University of Toronto
Information Security Council - Incident Response Workgroup
Incident Response Tabletop

Goals

- Educate workgroup members
- Consider items needed for playbooks
- Tune tabletop activity for community

Ground Rules

Overview

- Each participant will be given a copy of this overview page, a sheet for each scenario, and a comment form
- Each scenario form has spaces to respond to specific question and areas for additional comment
- It is not required to fill out the scenario forms, but it is appreciated
-

Format

- There are six different scenarios
- Each scenario has three questions to discuss in the tabletop
- Each scenario has additional “items to consider” to be used both as an education tool and for discussion if time permits

Each Scenario

- Facilitator will read the scenario
- Some details are left intentionally vague
- Participants will have a few minutes to read and ask clarifying questions
- Facilitator will ask one question at a time and group will discuss
- Each participant should respond at some point for each scenario

Agenda

- Opening
- Establishing ground rules and expectations (10 mins)
- Scenario 1 (20 minutes)
- Scenario 2 (15 minutes)
- Scenario 3 (15 minutes)
- Scenario 4 (15 minutes)
- Scenario 5 (10 minutes)
- Scenario 6 (15 minutes)
- Feedback on overall scenario (10 minutes)
- Closing

#1 CLOUD SERVICE

A group of users in your department frequently uses outside cloud storage to store large amounts of student data, some of which may be considered sensitive. You have recently learned that the cloud storage provider that is being used has been publicly compromised and large amounts of data have been exposed. All user passwords and data in the cloud provider’s infrastructure may have been compromised.

<u>Items to discuss</u>
Who do you report the incident to? How do you report it?

____

What should your initial response be?

____

Does your division have current guidelines that take into account third party cloud storage?

____

<u>Items to consider</u>
What should unit leadership do? Who else should be involved?
What, if anything, do you tell your unit staff? What, if anything, do you tell the affected students? How and when would you notify them? Who should notify them?
Does your organization have an appropriate contract with the cloud provider that covers security, breach and notification requirements and responsibilities?
Should your department be responsible for data breach notification and cost?

<u>Additional Notes</u>

____

____

____

____

____

____

____

#2 ACCIDENTAL DISCLOSURE

You receive news that one of your employees has accidentally disclosed personal information records for over 200 staff. This occurred when they accidentally emailed a document that had not been properly redacted to a contractor. The employee had been recently trained on the handling of personal information.

Items to discuss
Who do you report the incident to? How do you report it?

____

Would you contact the contractor? If so, what would ask them to do?

____

How does your department handle this disclosure of personal information?

____

Items to consider
What policies or practices do you have in place to address the data loss?
What should management do? Who else in the organization should be involved?
Is a formal notification required if the contractor has assured you that the email has been deleted?
How would you communicate the issue to your departmental staff?

Additional Notes

____

____

____

____

____

____

____

#3 RANSOMWARE

You just received a rather panicked call from a respected PI detailing that her computers used for climate modeling sponsored by NASA have been hit by ransomware. This ransomware seems to have infected and then encrypted all her data, including her external hard drive backups. According to the ransom she received, she must pay the $10,000 ransom in a week or the encryption key will be deleted and the data lost forever.

Items to discuss

Who do you report the incident to? How do you report it?

____

Does the researcher have an obligation to notify anyone?

____

Should we pay the ransom?

____

Items to consider

How can you determine the infection vector?
Are there any other forms of backup available?
What policies or practices do you have in place to address the situation?

Additional Notes

____

____

____

____

____

____

____

#4 PHISHING

A new staff member in your department received an urgent email request from a someone pretending to be one of the University's Directors.

The "Director" asked the employee to check calendar availability to organize a meeting with several staff members and later instructed to log into a website with their username and password.

The employee has access to confidential information and financial systems. After several email exchanges with the "Director" there was an additional request to purchase several gift cards. The employee realized something might be wrong.

<u>Items to discuss</u>
Who should they report the incident to?

What should your initial response be?

What steps do you take to find any other abuse?

<u>Items to consider</u>
What steps do you take to prevent financial loss?
What steps should the user take?
What guidelines, practices do you have in place to address this situation?

<u>Additional Notes</u>

#5 SOCIAL MEDIA

Your department’s website and social media are compromised.

Through public news outlets, an international terrorist group calling themselves the “Rebellion Cyber Forces” has displayed outrage against American politics. They have publicly claimed the successful cyber attacks on various government organizations. You learn that your unit’s official social media accounts have been compromised and someone is sending out notifications through your social media website to your students and alumni claiming that your unit has been compromised.

<u>Items to discuss</u>

How would you be alerted if account takeover notifications were being sent from your social media account?

____

Who do you report the incident to? How do you report it?

____

What do you tell your community both during and after the incident? How or when would you notify them?

____

<u>Items to consider</u>

How do you recover access to your account(s)?
What practices do you have in place to address the situation?
What is the impact to your department if you are unable to regain control of your accounts and systems for several days?
Once you regain control of your accounts, what do you do to help ensure that this doesn’t happen again?

<u>Additional Notes</u>

____

____

____

____

____

____

#6 DENIAL OF SERVICE

"Rebellion Cyber Forces" strikes again! Angry that you were able to take down their communications from your websites and social media, they launched an attack against the network. Your website no longer works, your internet connection slows to a crawl, and you cannot send or receive emails. Even worse, your new network controlled door locks stopped working too!

Items to discuss

Who do you report the incident to? How do you report it?

____

What should your initial response be?

____

How do you get your website back up?

____

Items to consider

Can you work without internet and email? How long?

What other physical control systems could break if they lost internet connection for a prolonged period of time?

What guidelines do you have in place to address the situation?

Additional Notes

____

____

____

____

____

____

____

Overall, was this exercise effective?

What was most useful for you?

What could have been better?

Scenario 1 Value: Least (1) (2) (3) (4) (5) Best

Scenario 2 Value: Least (1) (2) (3) (4) (5) Best

Scenario 3 Value: Least (1) (2) (3) (4) (5) Best

Scenario 4 Value: Least (1) (2) (3) (4) (5) Best

Scenario 5 Value: Least (1) (2) (3) (4) (5) Best

Scenario 6 Value: Least (1) (2) (3) (4) (5) Best

What other scenarios should be considered?

Additional Comments: