BISHOP FOX

# Developing and Testing an Effective Incident Response Program

ANDY JORDAN – SECURITY ASSOCIATE


May 6, 2016

# What You Will Learn?

OUTCOMES

1. The difference between typical IT incidents and security incidents

2. How to prepare and improve your company’s Security Incident Response Plan

3. Tips and tricks to make it through common incidents affecting real world organizations

# What is an incident?

# IT Incident vs. Security Incident

YES, THERE'S A DIFFERENCE

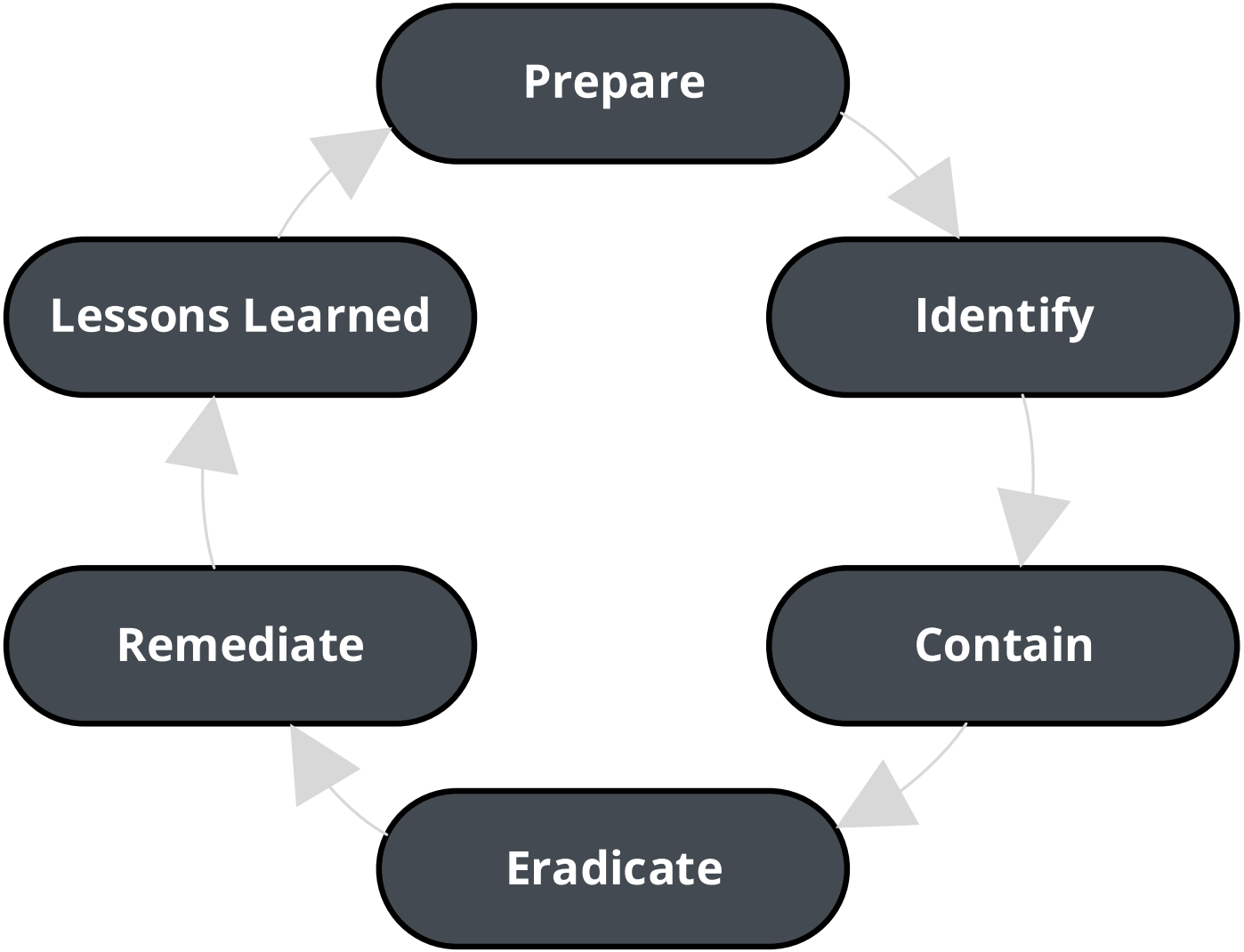
| IT Incident | Security Incident |
| --- | --- |
| Related to systems or services | Related to systems, services, users, or information |
| Defined by device criticality | Defined by malicious intent |
| Any IT service degradation or outage | Can impact the organization's users, reputation, intellectual property, or assets |

# How long does it take to resolve a security incident?

**You cannot solve a security incident within a defined time frame.**

# Security Incident Response Process Flow

THE BIG PICTURE



# Preparation

CREATING YOUR PLAN

- Do you have permission to monitor the organization?
- Have you leveraged other process to support your Security Incident Response Plan?
- Do you have the right visibility to what is happening in your environment?
- How are you providing security awareness to your users?

# Containment and Eradication

CREATING YOUR PLAN

- Who is your Incident Commander?
- Have you documented your investigation steps?
- What is Chain of Custody?

# Remediation and Lessons Learned

CREATING YOUR PLAN

- Were you able to close down other attack vectors?
- What improvements can you make to the plan?
- What types of security awareness can be communicated to the organization?

# IR Plans and Tabletops and Templates...Oh My!

IMPROVING YOUR SECURITY INCIDENT RESPONSE PLAN

## Make changes and updates

- Defined process to perform containment actions
- "Lessons learned" debrief to continually improve your plan

## Perform incident tabletop exercises

- Start with DDOS, malicious software, and breach notification scenarios
- Coordinate with other organizational teams

## Develop communication templates

- Holding statements while you gather more information
- Polished response while under fire

# Measuring Incident Response Effectiveness



## Were you able to correlate events with your logs?

- Visibility matrix of systems which are logging as expected

## Did internal teams communicate effectively?

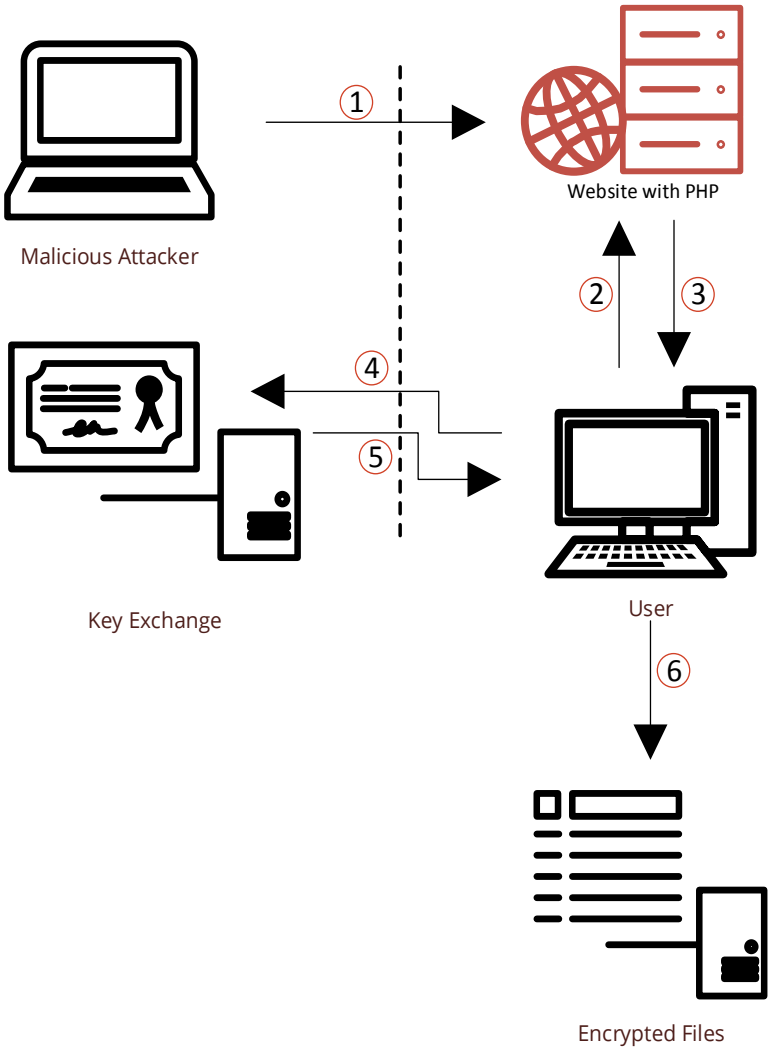
- HR
- Legal
- Compliance

## Did you make the right (emotional) decision?

- Information overload
- Pay or fight

# Ransomware

REAL WORLD INCIDENTS




1. Attacker compromises website
2. User visits compromised website
3. Malicious file is downloaded to machine
4. Malicious file contacts attacker's CnC
5. CnC encryption key is synchronized on machine
6. Malware encrypts files and leaves contact info

# Ransomware Incident Timeline

REAL WORLD INCIDENTS

1. Antivirus triggered on encrypted files within two Domain Controllers
2. Restored GPO files
3. Determined point of impact via internal research
4. Conducted threat intelligence research
5. Searched network storage for extension files
6. Correlated file creation with originating machine
7. Contacted business support team
8. Removed device from the network

# Three Key Takeaways



1. Your Security Incident Response Plan needs to be supported, reviewed, and used by the entire organization

2. Preparation and continual refinement will ensure your Security Incident Response Plan evolves with your organization

3. Use tabletop exercises to test your plan

# Thank You

BISHOP FOX®