Falconi® Sports Agency

Tabletop Exercise

Phishing Attack Leads to Data Breach

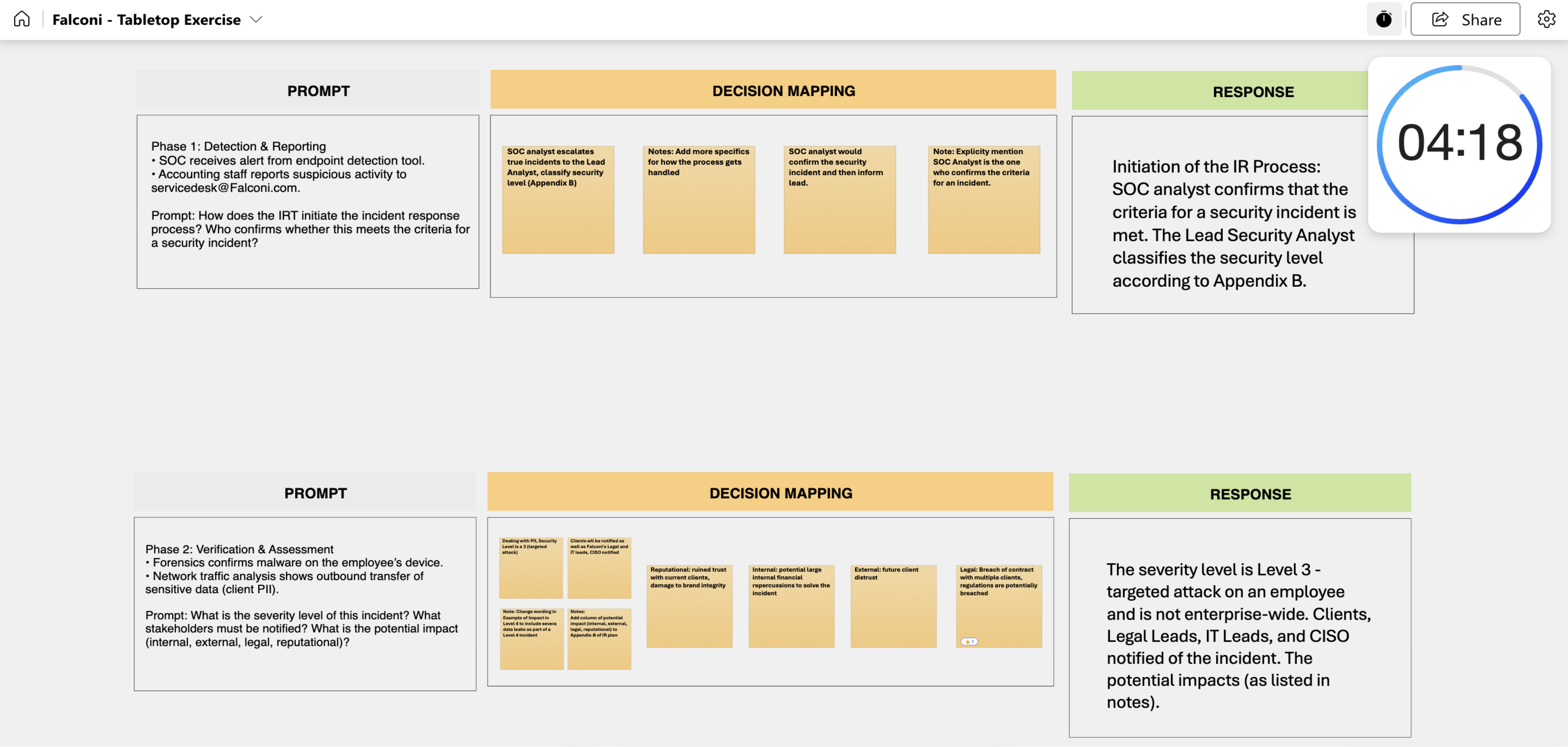
Presented by: Incident Response Team

In collaboration with: Risk Management and Cyber Essentials Teams

Introduction

- We conducted a Tabletop exercise based on a phishing attack
- Roles were assigned to interns:
  - Julia - IR Manager / Tabletop Leader / Participant
  - John, Aaron – Notetakers / Whiteboard Managers / Participants
  - Cyber Essentials + Risk Management Teams – Participants
- We worked through 5 phases of Incident Response
  - 8 minutes per phase

Whiteboard Mapping



PROMPT

Phase 1: Detection & Reporting
- SOC receives alert from endpoint detection tool.
- Accounting staff reports suspicious activity to servicedesk@Falconi.com.

Prompt: How does the IRT initiate the incident response process? Who confirms whether this meets the criteria for a security incident?

DECISION MAPPING

SOC analyst escalates true incidents to the Lead Analyst, classify security level (Appendix B)

Notes: Add more specifics for how the process gets handled

SOC analyst would confirm the security incident and then inform lead.

Note: Explicity mention SOC Analyst is the one who confirms the criteria for an incident.

RESPONSE

Initiation of the IR Process: SOC analyst confirms that the criteria for a security incident is met. The Lead Security Analyst classifies the security level according to Appendix B.

PROMPT

Phase 2: Verification & Assessment
- Forensics confirms malware on the employee's device.
- Network traffic analysis shows outbound transfer of sensitive data (client PII).

Prompt: What is the severity level of this incident? What stakeholders must be notified? What is the potential impact (internal, external, legal, reputational)?

DECISION MAPPING

Dealing with PII, Security Level is a 3 (targeted attack)

Clients wll be notified as well as Falconi's Legal and IT leads, CISO notified

Note: Change wording in Example of Impact in Level 4 to include severa data leaks as part of a Level 4 incident

Notes:
Add column of potential impact (internal, external, legal, reputational) to Appendix-B of IR plan

Reputational: ruined trust with current clients, damage to brand integrity

Internal: potential large internal financial repercussions to solve the incident

External: future client distrust

Legal: Breach of contract with multiple clients, regulations are potentially breached

👍 1

RESPONSE

The severity level is Level 3 - targeted attack on an employee and is not enterprise-wide. Clients, Legal Leads, IT Leads, and CISO notified of the incident. The potential impacts (as listed in notes).

Scenario Overview

On a Tuesday morning, an employee in the accounting department reports suspicious activity on their workstation.

After investigation, the SOC detects that the employee clicked a link in a phishing email disguised as a vendor invoice.

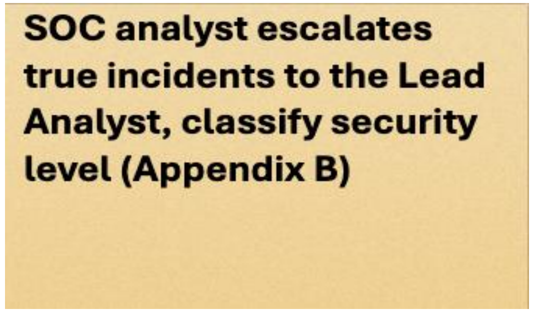
The link installed malware, which allowed the attacker to infiltrate a database containing client PII.

Phase 1 – Detection and Reporting

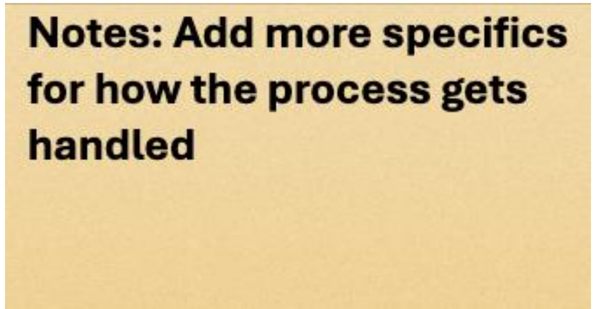
- SOC receives alert from endpoint detection tool.
- Accounting staff reports suspicious activity to servicedesk@Falconi.com.

Prompt: How does the IRT initiate the incident response process? Who confirms whether this meets the criteria for a security incident?

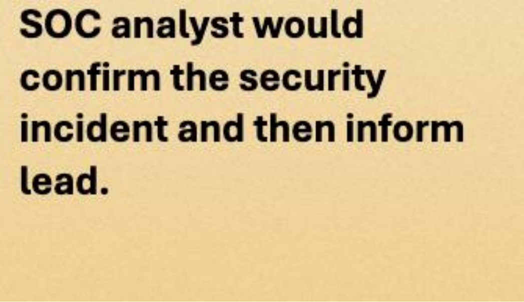
Notes/Concerns:



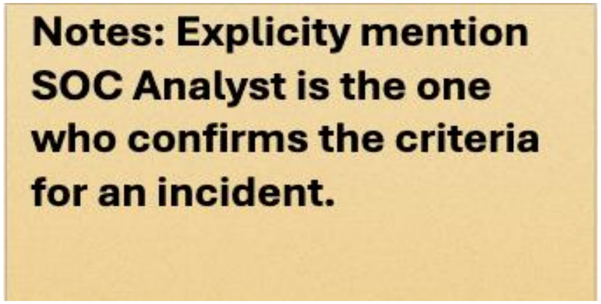
SOC analyst escalates true incidents to the Lead Analyst, classify security level (Appendix B)



Notes: Add more specifics for how the process gets handled



SOC analyst would confirm the security incident and then inform lead.



Notes: Explicity mention SOC Analyst is the one who confirms the criteria for an incident.

Response:

After receiving the alert through the detection tool, the SOC analyst confirms that the criteria for a security incident is met, then escalates it to the Lead Security Analyst. The Lead Security Analyst classifies the security level according to Appendix B.

Areas of Improvement:

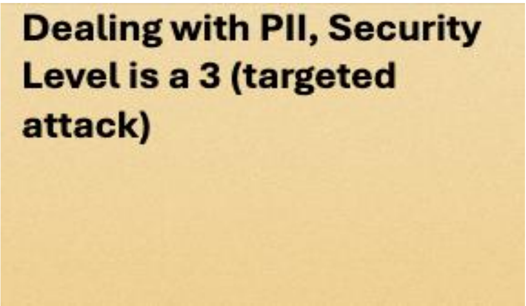
Explicit duties of each role should be specified between SOC Analyst and Lead Analyst when confirming incidents.

Phase 2 – Verification & Assessment

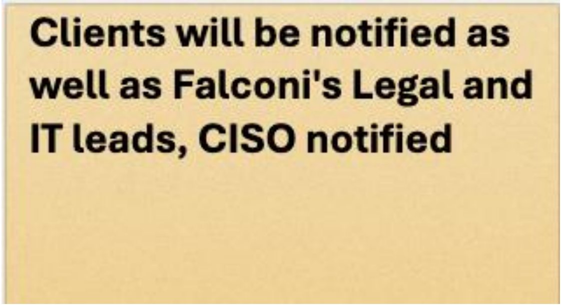
- Forensics confirms malware on the employee’s device.
- Network traffic analysis shows outbound transfer of sensitive data (client PII).

Prompt: What is the severity level of this incident? What stakeholders must be notified? What is the potential impact (internal, external, legal, reputational)?

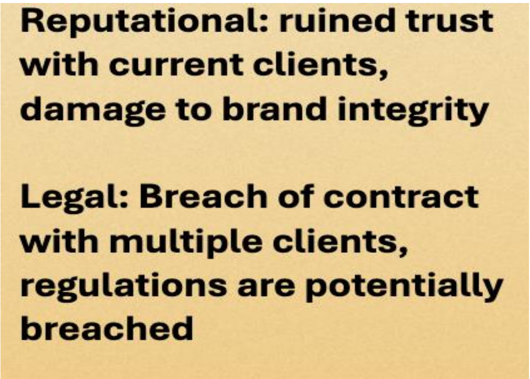
Notes/Concerns:



Dealing with PII, Security Level is a 3 (targeted attack)

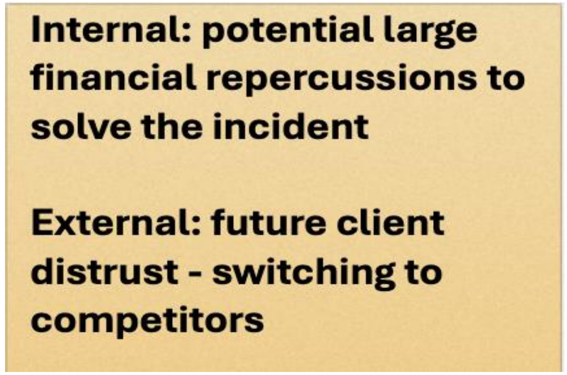


Clients will be notified as well as Falconi's Legal and IT leads, CISO notified



Reputational: ruined trust with current clients, damage to brand integrity

Legal: Breach of contract with multiple clients, regulations are potentially breached



Internal: potential large financial repercussions to solve the incident

External: future client distrust - switching to competitors

Response:

The severity level is Level 3 - targeted attack on an employee and is not enterprise-wide. Clients, Legal Leads, IT Leads, and CISO notified of the incident.

Areas of Improvement:

Change wording in Example of Impact in Level 4 to include several data leaks as part of a Level 4 incident

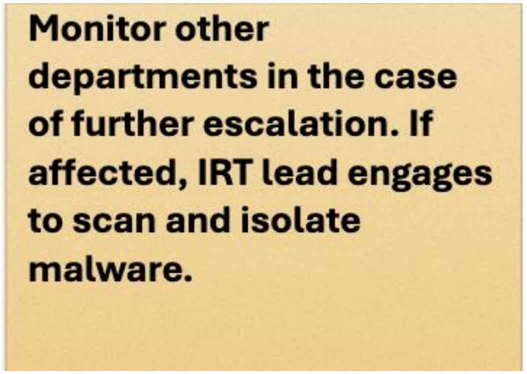
Add column of 'potential impact' to Appendix-B of IR plan

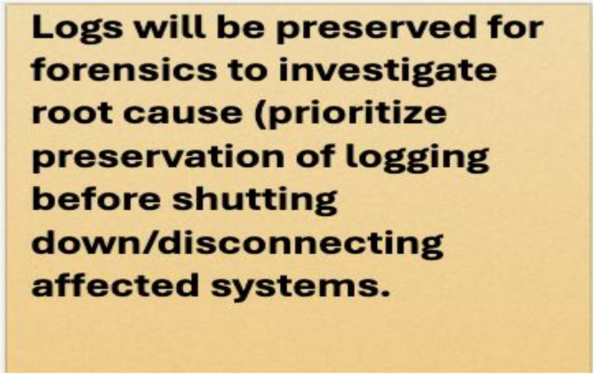
Phase 3 – Containment & Mitigation

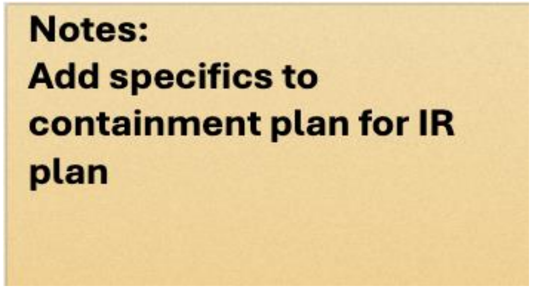
- Malware is active. The attacker may still have access.
- The team considers disconnecting affected systems.

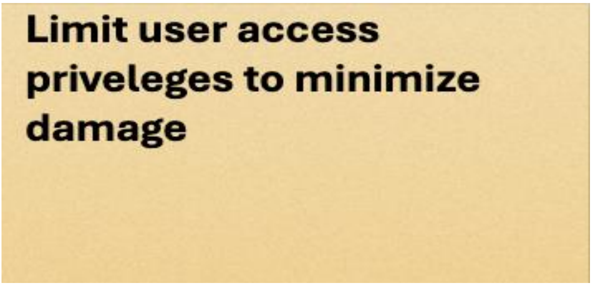
Prompt: What containment steps will be taken? Will any logs be preserved for forensics? Are additional users or systems at risk?

Notes/Concerns:


Monitor other departments in the case of further escalation. If affected, IRT lead engages to scan and isolate malware.


Logs will be preserved for forensics to investigate root cause (prioritize preservation of logging before shutting down/disconnecting affected systems.


Notes:
Add specifics to containment plan for IR plan


Limit user access priveleges to minimize damage

Response:

Steps include: isolating affected systems, preserving logs for forensics to conduct root cause analysis, limiting use access privileges to compromised victims, change passwords for potential systems/users at risk.

Areas of Improvement:

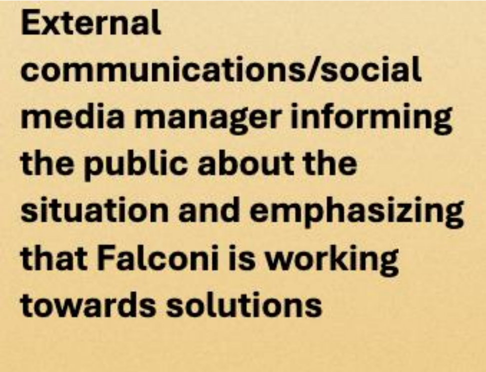
The 'Containment' section of IR Plan should be expanded to include clearer criteria for system isolation and log preservation protocols.

Phase 4 – Communication

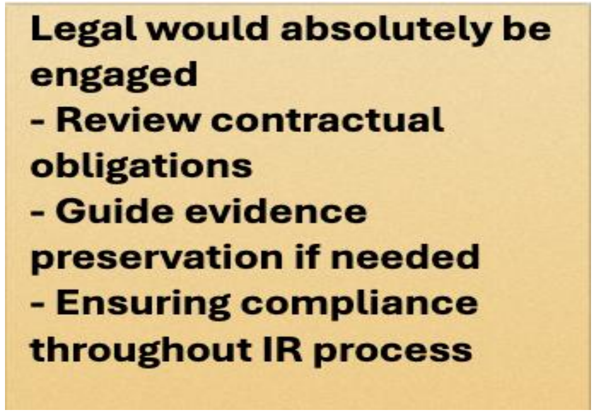
- External media outlets begin speculating on a Falconi data breach
- Clients inquire about suspicious activity on their accounts

Prompt: Who handles internal vs. external communications? What message is released to clients and the media? Has legal been engaged?

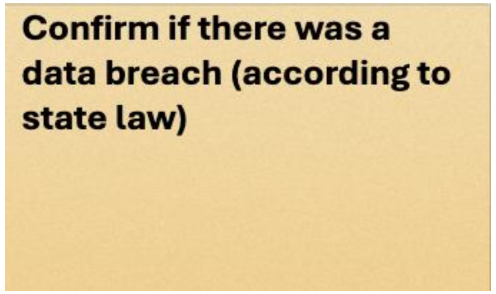
Notes/Concerns:



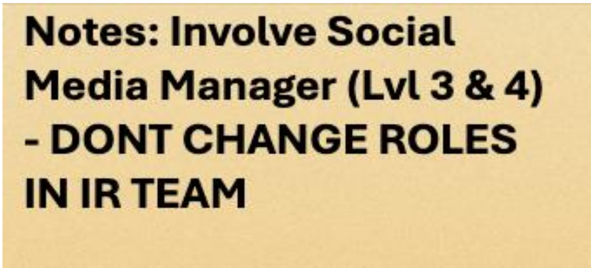
External communications/social media manager informing the public about the situation and emphasizing that Falconi is working towards solutions



Legal would absolutely be engaged
- Review contractual obligations
- Guide evidence preservation if needed
- Ensuring compliance throughout IR process



Confirm if there was a data breach (according to state law)



Notes: Involve Social Media Manager (Lvl 3 & 4)
- DONT CHANGE ROLES IN IR TEAM

Response:

Confirmation of the incident is made by the Head of and External Communications with a press release.

Head of Internal Communications sends a memorandum to all internal employees.

Legal team has been engaged.

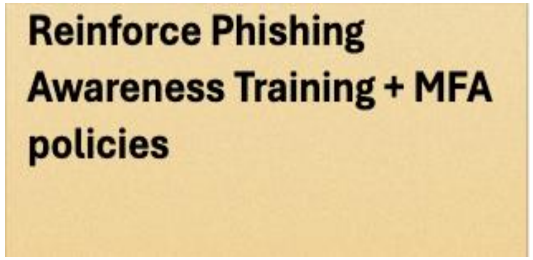
Areas of Improvement:
None

Phase 5 – Post-Breach & Recovery

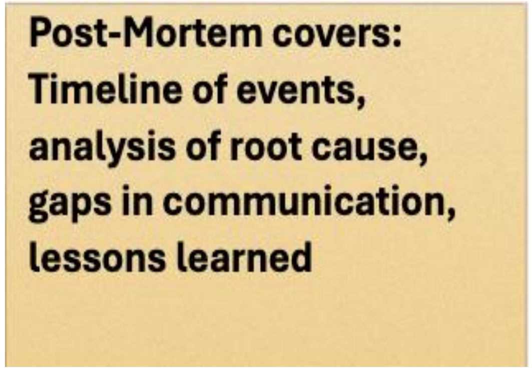
- Systems are restored, and client notification is underway.
- Incident Report and logs are compiled.

Prompt: What corrective actions and policy updates are needed? What would the post-mortem cover? How is this incident documented in Appendix-C format?

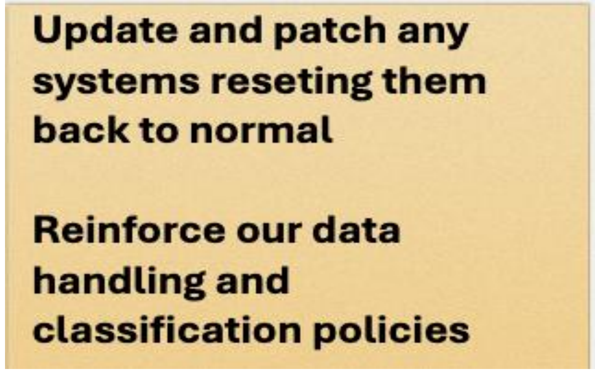
Notes/Concerns:



Reinforce Phishing Awareness Training + MFA policies

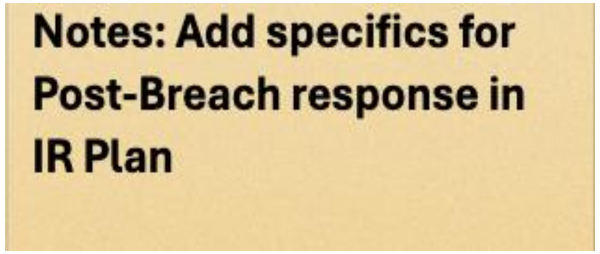


Post-Mortem covers: Timeline of events, analysis of root cause, gaps in communication, lessons learned



Update and patch any systems reseting them back to normal

Reinforce our data handling and classification policies



Notes: Add specifics for Post-Breach response in IR Plan

Response:

Reinforce Phishing Awareness Training & MFA policies. Post-Mortem covers: event timeline, root cause analysis, etc. See incident documentation in Falconi Incident Report Form.

Areas of Improvement:

Add specifics for Post-Breach response in IR Plan.

What Went Well

- All interns came into the exercise prepared and ready to participate.

- Microsoft whiteboard worked as a valuable collaboration tool for all participants.

- Strategy of Thinking out Loud
  - Allowed for all participants to be on the same page
  - Served as jumping off points for others' ideas

- Working through each phase in pieces with a time constraint (8 minutes per phase)
  - Timer kept everyone on task

Lessons Learned

- An IR Plan should have clear wording, with specified procedures, timelines, roles, and responsibilities.
- IR can be stressful and high-stakes so clarity is key.
- While there were some benefits to online (everyone is able to add notes in a centralized location), in-person is preferrable.
- Employee Security Training and Awareness could be the difference between a successful phishing attack and a failed one.

Thank You!

FALCONI

SPORTS AGENCY