RSAConference2015
San Francisco | April 20-24 | Moscone Center


SESSION ID: CXO-F03

# Wargaming for the Boardroom: How to Have a Successful Tabletop Exercise

**Serge Jorgensen**
Chief Technology Officer
The Sylint Group
sdj@usinfosec.com

**David Navetta**
Partner, Co-Chair, Data Protection, Privacy & Access to Information, United States
Norton Rose Fulbright LLP
@davidnavetta

# Mechanics of Wargaming for the Boardroom

- Three Separate Sessions
  - Each session at a different portion of scenario flow
  - Different sets of participants in each session
  - Key to keeping discussion focused and relevant to audience
- Specific Goals Attached to Each Session
  - Goals drive more detailed learning objectives
  - Facilitators ensure all learning objectives addressed
- Direction of Guided Discussion Organization Specific
  - Encourage free flow of potential organization course of action or options
  - Be prepared to provide additional scenario details, when asked (learning objective)
  - Intervene in discussions if learning objective achieved and productivity level starts to decrease
- Take detailed notes/recording for debrief/review purposes

# Ready…Set…Go!

- FBI Special Agent calls organization's legal department to inform their General Counsel of a potential cyber security issue involving the organization.
- FBI requests a confidential meeting with CEO, and whomever else appropriate, that afternoon. FBI requests someone knowledgeable of the organization's sensitive data be available
- CEO begins Pepto-Bismol regimen & decides to invite CIO to initial meeting

# WG Session 1: FBI Notification

- **Scenario**: At initial meeting, FBI informs the group of a potential data leak involving sensitive government, commercial client and internal documents. FBI believes the documents were exfiltrated from your organization. CIO confirms the documents in FBI possession are documents that were being held by and/or originated from the organization.

- **Primary Training Audience**: Senior Management, Legal department, and Public Relations team

# Session 1: FBI Notifies Organization of Breach

- **Goal Focus:** Lines of Authority / Roles & Identification of external interaction
- **Minimum Items/Questions that Target Audience Should Address**
  - Intelligence Collection
  - Investigative Cooperation or Guidance
  - Known/Suspected Identity & Goals of Attackers
  - Potential adversary course(s) of action (CoA)
  - Communication Methods
- **Desired Learning Objectives**
  - Understand law enforcement role/interaction
  - Postulate threat intentions
  - Initiate IR with Senior Management initial direction

# Session 2: IR Team Activated & Begins Investigation



- **Scenario:** FBI meeting concludes and Senior Management informs IT Director to active IR Team. Team assembles and is given Senior Management initial direction and guidance. IR Team creates an initial plan of action and begins investigative process using FBI documents as an initial starting point

- **Primary Audience:** IR Team

# Session 2: IR Team Activated & Begins Investigation



**Goal Focus** Preparedness; Awareness of Gaps & Identification of external interaction

## Minimum Items/Questions that Target Audience Should Address

- Contact groups, numbers & methods
- Playbook development
- Business operations vs. remediation
- Data Repository location identifications (and maintenance)
- Protective measures currently in place & tracking of potential indications of compromise
- Role of any business associates in IR team

## Desired Learning Objectives

- Verify current IR Plan (modify as required)
- Understand concept of IR plan & playbook
- Address potential conflict with business operational vs IR actions
- Improve organization's knowledge and awareness of sensitive data
- Identify 3rd party business associate interaction and initiate coordination
- Address importance of evidence/forensic collection versus remediation pressure

# Session 3: Review Organization's Response

- **Scenario:** IR Team verifies potential threat COA (threat entered into network via a spear-phishing email, compromised CIO credentials accessed specific documents relating to sensitive government contract and exfiltrated via FTP) and begins remediation actions. IR Team briefs Senior Management of technical response activity and progress. Senior Management discusses notification plan of action.
- **Primary Audience:** Senior Management, Legal Department, Public Relations Department & IR Team

# Session 3: Review Organization's Response

- **Goal Focus:** Lines of Authority, Preparedness; Awareness of Gaps & Identification of external interaction
- **Minimum Items/Questions that Target Audience Should Address:**
  - Address potential threat entry & exfiltration methodology
  - Identify why the organization failed to recognize threat
  - Probability of its continued threat presence
  - Follow-on vigilance plan of action
  - Potential impact on business operations and any potential mitigation actions
  - Address PR preparedness
  - Address Legal & Regulatory requirements
- **Learning Objectives:**
  - Increase awareness of the scope of technical remediation plan of action
  - Increase awareness of the notification plan execution

# Review: Get The Right Team

- **Strategic View** (Executives)
- **Operational View** (Internal and External Technical Expertise)
- **Legal View** (Internal and External)
- **External Communications View** (Internal and External Expertise)
- **Financial View** (Internal and Insurance Provider)

# Review: Grasp What Matters Before Crisis

- Know questions to ask
- Understand the potential effects of plans and procedures
- Have established partner/expertise connections
- Understand and appreciate the approach and viewpoints regarding a cyber incident of other divisions within your organization

# Wargaming Goals

- **Goal #1: Understand Lines of Authority and Roles**
  - Responsibility
  - Organizational view/approach to cyber incidents
  - Communication
- **Goal #2: Increase Preparedness**
  - Understand effects of plans and procedures
  - Create level of confidence and prevent future panic
- **Goal #3: Increase Awareness of Gaps and Vulnerabilities**
  - Investigative Capabilities
  - Detection & Reporting (Process & Communication)
  - Vendor management
  - Security Awareness buy-in and commitment of resources
- **Goal #4: Identify Points of External Interaction**
  - Individuals
  - Agencies
  - Press & Social Media
  - Vendors

# Exercise Takeaways

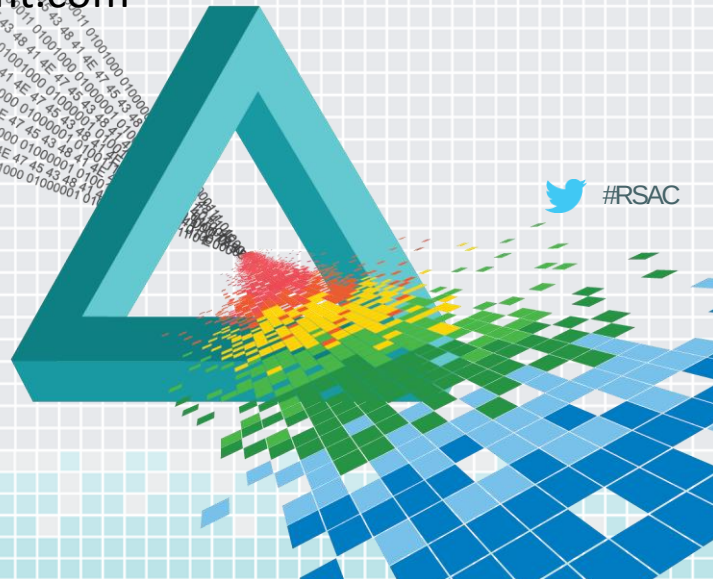
- Why
  - Involve cross-silo segments, including internal & external sources
  - Allow focused development of a cyber-security response playbook
  - Demonstrate increased security maturity

- How
  - Pick a scenario
  - Start to play
  - Take some notes

# Q & A

David Navetta
**Norton Rose Fulbright US LLP**
david.navetta@nortonrosefulbright.com
+1.303.801.2732

Serge Jorgensen
**Sylint Group**
sdj@usinfosec.com
+1.941.951.6015



# Alternate Scenarios

Scenario A: Stolen Documents

- On a Monday morning, the organization's legal department receives a call from the Federal Bureau of Investigation (FBI) regarding some suspicious activity involving the organization's systems. Later that day, an FBI agent meets with members of management and the legal department to discuss the activity. The FBI has been investigating activity involving public posting of sensitive government documents, and some of the documents reportedly belong to the organization. (Client / Partner / Internal information)

Scenario B: Compromised Database Server

- On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator suspects that the server has been attacked and calls for guidance. (The team's investigation determines that the attacker successfully gained root access to the server four months ago).

Scenario C: Unknown Exfiltration

- On a Sunday night, one of the organization's network intrusion detection sensors alerts on anomalous outbound network activity involving large file transfers. The intrusion analyst reviews the alerts; it appears that thousands of .RAR files are being copied from an internal host to an external host, and the external host is located in another country. (The IR team is unable to see what the .RAR files hold because their contents are encrypted. Analysis of the internal host containing the .RAR files shows signs of a RAT installation.)

# Alternate Scenarios

Scenario D: Unauthorized Access to Payroll Records

- On a Wednesday evening, the organization's physical security team receives a call from a payroll administrator who saw an unknown person leave her office and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved.

Scenario E: Disappearing Host

- On a Thursday afternoon, a network intrusion detection sensor records vulnerability scanning activity directed at internal hosts that is being generated by an internal IP address. Because the intrusion detection analyst is unaware of any authorized, scheduled vulnerability scanning activity, she reports the activity to her supervisor. (Activity stops and that there is no longer a host using the IP address).

Scenario F: Telecommuting Compromise

- On a Saturday night, network intrusion detection software records an inbound connection originating from a watchlist IP address. The intrusion detection analyst determines that the connection is being made to the organization's VPN server and contacts his supervisor. (The IR team reviews the intrusion detection, firewall, and VPN server logs and identifies the user ID that was authenticated for the session and the name of the user associated with the user ID)

# Alternate Scenarios

Scenario G: Peer-to-Peer File Sharing

- The organization prohibits the use of peer-to-peer file sharing services. The organization's network intrusion detection sensors have signatures enabled that can detect the usage of several popular peer-to-peer file sharing services. On a Monday evening, an intrusion detection analyst notices that several file sharing alerts have occurred during the past three hours, all involving the same internal IP address.

Scenario H: Unknown Wireless Access Point

- On a Monday morning, the organization's help desk receives calls from three users on the same floor of a building who state that they are having problems with their wireless access. A network administrator who is asked to assist in resolving the problem brings a laptop with wireless access to the users' floor. As he views his wireless networking configuration, he notices that there is a new access point listed as being available. He checks with his teammates and determines that this access point was not deployed by his team.