CYBER TABLETOP EXERCISE

September 5, 2025

Sharonville Convention Center

11355 Chester Road

Sharonville, Ohio

ERIC ADONTENG

CISM, Network+, SAP-C02, NIST-CSF Cert.

Cyber Risk Service Advisor

THE GOAL

Review the participant's ability to protect, detect, and respond to a cyber incident or breach in a roundtable format discussion. Facilitator will provide a scenario and moderate. Participants will respond to the scenario presented with discussion for mitigation.

CYBER TABLETOP EXERCISE STRUCTURE

Facilitated discussion-based exercise. Participants will discuss three modules.

MODULE 1 & 2

Business Compromise & Patch Management Insider Threat

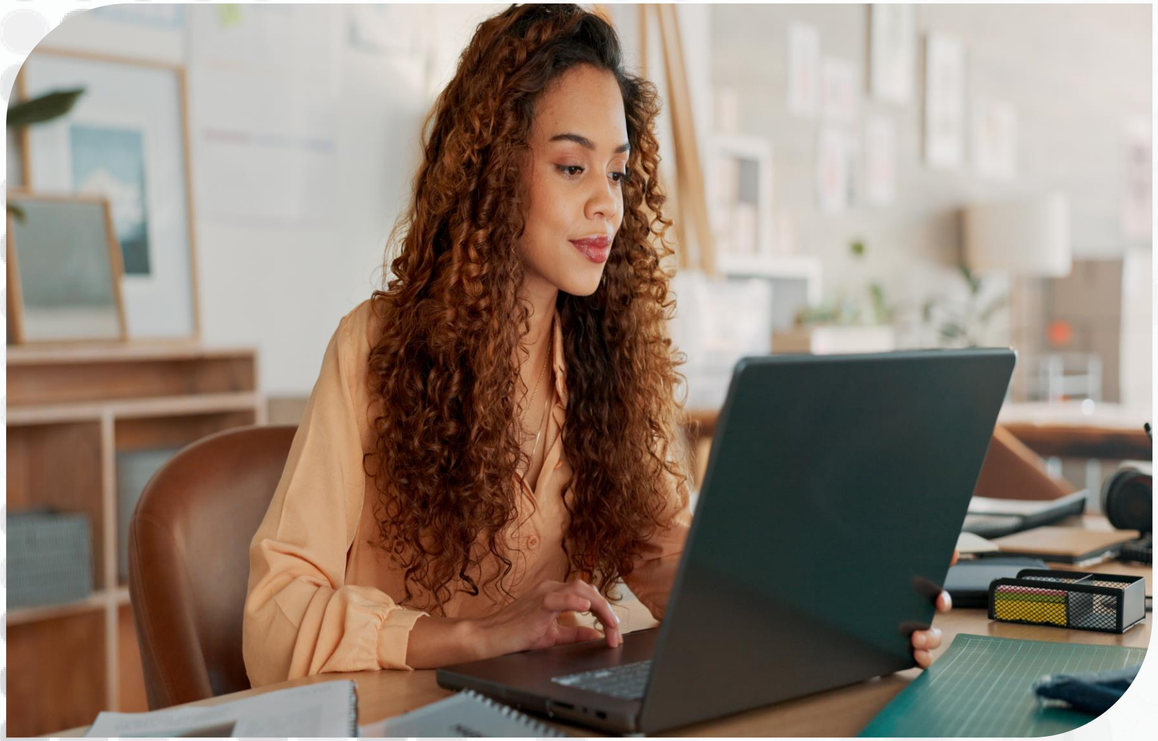
MODULE 3 & 4

Cloud Compromise & Unplanned Hacktivist Attack on Police Department

MODULE 5 & 6+

Ransomware from Phishing & Ransomware

Bonus Modules



AGENDA

CYBER TABLETOP EXERCISE GUIDELINES

1. This is an open, no-fault learning environment. Varying viewpoints are expected and encouraged.
2. Base responses on the plans and processes of your entity.
3. Decisions are not precedent setting. Consider different approaches and improvements.
4. Problem-solving efforts should be the focus of the exercise.

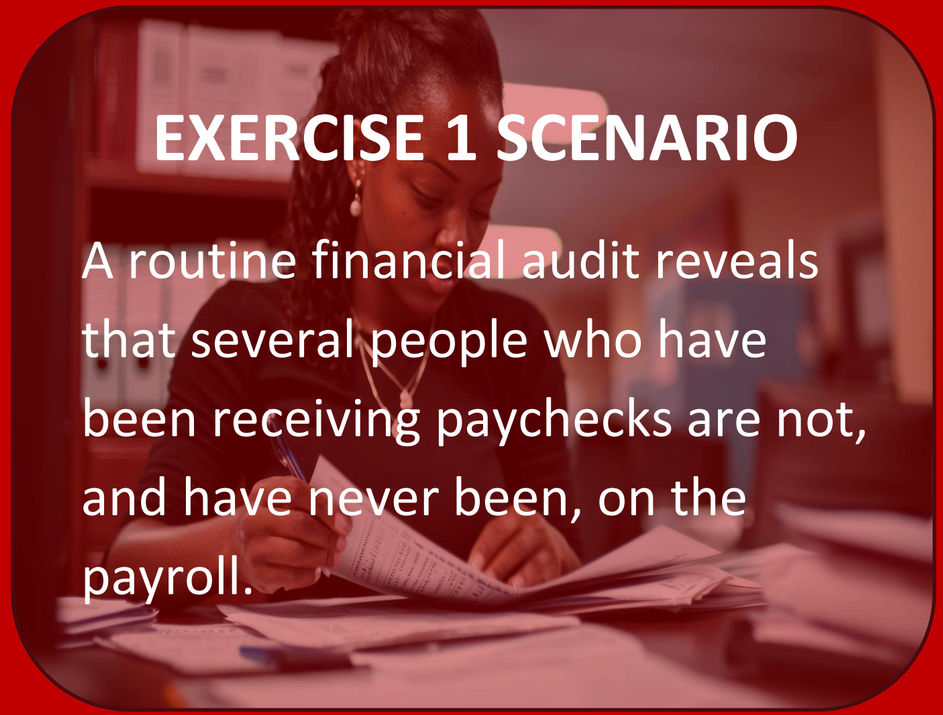
CYBER TABLETOP EXERCISE 1

BUSINESS COMPROMISE

FINANCIAL BREACH

BACKSTORY:

Your school's financial office had a physical break-in resulting in several laptops without sensitive data stolen. AI was used to defeat facial recognition access systems.



FINANCIAL BREACH

BACKSTORY:

Your school's financial office had a physical break-in resulting in several laptops without sensitive data stolen. AI was used to defeat facial recognition access systems.

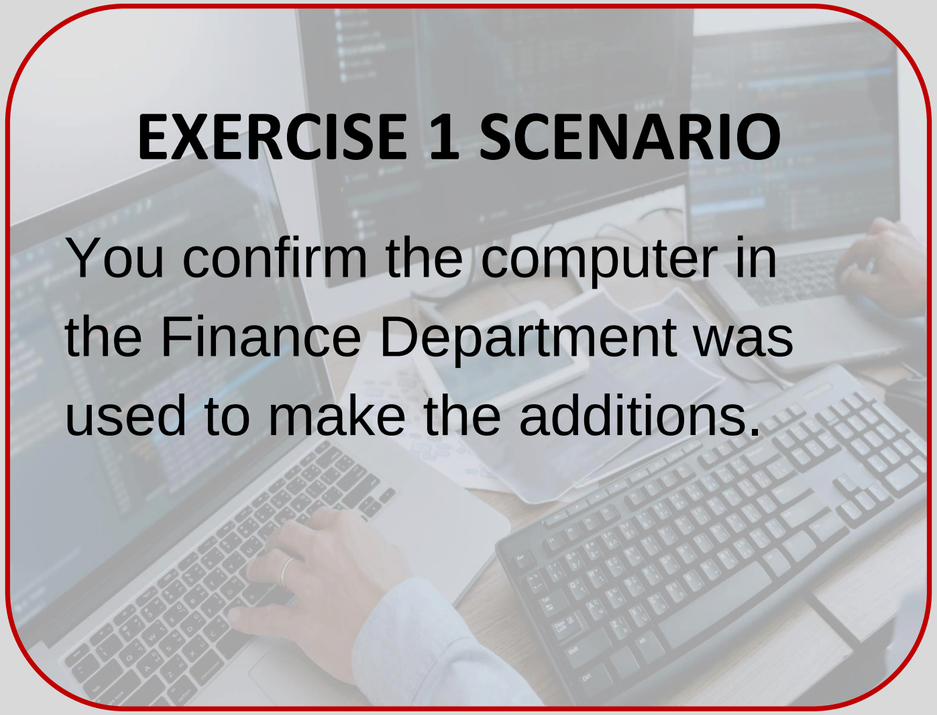
EXERCISE 1 SCENARIO

A system review indicates they were added to the payroll approximately one month prior, at the same time, on a computer in the Finance Department.

FINANCIAL BREACH

BACKSTORY:

Your school's financial office had a physical break-in resulting in several laptops without sensitive data stolen. AI was used to defeat facial recognition access systems.



EXERCISE 1 SCENARIO

You confirm the computer in the Finance Department was used to make the additions.

FINANCIAL BREACH

BACKSTORY:

Your school's financial office had a physical break-in resulting in several laptops without sensitive data stolen. AI was used to defeat facial recognition access systems.

EXERCISE 1 SCENARIO

Further review indicates that all employees have been paying a new fee of $20 each paycheck and that money is being siphoned to an off-shore account.

FINANCIAL BREACH

BACKSTORY:

Your school's financial office had a physical break-in resulting in several laptops without sensitive data stolen. AI was used to defeat facial recognition access systems.

CYBER TABLETOP EXERCISE

FINANCIAL BREAK-IN AND BREACH

Question 1:
What actions should you take after a break-in?

Question 2:
Are you able to audit your physical security system?

Question 3:
Who should be notified?

Question 4:
What credentials were stored on the laptop?

Question 5:
How do you notify employees of the incident?

Question 6:
How do you compensate the company employees?

CYBER TABLETOP EXERCISE 2

Idäify Patch & Vulrzability
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Perform Impact Analysis
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Pilot Patch
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Review & Report
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Assess Risk Of Vulnerability
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Test Patch
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Roll Out Patch
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Patch Rest Of Devices
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

PATCH MANAGEMENT INSIDER THREAT

INSIDER THREAT

BACKSTORY:

You're a school network administrator who is overworked, underfunded, and underpaid. Legislation affected property taxes causing underfunding of the budgets.

EXERCISE 2 SCENARIO

Joe, your network administrator, is overworked and underpaid. His bags are packed and ready for a family vacation to Disney World when he is tasked with deploying a critical patch. In order to make his flight, Joe quickly builds an installation file for the patch using Generative AI and deploys it before leaving for his trip.

EXERCISE 2 SCENARIO

Next, Sue, the on-call network service technician, begins receiving calls that nobody can log in. It turns out that no testing was done for the recently installed critical patch.

CYBER TABLETOP EXERCISE

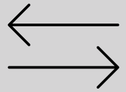
INSIDER THREAT

Question 1:

Does Sue have the expertise to handle the incident?

Question 2:

If not, are there defined escalation processes?

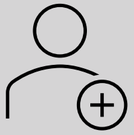


Question 3:

Do you have a formal change control policy?

Question 4:

Are your employees trained on change control?



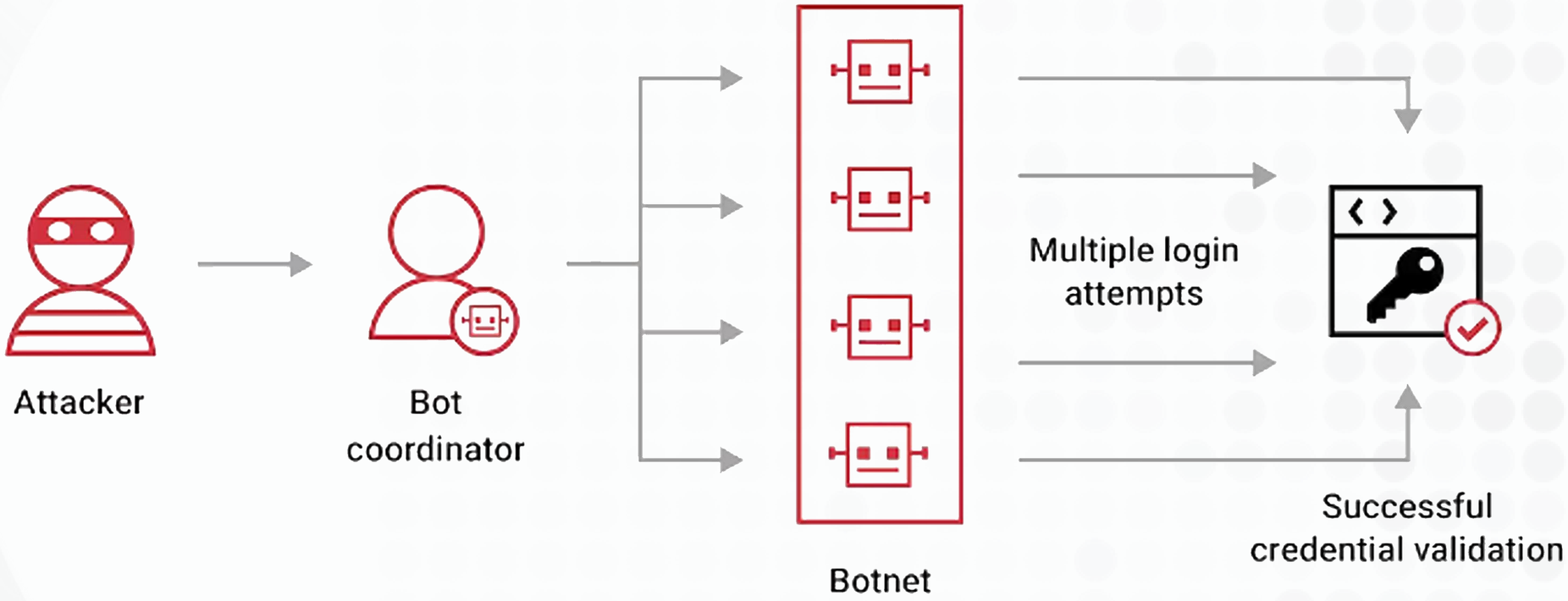
Question 5:

Do you have procedures when a policy isn't followed?

Question 6:

Are you able to "roll back" failed patches?

CYBER TABLETOP EXERCISE 3

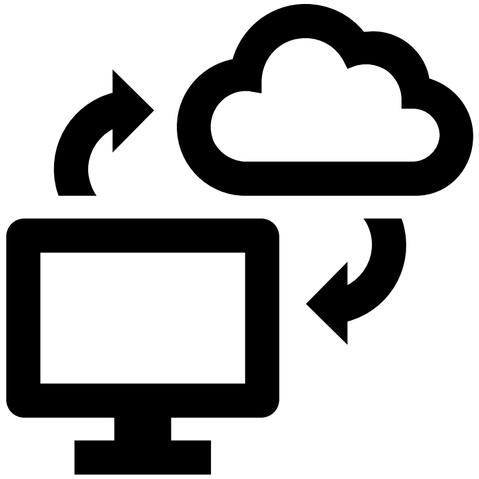


CLOUD COMPROMISE

CLOUD COMPROMISE

BACKSTORY:

You frequently use external cloud storage to store data that includes sensitive information. AI was used to listen to unencrypted channels to intercept account and password information.



EXERCISE 3 SCENARIO

The IT Department uses an external cloud provider and have recently learned that the provider has been publicly compromised, and large amounts of data have certainly been exposed.

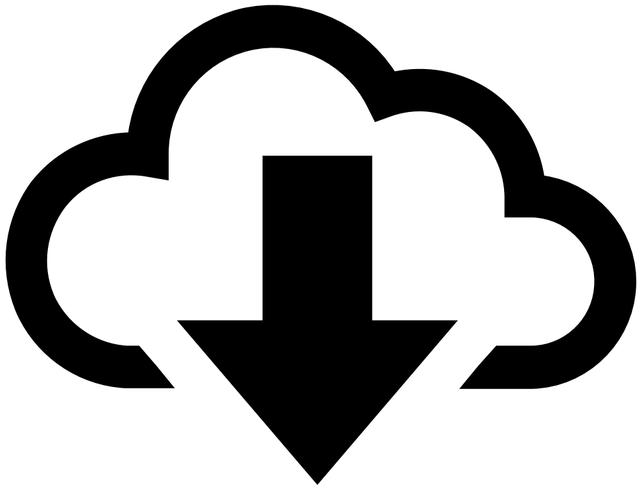
CLOUD COMPROMISE

BACKSTORY:

You frequently use external cloud storage to store data that includes sensitive information. AI was used to listen to unencrypted channels to intercept account and password information.

EXERCISE 3 SCENARIO

All user passwords and data that's stored in the external cloud provider's infrastructure may also be compromised.



CLOUD COMPROMISE

BACKSTORY:

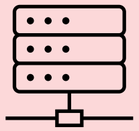
You frequently use external cloud storage to store data that includes sensitive information. AI was used to listen to unencrypted channels to intercept account and password information.

CYBER TABLETOP EXERCISE

EXTERNAL CLOUD COMPROMISE

Question 1:
Do you have policies for 3rd-party cloud compromise?

Question 2:
Should you be held accountable for the breach?



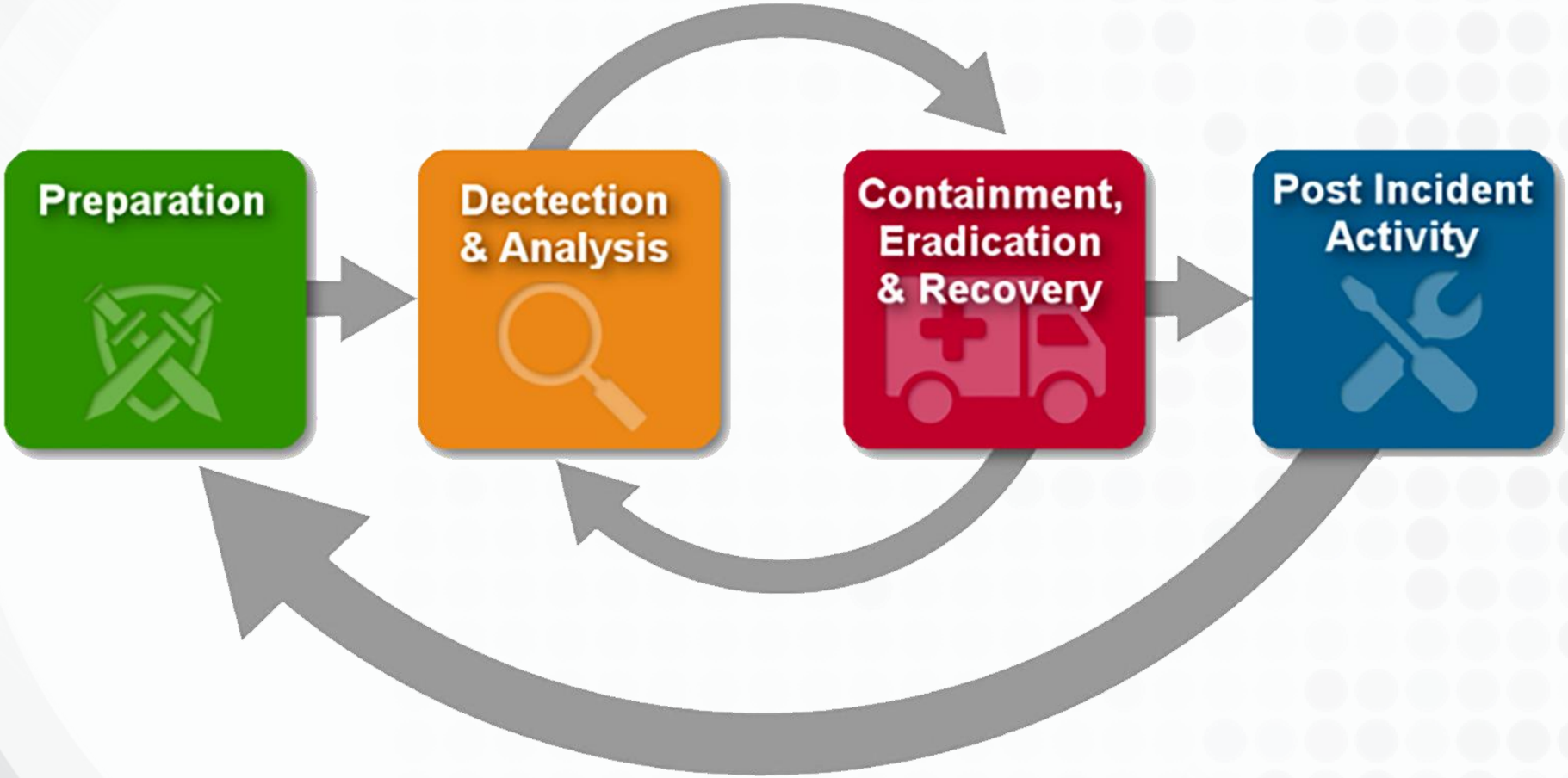
Question 3:
What would be different if it was on your local network?

Question 4:
What actions should management take?

Question 5:
What do you tell those who are involved in the breach?

Question 6:
When would you notify them and how is it done?

CYBER TABLETOP EXERCISE 4



INCIDENT RESPONSE UNPLANNED HACKTIVISM ATTACK

HACKTIVIST ATTACK

BACKSTORY:

You're local Police Department is being accused of excessive force. A hacktivist group is threatening they've integrated AI into their hacking tools and you're the target.

EXERCISE 4 SCENARIO

A hacktivist group threatens to target you after an allegation involving use of excessive force.
The nature of the attack being planned is unknown so you're preparing for the unknown.

CYBER TABLETOP EXERCISE

HACKIVIST ATTACK RESPONSE

Question 1:
What methods can be used to prioritize threats ?

Question 2:
How can you increase monitoring of IDS and IPS?

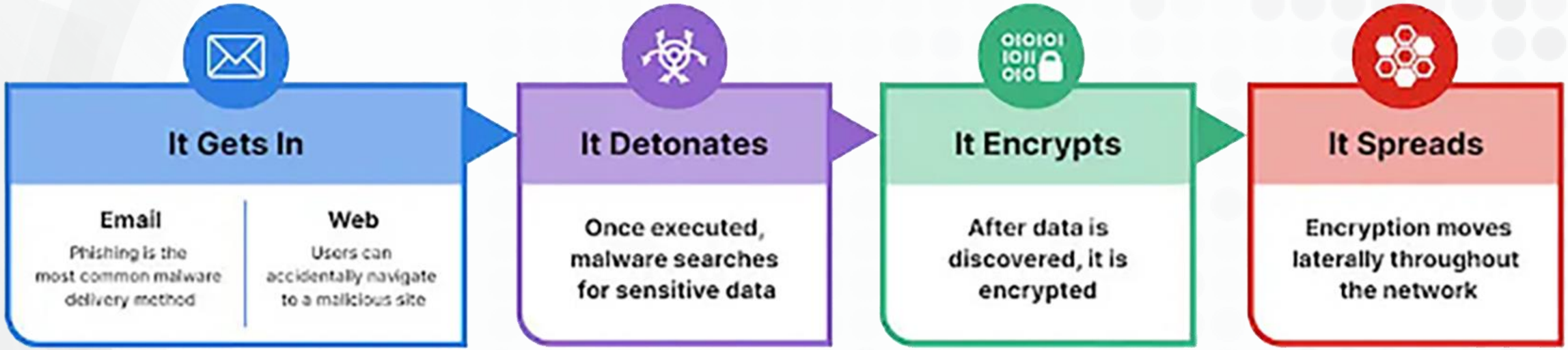
Question 3:
Who can assist you with analyzing malware?

Question 4:
How do you alert your IT Help Desk employees?

Question 5:
Do you have a process to notify other PD employees?

Question 6:
Does your IRP account for a similar type of scenario?

CYBER TABLETOP EXERCISE 5



PHISHING AND RANSOMWARE

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

DAY 1

Employees from the school's Treasurer's Office receive an email from Human Resources (HR) about new benefits for fiscal year 2024. The email instructs the user to sign the document and send it back to HR by close of business to ensure there is no lapse in benefits. Some employees follow the instructions and submit their information, while others report the email to the Information Technology Department Help Desk as suspicious.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

DAY 4

The Cybersecurity and Infrastructure Security Agency (CISA) releases an alert regarding phishing campaigns targeting state and local government networks. The phishing emails mention required updates to important HR documents and contain a malicious attachment that automatically installs ransomware. After gaining access to the network, threat actors escalate privileges for administrator rights without victims' action or authorization.

DAY 5

The school’s Information Technology Department sends a message stating that they have received reports of an email that may be a part of a phishing campaign and to immediately report any suspicious emails.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

DAY 7

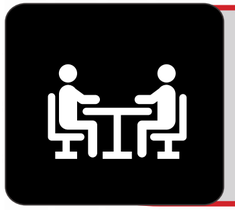
The school’s IT Department notices unusual traffic to an external IP address over a HTTP port leaving HR’s payroll servers. IT staff begin to investigate the anomaly, but it occurs only for a few minutes and stops, so they assume it was a one-time issue that has been resolved.

CYBER TABLETOP EXERCISE

PHISHING AND RANDSOMWARE

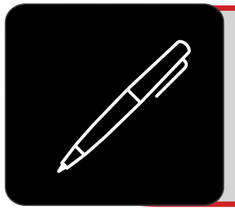
Question 1:

What plans/processes are followed for a cyber alert such as this one?



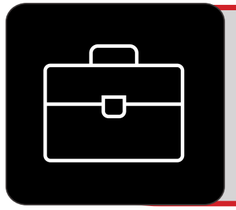
Question 2:

Does the cybersecurity training provided include this scenario?



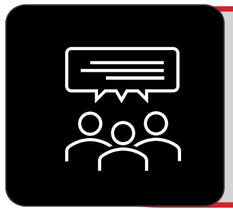
Question 3:

What's the process for employees to report suspicious emails?



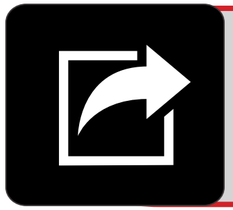
Question 4:

What steps should the IT Dept take to investigate unusual traffic to an external IP address?



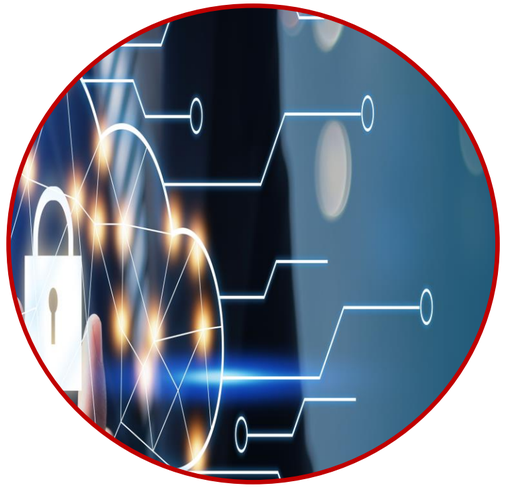
Question 5:

What cyber risk assessments are conducted to identify vulnerabilities?



Question 6:

What actions are needed after the recommendations are provided?



DAY 27

Early in the workday, a high volume of employees report that they are unable to log into their accounts and workstations using their credentials.

Later that day, several of the school's employee workstations display a red screen with a 72-hour timer counting down and the message:

"Every 24 hours there will be a new attack if the school waits to pay the equivalent of $250,000 in Bitcoin. Pay before the time runs out or your system will be wiped."

Due to the ransomware, the employee systems at the school are no longer functioning.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

DAY 28

The school has not paid the ransom. Multiple technology, transportation, food service, special education, and maintenance providers for the school are now reporting Distributed Denial of Service (DDoS) attacks. The County's Emergency Response reports all desktops and Voice over Internet Protocol (VoIP) systems are non-responsive.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

DAY 29

A social media account from someone claiming to be the attacker contains a warning to the school stating they are serious about the payment deadline. The post starts trending on social media, but skeptical local users comment that the account is fake.

In response, the alleged attacker account begins posting employee personally identifiable information (PII), with captions stating that they have more “for the right price and the longer the school waits to pay, the worse it will get.”

CYBER TABLETOP EXERCISE

PHISHING AND RANDSOMWARE

Question 1:

What actions are taken based on the Incident Response Plan?

Question 2:

How will the multiple DDoS attacks be mitigated?

Question 3:

What alternate communication is used with the primary VoIP inoperable?

Question 4:

What action is taken when a social media post is discovered with misinformation?

Question 5:

What are the potential legal and reputational ramifications?

Question 6:

What aid agreements are in effect with other cities, counties or the State?

DAY 30

A security researcher contacts your organization concerning a third-party provider employee's PII being advertised for sale on the dark web.

The third-party provider facilities impacted by the DDoS attack are currently relying on their backup systems/manual operations.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

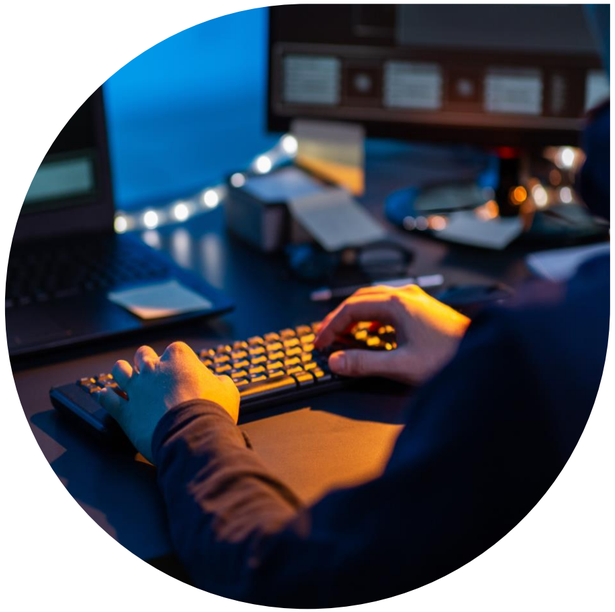
DAY 30
4:30 PM

The deadline for the ransom payment has passed and workstations remain locked. Several employees are reporting to their payroll office/Human Resources they have not received direct deposits for the most recent pay period, despite receiving a notification that they have been paid.

PHISHING AND RANDSOMWARE

BACKSTORY:

Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.



DAY 31

News of the ransomware attack has gone viral on multiple social media platforms with employees, parents, and students now using the tag #SCHOOL HACKED, stating that your school does not value their safety.

PHISHING AND RANDSOMWARE

BACKSTORY:

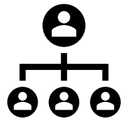
Threat actor targets school employees with a deep fake phishing email, compromises workstations and data, and demands a ransomware payment within 72 hours.

CYBER TABLETOP EXERCISE

PHISHING AND RANSOMWARE

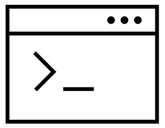
Question 1:

How quickly can backups be deployed and restored?



Question 2:

How will the organization respond to the social media posts and new inquires?



Question 3:

Are employees familiar with cyber terminology within the templates?

Question 4:

How would the public's confidence and trust be maintained?

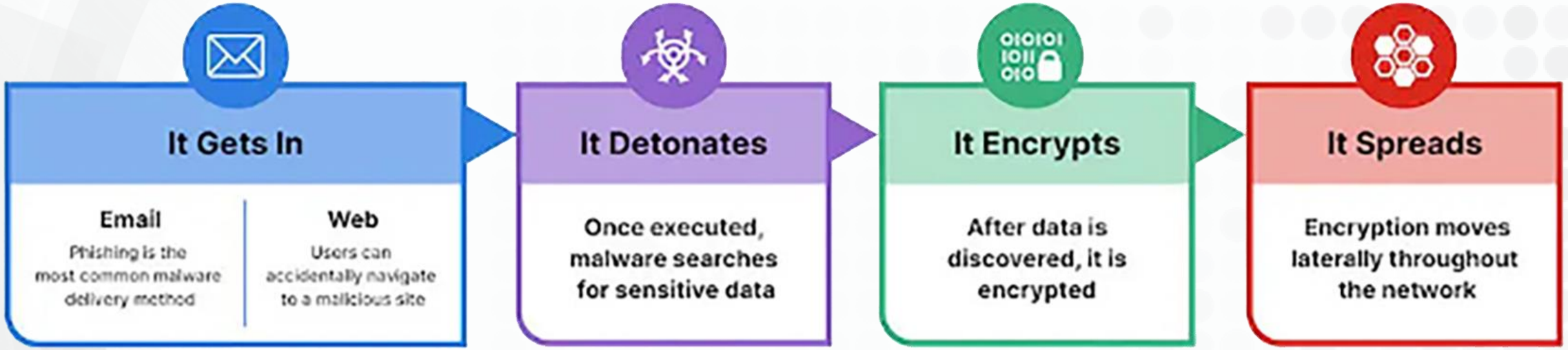
Question 5:

What post-incident actions or processes would be executed?

Question 6:

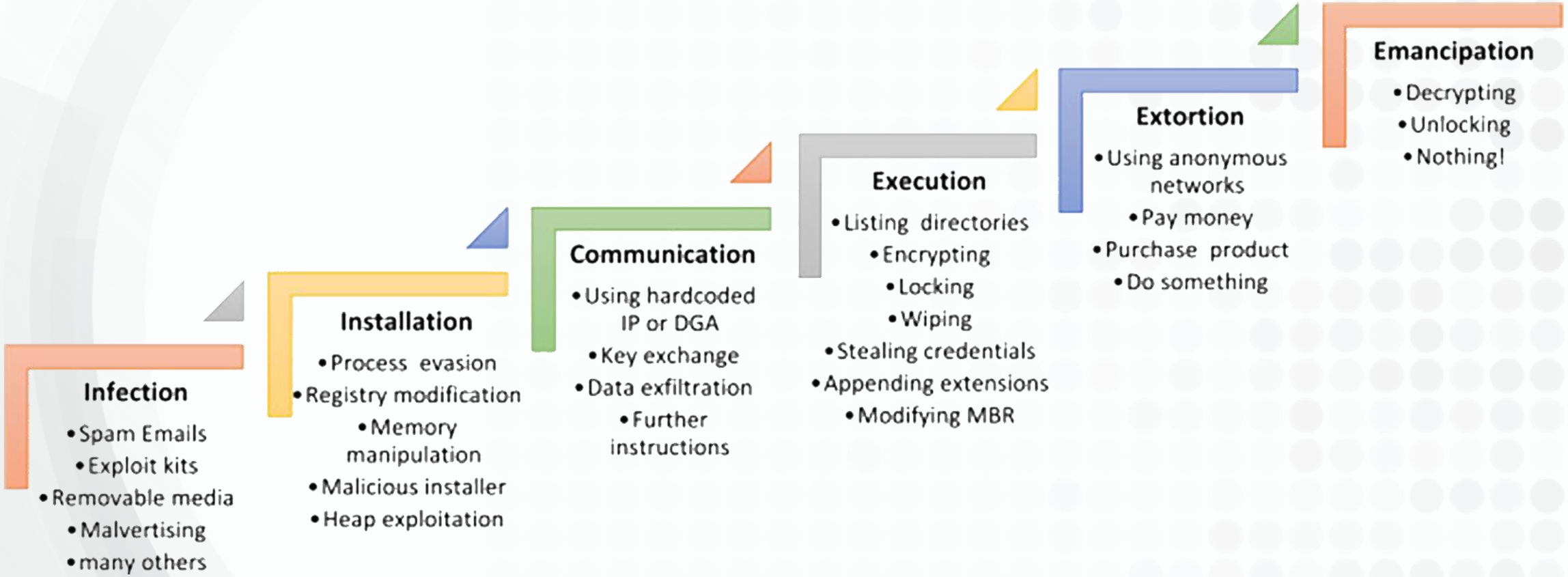
What aspects of the Incident Response Plan needs improvement?

TABLETOP - EXERCISE BONUS MODULE



RANSOMWARE ATTACK

CYBER TABLETOP EXERCISE - BONUS MODULE



RANSOMWARE

FLOODING AND RANSOMWARE

BACKSTORY:

Your school is located in a flood zone vulnerable to increasing global warming and digital disasters. Pooling in the basement took out the backup power generators and risers.

EXERCISE BONUS SCENARIO

Non-stop rain has caused flooding throughout the area. A state of emergency has been declared. In addition, you are also targeted for a ransomware attack taking systems down right before it occurs.

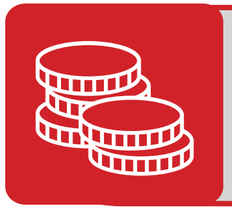
CYBER TABLETOP EXERCISE

FLOODING AND RANSOMWARE

Question 1:
Do you have a tested Disaster Recovery Plan?

Question 2:
Do you have a tested Incident Response Plan?

Question 3:
What if you're unable to restore from backup?

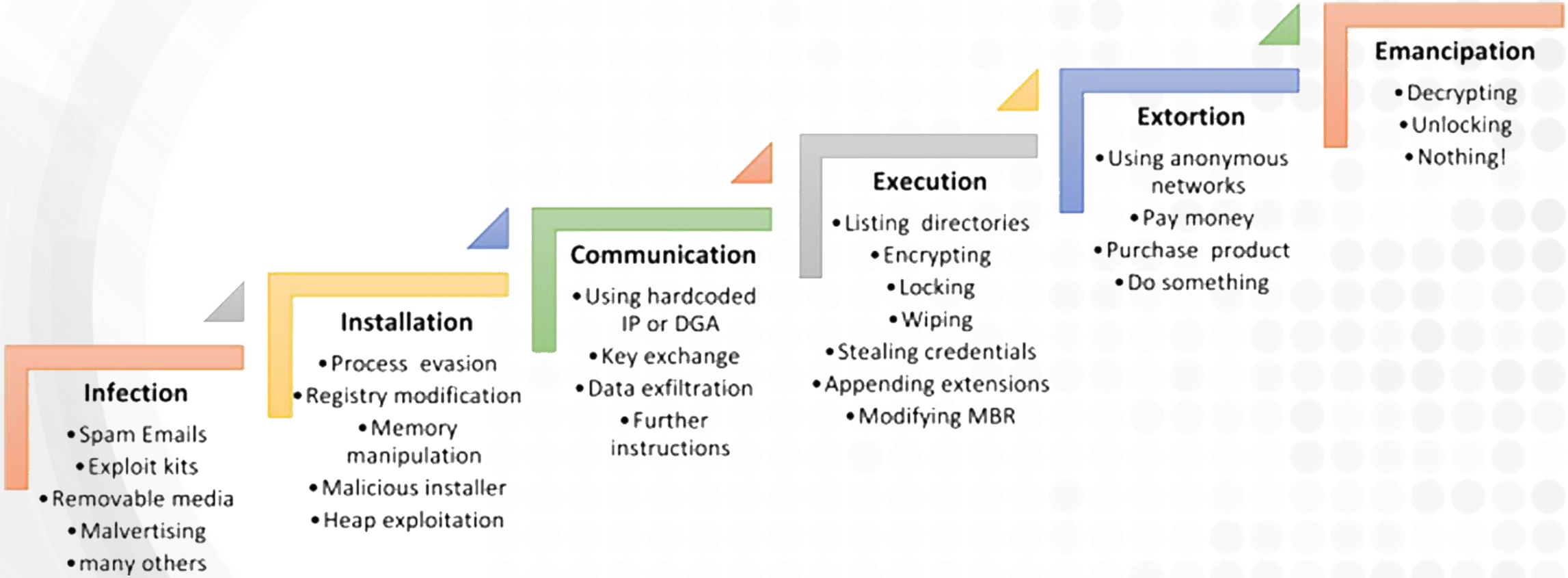


Question 4:
Do you have a plan if you must acquire bitcoin?

Question 5:
Can you reroute to another neighboring entity?

Question 6:
How do you notify with overwhelmed phone lines?

CYBER TABLETOP EXERCISE - BONUS MODULE



RANSOMWARE

RANSOMWARE

BACKSTORY:

You're a middle school with 100 employees, which includes a three-person Information Technology team. AI was used to scan for a zero-day vulnerability and instantly created a script for an attack.

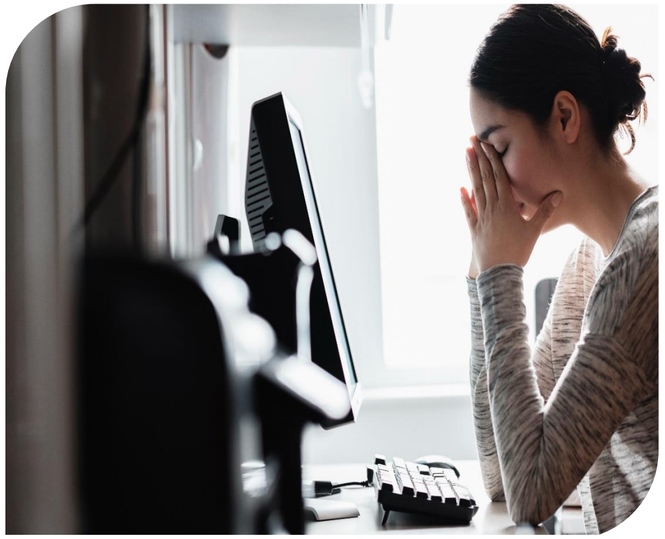
RANSOMWARE

BACKSTORY:

You're a middle school with 100 employees, which includes a three-person Information Technology team. AI was used to scan for a zero-day vulnerability and instantly created a script for an attack.

DAY 1
7:05 AM

After a long holiday weekend, a couple of early birds arrive at work and report to Information Technology that they can't access files on their workstations or the network drive.



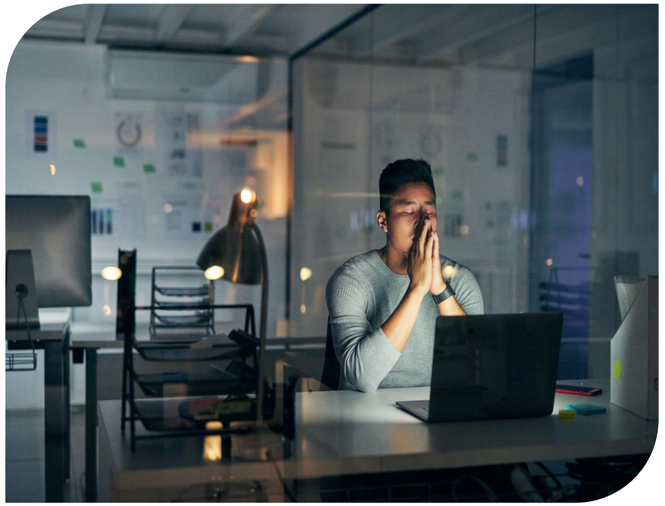
RANSOMWARE

BACKSTORY:

You're a middle school with 100 employees, which includes a three-person Information Technology team. AI was used to scan for a zero-day vulnerability and instantly created a script for an attack.

DAY 1
7:35 AM

Information Technology team members rush to the office and find that numerous files on the server and workstations appear to be encrypted.



RANSOMWARE

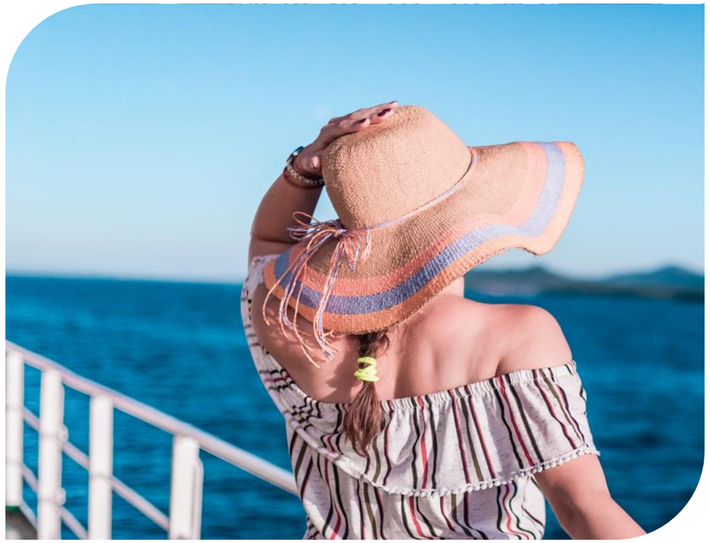
BACKSTORY:

You're a middle school with 100 employees, which includes a three-person Information Technology team. AI was used to scan for a zero-day vulnerability and instantly created a script for an attack.

DAY 1
7:55 AM

The only file anyone can open is one that has appeared in every directory. It's called RECOVER-FILES.txt.

Upon review, the team discovers that this is a ransom message and decides to notify the Information Technology leader.



RANSOMWARE

BACKSTORY:

You're a middle school with 100 employees, which includes a three-person Information Technology team. AI was used to scan for a zero-day vulnerability and instantly created a script for an attack.

DAY 1
8:05 AM

The Information Technology team realizes that the IT leader is currently on a cruise and completely unreachable.

RANSOMWARE

BACKSTORY:

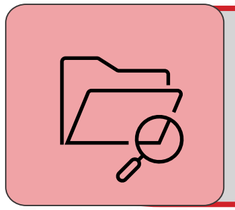
You're a middle school with 100 employees, which includes a three-person Information Technology team. AI was used to scan for a zero-day vulnerability and instantly created a script for an attack.

DAY 1
3:50 PM

Upon further investigation, 80% of your workstations and 50% of your servers and applications were encrypted. Forensic analysis found evidence of data exfiltration and indicated that the threat actors were actively in your network for months before the attack. Recovery will probably take several days or weeks. Not all data is recoverable.

CYBER TABLETOP EXERCISE

RANSOMWARE

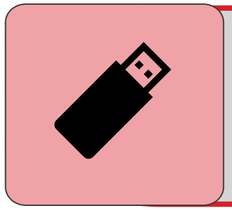


Question 1:

Does this qualify as an incident? Is PII, PCI, and/or PHI involved?

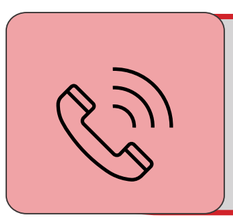
Question 2:

How do you investigate and discover what was exfiltrated?



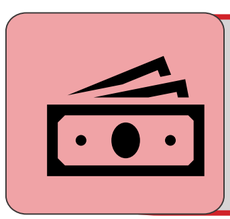
Question 3:

How long will it take to recover data from backup(s)?



Question 4:

What are the talking points for staff who get calls from customers?



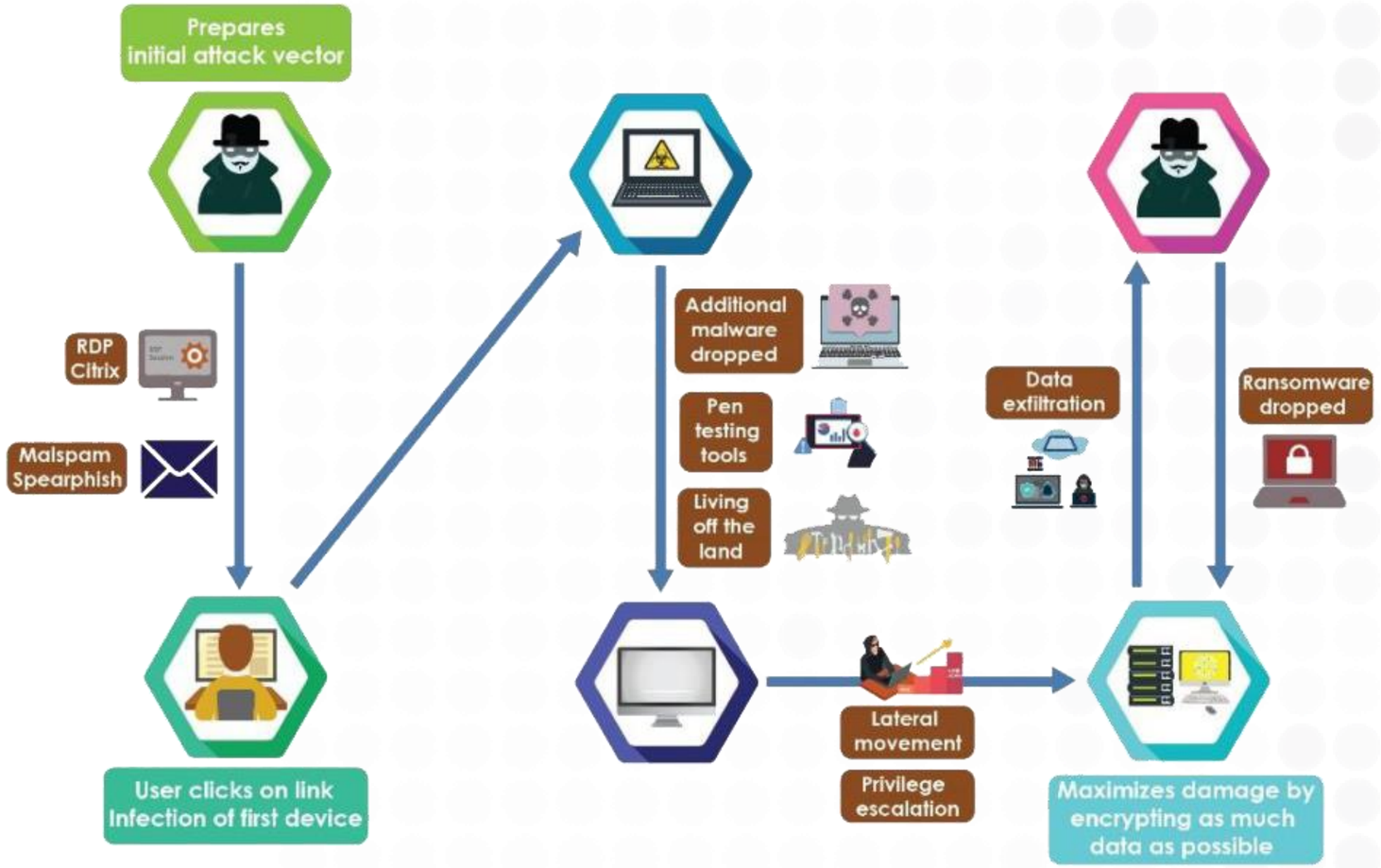
Question 5:

Will you pay the ransom? Who's involved in that decision?

Question 6:

What are reporting requirements after the incident is over?

CYBER TABLETOP EXERCISE - BONUS MODULE



DOUBLE-EXTORTION RANSOMWARE

DOUBLE-EXTORTION RANSOMWARE

BACKSTORY:

You're an entity that runs a cloud-based sourcing service. Customers log into your portal to order the parts they need to conduct operations each day. AI redirected an employee to a malicious site to steal credentials to get in.

DOUBLE-EXTORTION RANSOMWARE

BACKSTORY:

You're an entity that runs a cloud-based sourcing service. Customers log into your portal to order the parts they need to conduct operations each day. AI redirected an employee to a malicious site to steal credentials to get in.

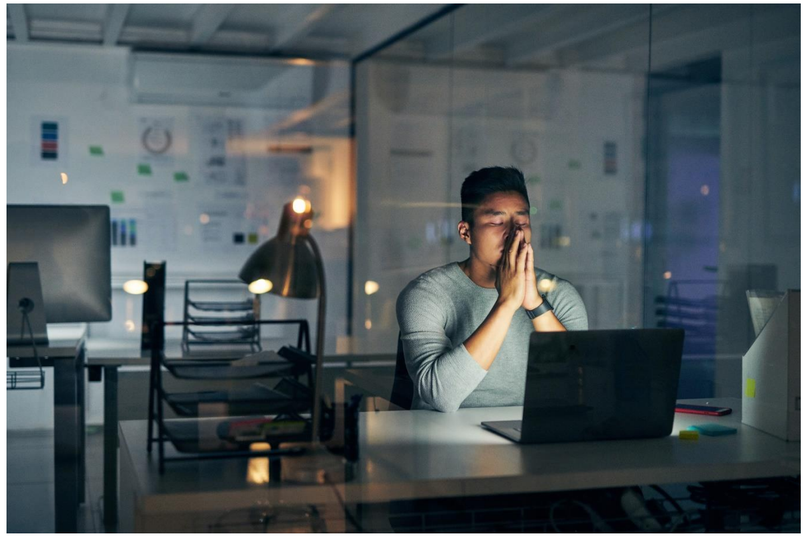
DAY 1
10:02 AM

A customer submits a support ticket saying that they can't get into the Admin Console for your service and can't query data from their database for custom reporting. Your support team attempts to use the service and discovers they can't get into it either.

DOUBLE-EXTORTION RANSOMWARE

BACKSTORY:

You're an entity that runs a cloud-based sourcing service. Customers log into your portal to order the parts they need to conduct operations each day. AI redirected an employee to a malicious site to steal credentials to get in.



DAY 1
10:10 AM

Your internal team sends the issue to your offshore software development team, and they can't get into the service either.

Questions are coming in from clients and partners inquiring when it will be available again.

DAY 1
3:45 PM

The forensic investigation finds a ransom note and discovers that the threat actor was able to capture cached admin credentials and pivot to other systems and resources.

DOUBLE-EXTORTION RANSOMWARE

BACKSTORY:

You're an entity that runs a cloud-based sourcing service. Customers log into your portal to order the parts they need to conduct operations each day. AI redirected an employee to a malicious site to steal credentials to get in.

DAY 1
4:59 PM

You realize that the attacker successfully exfiltrated critical data and is threatening to disclose it if ransom isn't paid. You haven't yet determined what data they exfiltrated.

Clients and partners have now alerted the media who's now contacted you.

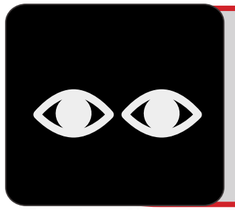
DOUBLE-EXTORTION RANSOMWARE

BACKSTORY:

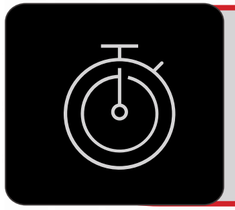
You're an entity that runs a cloud-based sourcing service. Customers log into your portal to order the parts they need to conduct operations each day. AI redirected an employee to a malicious site to steal credentials to get in.

CYBER TABLETOP EXERCISE

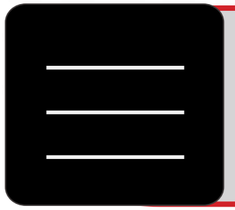
DOUBLE-EXTORTION RANSOMWARE



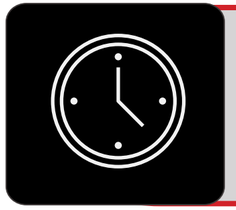
Question 1:
How do you investigate and discover what was exfiltrated?



Question 2:
How long will it take to recover data from backup(s)?



Question 3:
What are the talking points for staff who get calls from customers?



Question 4:
What deadlines are at risk while the system is compromised?

Question 5:
Will you pay the ransom? How will insurance be affected?

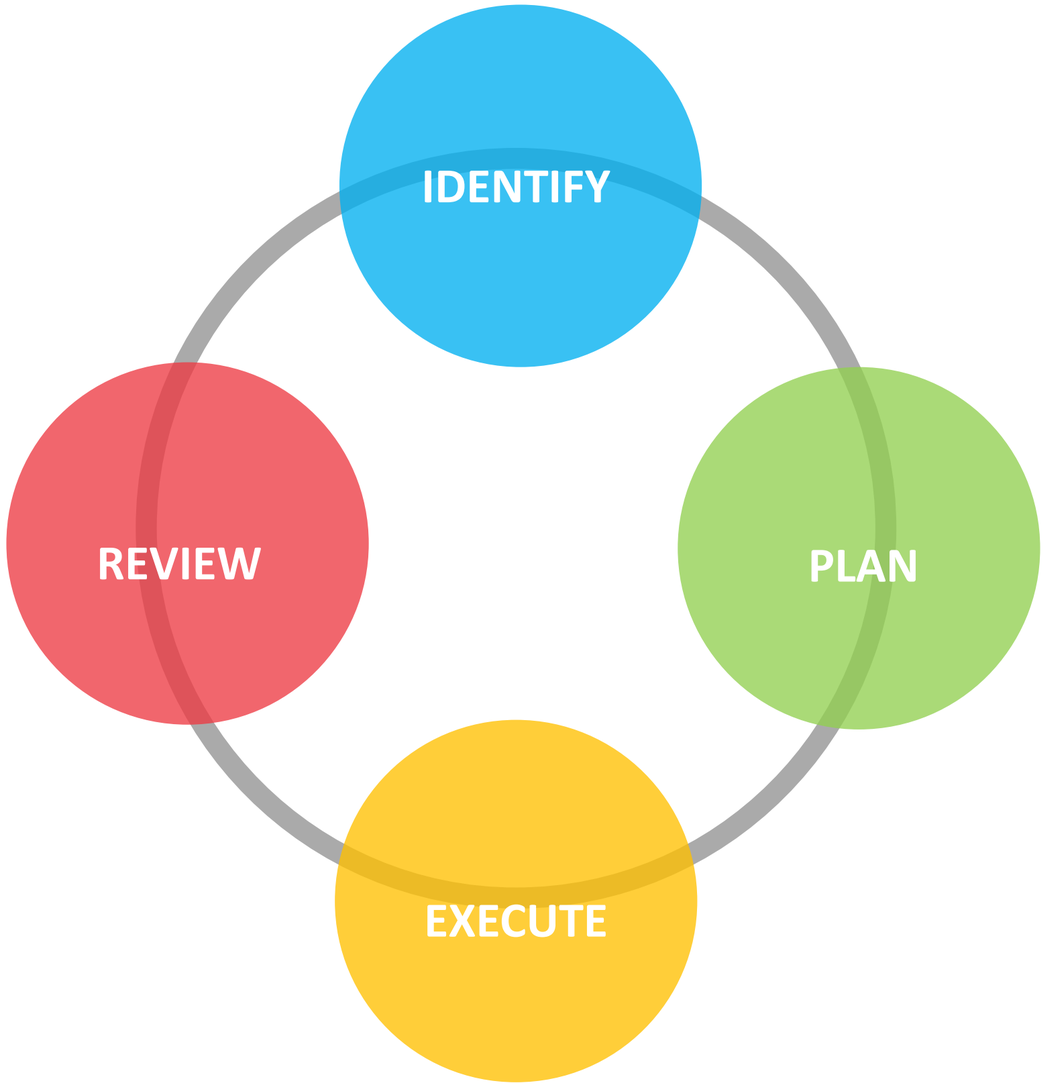
Question 6:
What are reporting requirements after the incident is over?

QUESTIONS

ERIC ADONTENG, CISM, Network+, SAP-C02, NIST-CSF Cert.

Eric. Adonteng@Persopool.com

CONTINUOUS IMPROVEMENT



THANK YOU