

Tabletop Session



Patterson Cake

Director of Incident Response
Black Hills Information
Security



Ben Wilkens

Director of Cybersecurity
NMFTA

TACTICAL IR PLAN

Ruthless Prioritization & Allocation of Resources

“Your technical controls failed...”

- Kill Ingress/Egress
- Isolated Impacted Endpoints
- Kill Authenticated Sessions & Rotate All Credentials
- Identify Indicators of Compromise [IOCs]
- Configure Technical Controls to Contain/Eradicate IOCs
- Validate...Restore/Return to Production
- Be VIGILANT

...REPEAT AS NEEDED...

Interpersonal, Workflow & Collaborative Priorities

- Stay Calm
- Focus/Re-Focus on PRIORITY #1
- Directly Assign/Monitor Tasks
- Validate ALL Responsive Actions
- Start with EFFECTIVE (Simple/Expedient)
- Document EVERYTHING

..."who is in charge?"...

Critical Recuring QUESTIONS

"What have we completed so far?"

"Are you sure?"

"What are we working on right now?"

"What is our next priority?"

<https://git.new/simple-ir-plan>

The **MOST** Important IR Playbooks...

- Ingress/Egress
- Isolation
- Authentication

P1: Ingress/Egress (C2)

Disconnect the Internet [“deny” everything]:

- Create/Test a Granular Plan [technical how-to]*
- Pre-Define Business Critical Sites & Services [“allow” list]*

*[...Define/Document Criteria & Authority...]

P2: Isolation

Network Isolate Endpoints:

- Create/Test a Granular Plan [technical how-to]*
- Pre-Define Tiers of Criticality [laptop vs server]*

..."out of an abundance of caution"...

*[...Define/Document Criteria & Authority...]

P3: Authentication

Disconnect Authenticated Sessions/Rotate **ALL** Passwords:

- Create/Test a Granular Plan [technical how-to]*
- Prioritize Accounts [Domain Admin...Global Admin...Server Admin...]*

..."don't forget non-AD/Entra integrated accounts"...

*[...Define/Document Criteria & Authority...]

The **MOST** Important IR Playbooks...

- Ingress/Egress
- Isolation
- Authentication

"evict the adversary from the battlefield, proceed with remediation/recovery"

“WOULD YOU RATHER...?”

Incident Response Edition

You are responsible for the **C**onfidentiality, **I**ntegrity, and **A**vailability of your business IT systems, services, and data.

“Would you rather...?”

A. Proactively contemplate difficult incident-response questions in advance of crisis...

- or -

B. ~~Switch conference sessions?~~

NOTE: *It's too late now! I told you you should do this in advance of crisis!*

You've received confirmation of a high-severity malicious software alert on a corporate workstation.

“Would you rather...?”

A. Network isolate all business-critical workstations and servers immediately...

- or -

B. Network isolate just the single workstations and investigate further?

NOTE: *Do you have a tested/documentated method for isolating endpoints?*

You've confirmed a "true positive" security event but are unsure of the depth and breadth of impact.

“Would you rather...?”

A. Wait until you know more before contacting additional resources (insurance, third-party IR retainer, legal counsel, etc.)...

- or -

B. Engage outside resources immediately (insurance, third-party IR retainer, legal counsel, etc.)?

NOTE: *Do you have internal resources capable of this investigation, estimated time to completion?*

You've confirmed unauthorized access to a business-critical server/system.

“Would you rather...?”

A. Review the server/system, attempt to fully eradicate all unauthorized access/activity, and return the server/system to production ASAP (approx. 2 hours downtime)...

- or -

B. Reimage the server/system, restore data from the previous night's backup, and return to production (approx. 8 hours downtime & 12 hours of production data loss)?

NOTE: *Do you have immutable backups? Have you tested and timed restoration?*

You've been informed that an employee's email account (mailbox) was compromised and used to send a Phishing email to employees and customers asking them to "update their account information," requesting sensitive information.

"Would you rather...?"

A. Immediately draft an email notification to all employees and customers, warning them of the malicious email message/s...

- or -

B. Wait approximately 8-10 hours for full email-activity reporting and analysis to identify specific employees and customers to notify?

NOTE: *Do you have internal resources capable of this investigation, estimated time to completion?*

You have strong suspicion that an employee stole company property and possibly embezzled money.

“Would you rather...?”

A. Contact law enforcement immediately to report your suspicion and seek assistance...

- or -

B. Perform further internal investigation and/or not involve law enforcement.

NOTE: *Do you have points of contact with local law enforcement and the local FBI field office?*

You've identified unauthorized access to your corporate payroll system and potential exposure of employee personally identifiable information (PII).

“Would you rather...?”

A. Work with internal legal/compliance/HR/security teams to determine next steps...

- or -

B. Engage external legal/security services to determine next steps?

NOTE: *What represents a “reportable incident” and what are the timelines for reporting?*

BACKDOORS & BREACHES

Incident Response TTX Card Game

<https://play.backdoorsandbreaches.com>

- **Introduction**
- **Gameplay**
- **Creating a Scenario**
- **Tips & Tricks for your TTX**

