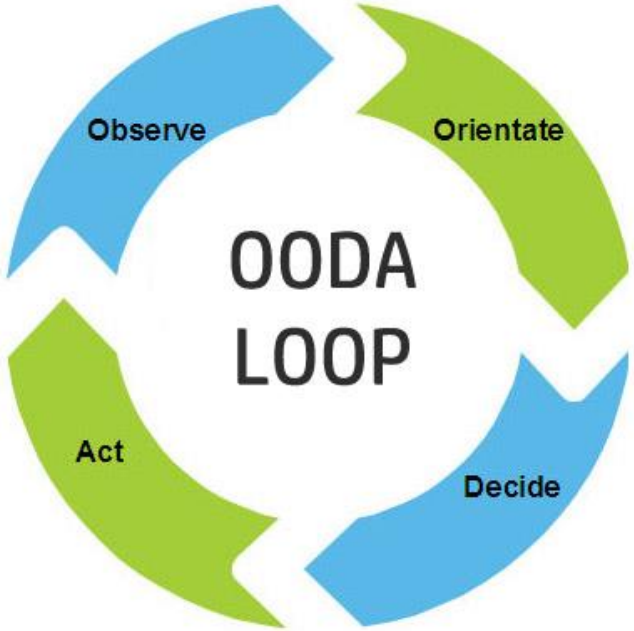
Cybersecurity Framework, v 1.1. NIST, 2018

Critical Importance of Visibility: Case Studies

- No Visibility
- Partial Visibility
- Complete Visibility

Visibility Provides Situational Awareness

- The faster you can see what's going on, the faster you can contain it.
  - Prevent Incident
  - Contain It Sooner
- The faster you can contain it, the less you will lose and the less it will cost



Speed is Crucial

Getting Prepared: Attack & Response

- Test. Test. Test.
  - Visibility
  - Monitoring
- Test Response to Simulated Attacks
  - Phishing leads to BEC and/or ransomware
  - RDT attack leads to corporate espionage
- Ensure visibility over ‘dangerous’ practices
  - LogMeIn
  - RDT
  - TeamViewer
  - GoToMeeting
  - VPN Access

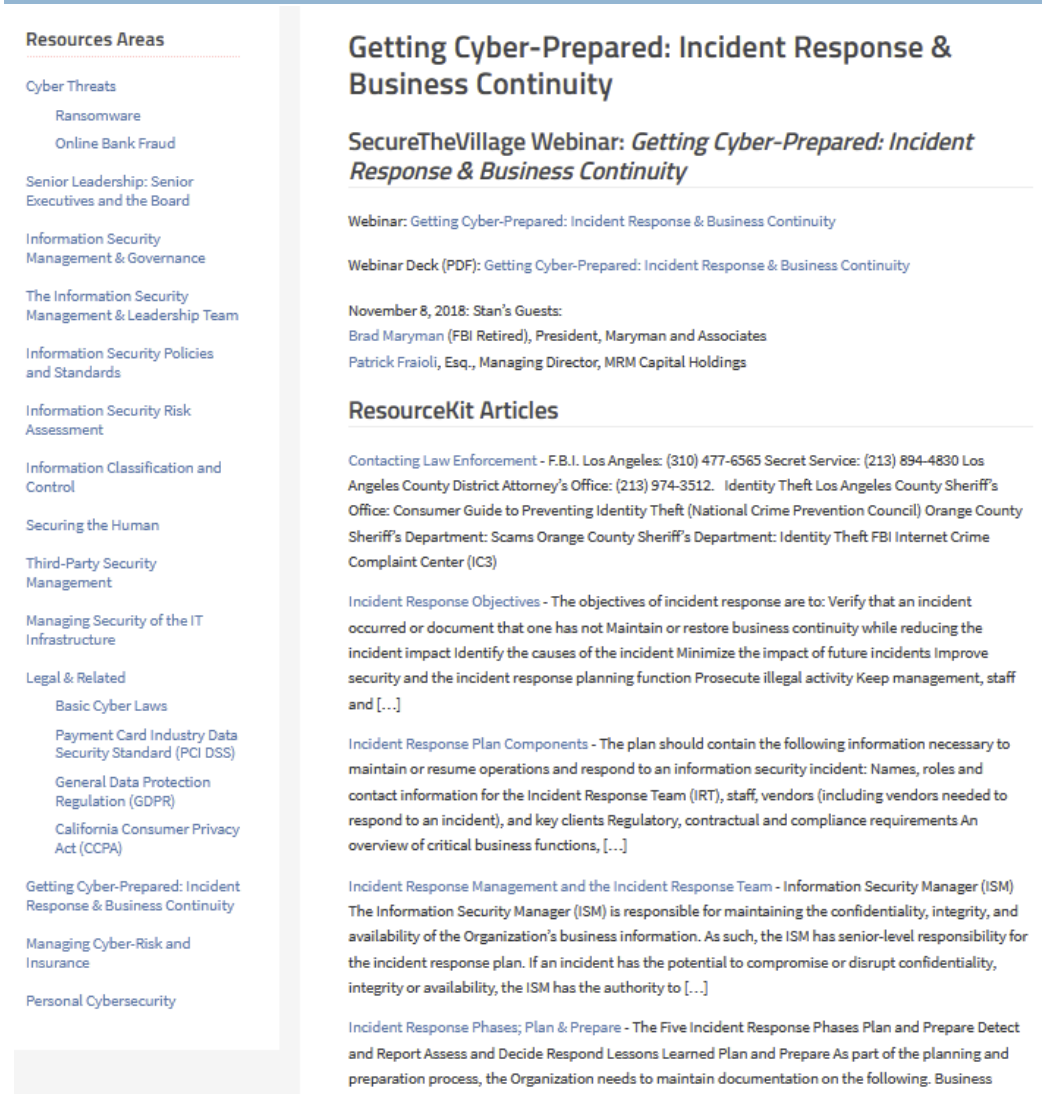
Test Both IT Visibility and Organizational Visibility

- IT Team
  - Information Security Manager
  - CIO, IT Director, IT Vendor
  - Information Security Subject Matter Expertise
  - Computer Forensics / Investigator Subject Matter Expertise
- Full 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

This Month's Assignment

- Conduct an IT test of your Incident Response Plan
  - Ransomware
- Look for holes in visibility
  - How much better could we be if we had visibility into X?
- Get visibility into X
- Update Plan

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



Resources Areas

- Cyber Threats
  - Ransomware
  - Online Bank Fraud
- Senior Leadership: Senior Executives and the Board
- Information Security Management & Governance
- The Information Security Management & Leadership Team
- Information Security Policies and Standards
- Information Security Risk Assessment
- Information Classification and Control
- Securing the Human
- Third-Party Security Management
- Managing Security of the IT Infrastructure
- Legal & Related
  - Basic Cyber Laws
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
  - California Consumer Privacy Act (CCPA)
- Getting Cyber-Prepared: Incident Response & Business Continuity
- Managing Cyber-Risk and Insurance
- Personal Cybersecurity

Getting Cyber-Prepared: Incident Response & Business Continuity

SecureTheVillage Webinar: *Getting Cyber-Prepared: Incident Response & Business Continuity*

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

Webinar Deck (PDF): Getting Cyber-Prepared: Incident Response & Business Continuity

November 8, 2018: Stan's Guests:
Brad Maryman (FBI Retired), President, Maryman and Associates
Patrick Fraioli, Esq., Managing Director, MRM Capital Holdings

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 plan 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, […]

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

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

Next Webinar: November 7

Under Development

Stay Tuned

SecureTheVillage Webinar Series

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

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 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.

Minimum Reasonable Security Practices: A set of information security management practices so basic as to be necessary for a claim that one's information security practices and procedures are reasonable. *Developed in support of CCPA.*

Community-Based Programs: 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*

Register at SecureTheVillage.org

I hear and I forget. I see and I remember. I do and I understand. … Confucius

PEPPERDINE | GRAZIADIO BUSINESS SCHOOL

CyRP

CITADEL
INFORMATION GROUP, INC.

Cybersecure SoCal 2019
Cybersecurity is a Team Sport.
Building a Winning Cybersecurity Team

… a joint presentation of SecureTheVillage and Pepperdine Graziadio Business School

Keynote Speaker: Ron Ross
Fellow at National Institute of Standards and Technology

October 17, 2019 … Mark Your Calendars

For More Information …

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

Joe Greenfield, Managing Director & Chief Forensic Examiner, Maryman & Associates; Associate Professor, USC Viterbi
jgreenfield@maryman.com
805-522-2264

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

Interested in Cybersecurity? Please Get Involved!!!

Follow SecureTheVillage on LinkedIn
https://www.linkedin.com/company/secure-the-village

Attend an Event
https://securethevillage.org/events/

Join the SecureTheVillage Leadership Council
https://securethevillage.org/about/leadership-council/
https://securethevillage.org/about/leadership-council-faq/

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

Thank You

Securing the Network—Lessons Learned From Cyber Investigations
October 2019