WOLF & COMPANY, P.C.

Incident Response on a Budget
New England HIMSS 2017

Baseline Knowledge

- What is an Incident Response Plan?
- Why do we need to create and manage another document?
- What are the management phases of IRP?

Section One

WHAT IS IT?

Definitions

- “An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.” - NIST SP 800-53r4 *Security and Privacy Controls for Federal Information Systems and Organizations*

- “A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” - NIST SP 800-61r2 *Computer Security Incident Handling Guide*

Section Two

WHY DO WE NEED IT?

Legal and Regulatory Implications

- HIPAA Security Rule 164.08(a)(6) – *Security Incident Procedures – Response and Reporting*
  - Requires formal documentation

- OCR "Wall of Shame"
  - Encourages a functional response plan
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

Best Practice

- CIS CSC #19 *Incident Response and Management*
- *NIST SP 800-53r4* Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-61r2 Computer Security Incident Handling Guide

2016 Verizon DBIR

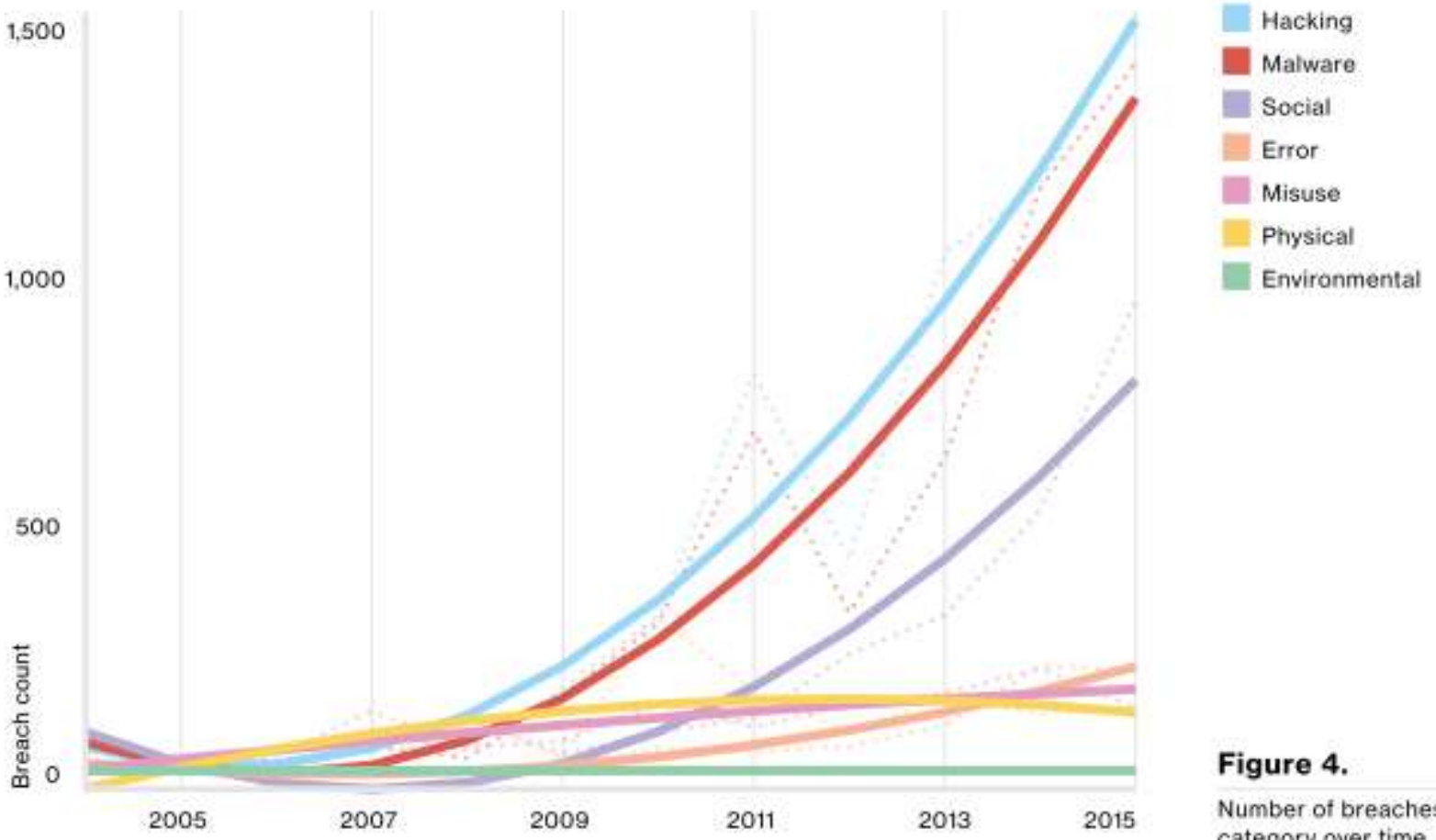


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

2016 Verizon DBIR

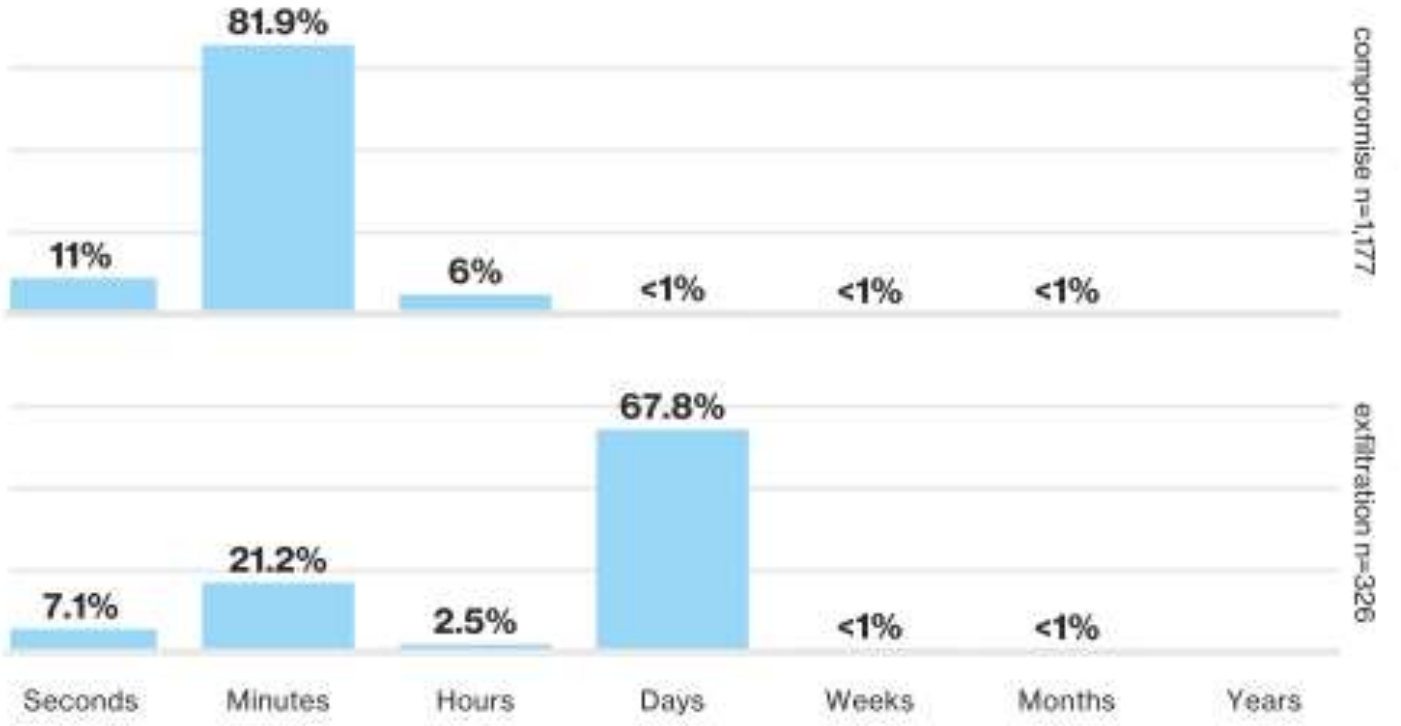


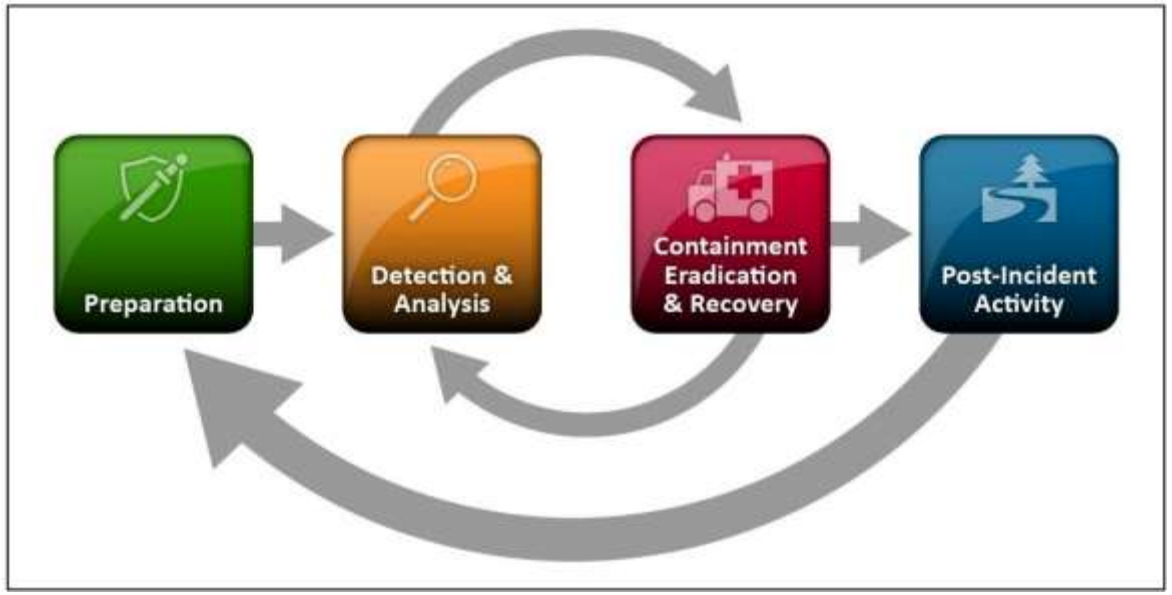
Figure 7.

Time to compromise and exfiltration.

Section Three

WHAT ARE THE PHASES?

Phase One: Preparation



Management Phases

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident

Phase One: Preparation

- Incident Handling Team
  - Incident Response Manager
  - Security Analysts
  - Triage Analysts
  - Forensic Analysts
  - Threat Researchers
  - Management
  - Human Resources
  - Audit and Risk Management Specialists
  - General Council
  - Public Relations

Phase One: Preparation

- Preparing to handle incidents
  - Communication
  - Hardware and Software
  - Analysis
- Preventing incidents
  - Risk Assessments
  - Host Security
  - Network Security
  - Malware Prevention
  - User Awareness and Training

Phase Two: Detection and Analysis

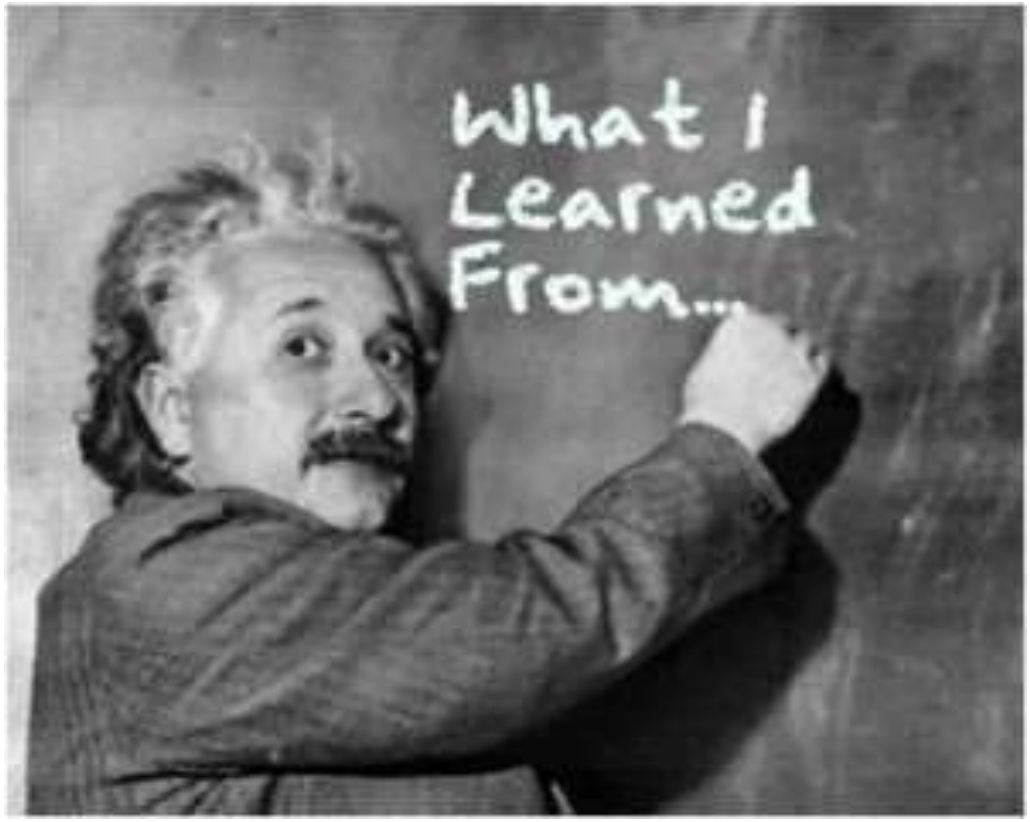
- Attack Vectors
- Signs of an Incident
- Sources of Precursors and Indicators
- Incident Analysis
- Incident Documentation

Phase Three: Containment, Eradication, and Recovery

- Choosing a Containment Strategy
- Evidence Gathering and Handling
- Identifying the Attacking Hosts
- Eradication and Recovery

Phase Four: Post-Incident

- Lessons Learned
- Using Collected Incident Data
- Evidence Retention



THEORY IS GREAT… HOW ABOUT IN THE REAL WORLD??

Malware Infection

On Tuesday afternoon around 16:30, an end user in the Marketing department gets a warning from the anti-virus engine saying a potentially malicious file has been identified. At the same time, this end user notices the files on her desktop wont open, and a webpage (.html file) has opened demanding a ransom for the safe return of her files.

Real World

1. Who does the Help Desk technician contact?

2. Suppose upon isolation of this PC, additional users in various departments are reporting similar issues. What steps would be taken to identify the full scope?

3. Suppose this occurs after hours, rather than during normal business hours. How would end users report such an issue?

Phishing Email

On Tuesday morning after a long weekend a member of the Finance department is quacking running through missed emails trying to identify any major activities while he was out. He sees an email from the head of IT saying that the organization had found some users were using weak passwords, and had created a site on the Intranet for users to ensure their password would meet the new requirements. The Finance employee clicks the link provided and enters his credentials. He lets out a sigh of release when he is shown that his password is very strong, and there is no need for him to create a new one.

Real World

1. How would this event be detected?
2. How would the IRP team identify all effected end users?
3. How would the IRP resolve this incident?
4. Suppose this user was working remotely when this happened, does that change response activities? What if multiple executives are traveling?

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, run down the hallway, 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. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

Real World

1. How would the team determine what actions had been performed?

2. How would the handling of this incident differ if the payroll administrator had recognized the person leaving her office as a former payroll department employee?

3. How would the handling of this incident differ if the team had reason to believe that the person was a current employee?

4. How would the handling of this incident differ if the physical security team determined that the person had used social engineering techniques to gain physical access to the building?

Real World

5. How would the handling of this incident differ if logs from the previous week showed an unusually large number of failed remote login attempts using the payroll administrator's user ID?

6. How would the handling of this incident differ if the incident response team discovered that a keystroke logger was installed on the computer two weeks earlier?

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 the incident response team. The 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.

WOLF & COMPANY, P.C.

Real World

1. What should the team's next step be (e.g., calling the user at home, disabling the user ID, disconnecting the VPN session)? Why should this step be performed first? What step should be performed second?

2. How would the handling of this incident differ if the external IP address belonged to an open proxy?

3. How would the handling of this incident differ if the ID had been used to initiate VPN connections from several external IP addresses without the knowledge of the user?

Real World

4. Suppose that the identified user's computer had become compromised by a game containing a Trojan horse that was downloaded by a family member. How would this affect the team's analysis of the incident? How would this affect evidence gathering and handling? What should the team do in terms of eradicating the incident from the user's computer?

5. Suppose that the user installed antivirus software and determined that the Trojan horse had included a keystroke logger. How would this affect the handling of the incident? How would this affect the handling of the incident if the user were a system administrator? How would this affect the handling of the incident if the user were a high-ranking executive in the organization?

Questions?

Michael Keighley, CISSP
Manager of Information Security
MaineGeneral Health
michael.keighley@mainegeneral.org

Michael Kanarellis, HITRUST CCSFP
IT Assurance Senior Manager
Mkanarellis@wolfandco.com

Sean D. Goodwin, CISSP, CISA, QSA
IT Assurance Senior Consultant
SDGoodwin@wolfandco.com