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

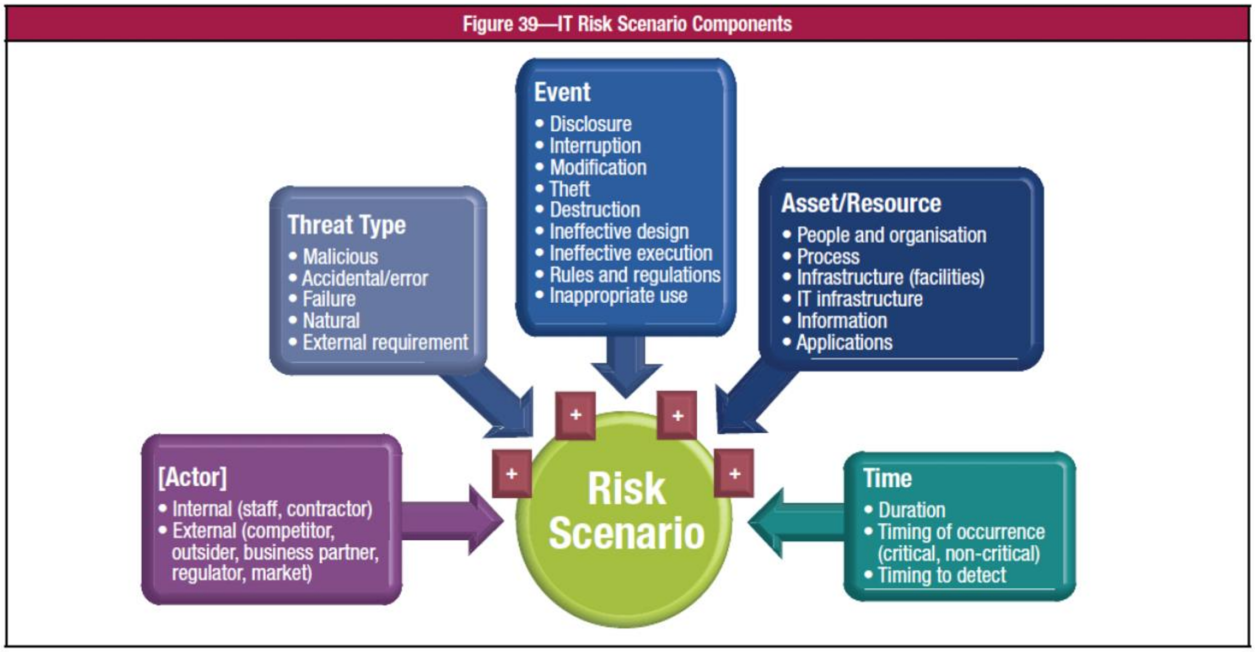
INDEX

Goals

- Through incident scenarios we can make information security incidents more concreate and tangible
- Scenarios allow also allow for proper incident response analysis and assessment
- The exercise brings realism, insight, organizational engagement, improved analysis and structure to often multi-dimensional and complex concepts.
- It's important to identify "what could go wrong" situations within each scenario
- There are two approaches in developing scenarios: top-down and bottom-up. In this exercise, all scenarios are using bottom-up approach where generic incident scenario is presented.
- In terms of Risk Identification, each scenario helps to refine and focus on particular risk factors (environmental external and internal, risk management capability, IT capability, IT-related business capability).
- For each scenario estimation of frequency and Impact would be provided.

IT Risk Scenario Components:

Figure 39—IT Risk Scenario Components



Overall Feedback

- Overall a very helpful exercise
- Helpful to understand different perspective on incident response.
- Surfaces some gaps in our processes
- Importance of identifying the notification order, and expectations of the University
- Highlights dependencies on our FOILs, privacy office, and the ISEA team, as well as ability to connect "call-tree" and communicate (phone, email, etc. …)
- We assumed that all points of contact are available, what if that is not the case?

Feedback on Ground Rules

- Keep it as a one-person response , as oppose to a conversation which got a little off track occasionally
- Would be helpful to strike a more serious tone, as one would in a crisis

What other scenarios should be considered

- Include scenario on mobile devices & data stewardship (someone leaves University with important information)
- Wide spread power or communication outage (cut fibre links channels).
- Outage caused by human error
- Building automation system attack
- A specific critical U of T service is attacked
- Subtle/covert site takeover collecting personal/confidential/financial information from un-suspecting users/community

Feedback on exercise format

- Potentially less scenarios leaving more time for discussion
- Include more focused scenarios.

Scenarios Scores

- Opening
- Establishing ground rules and expectations (10 mins)
- Scenario 1 (20 minutes) 5, 4, 5, 3
- Scenario 2 (15 minutes) 5, 4, 5, 5
- Scenario 3 (15 minutes) 5, 4, 5 Best, 4
- Scenario 4 (15 minutes) 5, 4, 5, 4
- Scenario 5 (10 minutes) 5, 3, 5 Best, 4
- Scenario 6 (15 minutes) 5, 2, 5, 4
- 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.

Discussion Items

- The nature of the breach unclear. Is it a compromise and what is compromised?
- Is it possible to communicate with the cloud provider to determine the scope? We should not assume it would be easy to talk to the cloud provider.
- What is the nature of data which has been compromised and who is affected, is it "our" data and how do we determine?
- If this is a non-sanctioned service, could we validate through third party and if so, what is the next step/how?
- List of users or disclosed usernames/passwords impacted by the compromise, and data classification? We might not be able to identify users at all. If so, what is the next step?
- Assuming sensitive data, communicate to IT, FOIL, Dean, Privacy Office, ISEA, Legal, CISO, CIO
- Is this a University wide impact?
- Gather facts and pass it on.
- Get institutional response ready, put "pieces" in place to be ready for response. Gather the data to find out who is involved.

Final remarks: Who determines severity and ownership? Who and what will determine who needs to come together to address this breach/incident?

#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.

<u>Discussion Items</u>

- Consensus on reporting to the Director / Office of the Dean / Unit Head followed by FOIL, HR and people who are directly connected. In some cases, defer to FOIL immediately. However, the question remains, who are all the people that should be involved and who should be notified first?
- Organize a meeting to talk this through to identify the next step and who should be notified
- We live in time where people are very sensitive about privacy
- Was it a point to point communication, and where was it sent from? Once the email is sent, we assume the data is lost.
- What are our obligations, and do we have a process? Protocol could be decided by policy and procedures.
- Request deletion and request confirmation of deletion from the contractor. The success of this could depend on relationship with the contractor. The note could be written with the help of the FIPPA office
- How do we communicate to be on the same page?

Final remarks: Do we need a specific team to address this? How can we establish ahead of time what to do? How do we ensure that every incident does not make all phones light up and overwhelms the response?

#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.

Discussion Items

- Report to VP, Dean of Research. Will this have an impact on sponsorship?
- Follow-up the standard escalation, check to see if there is a back-up.
- Back-up would most likely be also compromised, what is the next step?
- Legal needs to be brought in, as there is a University contract
- Verify and determine severity
- How do we determine if this is a U of T response? The bottom line is we don't know. Consistent approach should be identified, however not everyone would have the same response.
- What is the vector of attack and has it been addressed? Sometimes it is not enough to change your password, as it could be a "bigger thing".
- Should we treat this as a data breach? From US perspective, if it's a ransomware it is a data breach.
-

Final remarks: does the researcher has an obligation to notify anyone? Most researches are not aware or do not understand notification requirements for their sponsors. How do we get this message out?

#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>Discussion Items to discuss</u>

- Contact ISEA and follow their advice. Procurement and Police could be contact, as there is potential for fraud.
- Essential to contact Audit, due to accountability reporting, financial impropriety and financial management. It is currently not a big "P" policy. This exercise might help us to get there.
- The response to similar occurrences was less than desirable.
- There is a tendency to minimize this type of incidents
- The response not well coordinated. However, the question is what should the response be?
- It would be helpful if the University would warn us of what is trending.
- Staff training and on-boarding process are essential to make sure all are informed of potential phishing and social engineering attacks.
- As a precaution, reset all password for recipients on meeting invite
- Depending on the extent, send notification to all faculty and staff
- If this person followed instructions this time, they could've followed other previous instructions. Encourage person to person conversation.
- Is there a U of T policy or guidelines? Yes, but it was last revised in 1995 and needs to be updated.

#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.

Discussion Items

- Notify students, there is no formal way to do this right now
- Take site off-line and replace it with a temporary page
- Work to get social media account back. The question though is how?
- Engage communications department. There should be a standard.
- Leverage other communication channels. Talk to U of T communications. Who would be the contact person?
- Leverage IT&S status page. Contact ISEA.
- What steps could we take to prevent and prepare for this type of incidents? Two-factor authentication for social media channels is essential. How do we communicate this?
- Social accounts should be monitored, and accountability assigned
- Engage infrastructure team and come to the leadership for the purpose of triage.
- What is the technology risk, reputation?
- How do we determine the scope and what tools/capabilities we have available?
- How do we contain and continue to operate if unable to block or stop the attack?
- What are the remediation steps?
- Restoring from back-up might not be feasible in most cases, as it will be compromised
- Should there be a policy/guideline as to what could be placed under U of T banner using third party services?
- Distributed nature is a strength.
- A more serious concern is where there is a subtle/covert takeover, which could collect personal/confidential/financial information. What would be the process to deal with this?

Final Remarks: What do we tell our community both during and after the incident? How or when would we notify them?

#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!

Discussion Items

- We will need multiple levels of response, ISEA would be a partner to identify where it is coming from and how to mitigate depending on the nature of the attack.
- Call-tree would be helpful
- Is there a big fire / small fire scenario in play? How would we know?