UNIVERSITY of GUELPH | CANADA CYBER FOUNDRY

Cybersecurity Tabletop Exercise:

Objective:

To simulate a ransomware attack targeting a farm or research facility, thereby focusing on improving response strategies by encouraging team collaboration during incidents. Further, ensuring the protection of management systems, production, storage operations, and critical data.

Duration:

2 hours

Participant roles:

1. **Site Manager (CEO, farm manager, division manager, etc.)**
2. **Personnel (IT rep, HR rep, etc.)**
3. **Cybersecurity Specialist (CCS)**
4. **Scientific Representative (researcher, nutritionist, regulatory, etc.)**
5. **Regular Employee Representative**
6. **Finance Representative**
7. **Legal Advisor**

Facilitators: [Insert names here]

Tips for Keeping on Time:

- **Timekeeping**: Assign a timekeeper to ensure each stage stays within the allocated time.
- **Clear Instructions**: Provide clear and concise instructions for each stage.
- **Limit Discussions**: Encourage focused discussions to avoid going over time. If discussions are going well, the debriefing session can be extended by 5-10 minutes, making the total duration slightly over 2 hours.

- **Pre-distributed Materials**: Provide any necessary materials or instructions beforehand to save time during the exercise.

Introduction:

Facilitator: Welcome to our Tabletop Exercise. Today, we will simulate a ransomware attack targeting a farm or research facility. The goal is to evaluate our response capabilities, identify areas for improvement, and foster collaboration. Please participate actively and share your insights.

Explanation of the Exercise:

Facilitator: Now, I will divide you into roles. Each role will represent a different professional view to analyze the attack scenario better. We will go through each phase step-by-step, with specific actions and decisions. Let us begin with the initial detection phase.

Facilitator: At 8:00 AM on Friday, the Site Manager received a report from an employee that the workstation managing the system operations had malfunctioned. Upon investigation, the manager discovers a ransom note displayed on the central control system screen. The note demands payment of 20 Bitcoin (approximately CAD 3,000,000) within 48 hours for a decryption key. The note warns against seeking help from law enforcement or attempting to decrypt files, threatening to purge all encrypted data.

Key systems affected include:

1. **Monitoring tools**, i.e. delaying detection of illnesses or anomalies.
2. **Automated schedules**, i.e. disrupting the precision nutrition critical to animal welfare or processing flow, and research outcomes.
3. **Tracking systems**, i.e. halting data collection needed for yield and quality analysis.

The incident has immediate implications for production, animal welfare, operational continuity, and the integrity of research projects, potentially causing financial losses and reputational damage to the organization.

Initial Response:

Question 1: Site Manager

Facilitator: You've discovered the ransom note on the system operations workstation. The attack has disrupted critical functions, including schedules, monitoring, and temperature regulation, which poses risks to production continuity. What is your immediate response?

Action Steps:

- **A:** Notify all staff to cease using devices connected to the network and implement manual protocols for critical operations.
- **B:** Contact IT Personnel to immediately isolate the compromised workstation and begin assessing the ransomware's impact on other systems.
- **C:** Attempt to restart the workstation to remove the ransomware and restore normal operations.
- **D:** Notify senior leadership of the incident and prepare a communication plan for staff and external stakeholders, including potential regulatory notifications.

Allow time for participants to choose an option.

Answer Key:

Option A (Correct): Notifying related staff and switching to manual operations is the immediate action to be taken

Option B: While this operation is correct, it should be followed the first action step

Option C: Restarting risks worsening the ransomware's impact.

Option D: This option is implemented after the initial containment methods are applied.

Question 2: Personnel

Facilitator: The Site Manager has reported a ransomware attack. Network traffic indicates unusual outbound communication from several devices, suggesting possible lateral movement. What steps should you take to contain the incident?

Action Steps:

- **A:** Immediately disconnect the affected workstation and any other suspicious devices from the network.
- **B:** Begin restoring systems from the most recent backup to ensure minimal downtime.
- **C:** Contact the Cybersecurity Specialist (CCS) for assistance in conducting a forensic investigation of the compromised systems.

- **D:** Change all administrative passwords and disable remote access while investigating the breach.

Allow time for participants to choose an option.

Answer Key:

Option A (Correct): Disconnecting compromised devices is critical to stop lateral movement and prevent further spread.

Option B: Restoring systems without containment risks reinfection or further spread.

Option C: Forensics are important but should follow initial containment.

Option D: Password changes are useful but secondary to isolating affected devices.

Question 3: Cybersecurity Specialist (CCS)

Facilitator: You've been called in by IT Personnel to assist with the forensic investigation. The ransomware seems to have been delivered via a phishing email that a Regular Employee accessed. How will you prioritize your tasks?

Action Steps:

- **A:** Conduct a root cause analysis to identify the email source and any other compromised accounts.
- **B:** Work with IT Personnel to isolate affected systems and monitor network traffic for additional threats.
- **C:** Engage with the Legal Advisor and senior leadership to assess compliance obligations and data breach reporting requirements.
- **D:** Develop a remediation plan that includes patching vulnerabilities, implementing stronger email security measures, and conducting staff training on phishing awareness.

Allow time for participants to choose an option.

Answer Key:

Option A: Root cause analysis is necessary but should follow immediate containment and remediation actions.

Option B (Correct): Isolation and monitoring are critical to prevent further damage while beginning the investigation.

Option C: Legal considerations are important but secondary to addressing the immediate security risk.

Option D: Remediation planning is vital but comes after ensuring the threat is contained.

Question 4: Scientific Representative

Facilitator: The ransomware attack has disrupted automated schedules and monitoring. What are your immediate priorities?

Action Steps:

- **A:** Notify regulatory bodies about any significant risks and propose mitigation plans.
- **B:** Collaborate with IT and CCS to understand when automated systems might be restored.
- **C:** Work with the Site Manager to implement manual protocols.
- **D:** Document the impact of the incident on research data and suggest alternative methods for data collection.

Allow time for participants to choose an option.

Answer Key:

Option A: Notifications are necessary but should follow urgent mitigation measures.

Option B: Collaborating with IT is helpful but secondary to immediate welfare actions.

Option C (Correct): Manual protocols ensure continuity while systems are restored.

Option D: Documenting impacts is important but does not directly address needs.

Question 5: Regular Employee Representative

Facilitator: You receive a phishing email and accidentally open the attachment, which appears to have triggered the ransomware attack. How do you handle this situation once you realize the mistake?

Action Steps:

- **A:** Immediately notify IT Personnel and provide them with the details of the email.
- **B:** Attempt to delete the suspicious email and remove the ransomware yourself to mitigate the issue.
- **C:** Communicate with your manager about the incident and follow any instructions for reporting.

- **D:** Share the phishing email with colleagues to warn them of similar attacks.

Allow time for participants to choose an option.

Answer Key:

Option A (Correct): Immediate notification to IT allows for containment and response.

Option B: Attempting to remove the ransomware yourself may worsen the situation or delay proper containment.

Option C: Reporting to management is useful but should follow notifying IT.

Option D: Warning colleagues is important but secondary to reporting to IT to stop the spread.

Question 6: Finance Representative

Facilitator: The attack has locked access to financial systems, and the ransom note demands payment in cryptocurrency to regain control. What should you do next?

Action Steps:

- **A:** Contact the Legal Advisor to assess the legality and implications of paying the ransom.
- **B:** Prepare a report on the potential costs of recovery, including lost productivity and ransom payment options.
- **C:** Notify senior leadership about the financial impact and assess potential losses or delays.
- **D:** Work with IT and CCS to understand whether backups or alternative systems can restore financial data.

Allow time for participants to choose an option.

Answer Key:

Option A: Legal input is important but should follow efforts to understand alternative recovery options.

Option B: Cost assessments are useful but secondary to resolving immediate operational impacts.

Option C: Informing leadership is necessary but should follow technical assessment.

Option D (Correct): Understanding whether backups or systems can restore access is critical before considering ransom payment.

Question 7: Legal Advisor

Facilitator: The ransomware attack has exposed sensitive research data and potentially personal information of staff. What legal considerations should you address first?

Action Steps:

- **A:** Assess whether data breach notification laws require reporting to regulators or affected parties.
- **B:** Advise against paying the ransom until all legal and compliance risks are fully evaluated.
- **C:** Consult with senior leadership on drafting external communications to stakeholders, ensuring compliance with legal requirements.
- **D:** Begin documentation of the incident to support future litigation or regulatory inquiries.

Allow time for participants to choose an option.

Answer Key:

Option A (Correct): Data breach notification laws must be addressed immediately to ensure compliance.

Option B: Evaluating ransom payment is important but secondary to meeting regulatory obligations.

Option C: Drafting communications is necessary but depends on the compliance evaluation.

Option D: Incident documentation is valuable but not the immediate priority during the initial response.

Initial Analysis and Isolation:

Facilitator: " Before we move to the next phase, let's quickly recap where we are in the incident. Early Friday morning, the Site Manager discovered a ransom note demanding 20 Bitcoin. A workstation managing the operations has been affected, and it malfunctions and becomes inaccessible. The IT team acted promptly to disconnect affected systems to contain the attack.

In this phase, we will analyze the scope of the attack, isolate remaining threats, and begin investigating the incident further. Let’s proceed with your roles and responsibilities during this phase."

Question 8: Finance Representative

Facilitator: With the ransom demand at 20 Bitcoin (approximately $500,000), senior leadership is seeking your input on whether paying the ransom is a feasible option. The organization lacks a robust cybersecurity insurance plan but has some emergency funds reserved. What is your role during this phase?

Action Steps:

- **A:** Calculate the financial impact of prolonged downtime versus the cost of paying the ransom and consult with the Legal Advisor on the implications.
- **B:** Recommend paying the ransom immediately to minimize operational disruption.
- **C:** Work with IT to assess whether backups can recover financial systems without considering the ransom payment.
- **D:** Focus on updating financial forecasts to reflect the cost of recovery and loss of productivity.

Answer Key:

- **A (Correct):** Balancing financial analysis with legal compliance is critical to making an informed decision.
- **B:** Paying the ransom without exploring alternatives or legal considerations is premature.
- **C:** Backup assessments are valuable but fall outside the primary role of the finance representative.
- **D:** Forecast updates are important but secondary to the immediate financial analysis.

Question 9: Cybersecurity Specialist (CCS)

Facilitator: After reviewing the logs, you suspect that the ransomware originated from an email attachment and spread through the network via an unpatched vulnerability in the monitoring system. What are your responsibilities during this phase?

Action Steps:

- **A:** Recommend immediate patching of the suspected vulnerability across all systems.
- **B:** Develop indicators of compromise (IOCs) to help IT Personnel monitor for similar malicious activity.
- **C:** Perform a deeper forensic analysis of the affected systems to confirm the attack vector and identify unpatched vulnerabilities.
- **D:** Focus on containment efforts to prevent further spread while assisting IT with system isolation.

Answer Key:

- **A:** Patching is essential but should wait until forensics are complete to avoid disrupting evidence.
- **B:** Indicator of compromise (IOC)s are useful but secondary to identifying the root cause.
- **C (Correct):** A thorough forensic analysis helps confirm the attack vector and mitigate future threats.
- **D:** Containment was handled in the prior phase; analysis now takes precedence.

Question 10: Regular Employee Representative

Facilitator: Employees are concerned about whether their personal or professional data may have been compromised. Some employees are hesitant to use their devices, while others demand clarity about the situation. What is your role in this phase?

Action Steps:

- **A:** Communicate openly with employees, reassuring them about containment efforts and sharing basic cybersecurity hygiene practices.
- **B:** Investigate the incident on your own to determine if employee data was compromised.
- **C:** Advise employees to refrain from using any organizational devices until further notice from IT or the CCS.
- **D:** Assist the CCS in identifying employees who may have interacted with phishing emails.

Answer Key:

- **A (Correct):** Open communication builds trust and prevents panic, while reinforcing good practices.
- **B:** Investigating is not within the scope of this role and could interfere with official efforts.
- **C:** Blanket advisories are unhelpful unless issued by IT or cybersecurity experts.
- **D:** Assisting with the investigation is useful but secondary to employee engagement and education.

Question 11: Scientific Representative

Facilitator: The operations are still disrupted, with system and monitoring on manual protocols. As data from automated systems is unavailable, research activities have been

halted. How do you proceed?

Action Steps:

- **A:** Prioritize company processes by refining and streamlining manual protocols for systems and monitoring.
- **B:** Work with IT to determine whether offline backups of data can be accessed for critical research needs
- **C:** Begin documenting how the lack of automated data impacts research outputs for compliance purposes.
- **D:** Communicate with research teams about delays and create alternative plans to collect necessary data.

Answer Key:

- **A:** While critical in the prior phase, manual protocols are already in place and are now secondary.
- **B (Correct):** Accessing offline backups ensures research continuity while minimizing further delays.
- **C:** Documentation is important but does not immediately address research continuity.
- **D:** Team communication is valuable but insufficient without actionable plans.

Question 12: Site Manager

Facilitator: As the organization's leader, you're tasked with keeping senior leadership informed while ensuring operational continuity. What actions are you prioritizing during this phase?

Action Steps:

- **A:** Begin reviewing post-incident recovery plans to prepare for the next phase.
- **B:** Press IT and CCS to accelerate system restoration to minimize downtime.
- **C:** Draft an external communication plan for potential stakeholders, including regulatory agencies.
- **D:** Ensure continued communication between all involved parties and monitor progress on containment and analysis.

Answer Key:

- **A:** Pressuring teams may lead to rushed actions that compromise recovery efforts.
- **C:** External communication is important but should follow internal containment and analysis.

- **D:** Recovery planning is necessary but secondary to addressing the ongoing incident.
- **D (Correct):** Coordinating communication ensures smooth collaboration and informed leadership decisions.

Question 13: Legal Advisor

Facilitator: It is becoming evident that the ransomware may have accessed or encrypted sensitive research data. There's also a possibility of a breach involving employee personal information. What legal priorities should you address in this phase?

Action Steps:

- **A:** Collaborate with CCS to determine whether the breach meets thresholds for regulatory reporting.
- **B:** Begin drafting data breach notifications to employees and regulators based on initial findings.
- **C:** Work with leadership to assess liability exposure and outline potential legal strategies.
- **D:** Advise against sharing information externally until a full forensic analysis is completed.

Answer Key:

- **A (Correct):** Determining compliance obligations is critical to meet legal and regulatory requirements.
- **B:** Premature notifications risk spreading inaccurate information.
- **C:** Liability assessments are important but secondary to compliance with reporting laws.
- **D:** External communication must align with legal obligations and cannot be unilaterally delayed.

Question 14: IT Personnel

Facilitator: As the incident continues to unfold, senior leadership wants an updated assessment of system status, including which devices remain compromised or inaccessible. What should be your focus during this phase?

Action Steps:

- **A:** Begin restoring affected systems to operational status as quickly as possible.
- **B:** Reassess and fortify network segmentation to limit further exposure.

- **C:** Work with the CCS to map out all affected devices and monitor for signs of ongoing threats
- **D:** Share regular updates with leadership and other teams about the status of affected systems.

Answer Key:

- **A:** System restoration should only occur after full analysis and threat containment.
- **B:** Strengthening segmentation is valuable but secondary to identifying ongoing threats.
- **C (Correct):** Mapping affected devices and monitoring threats is essential to understanding the scope of the attack.
- **D:** Updates are helpful but must follow accurate threat assessments.

Initial analysis and Isolation - Discussion Questions - 10 minutes

At this point, the facilitator needs to reinforce that these points were discussed, or ask the following questions:

- Were all critical roles, including the Site Manager, IT Personnel, and Scientific Representative, effectively involved in implementing manual protocols during the system downtime?
- Did the Regular Employee Representative effectively communicate containment strategies to staff, and were their actions aligned with the overall response plan?
- Were the existing offline backups of data promptly verified to assess their usability for system restoration
- Did any gaps in the availability of critical personnel or tools hinder the containment and analysis process? How could these be mitigated for future incidents?
- What specific improvements could be made to the isolation strategy to better protect interconnected systems?

Communication with Other Teams:

Facilitator: "During the previous phase, the ransomware strain was identified as **LockBit**, a ransomware group notorious for targeting critical infrastructure, including agricultural systems. This strain has previously impacted food and farm operations by disrupting IoT devices and automated systems. In this instance, logs revealed that the ransomware likely entered through a phishing email sent three days ago, disguised as an invoice from a supplier frequently used for equipment.

The compromised system controls critical operations, including data monitoring, schedules, storage, and regulation. These disruptions pose immediate risks to operational continuity.
In this phase, we will focus on ensuring clear and effective communication within the organization, as well as with external stakeholders such as equipment suppliers, regulatory authorities, and partners. Maintaining transparency and trust is critical to managing the situation while avoiding potential reputational damage. Coordination is key to ensuring that all response efforts are aligned and effective. Let's begin."

Question 17: Site Manager
Facilitator: How can you ensure that critical updates from recovery efforts are relayed effectively to external partners like regulatory agencies and suppliers?

Action Steps:

- **A:** Assign a dedicated liaison team to handle all external communications and inquiries.
- **B:** Share internal recovery status updates directly with external partners to foster transparency.
- **C:** Focus external updates only on timelines for restored operations to minimize concern.
- **D:** Use standardized templates for all communications to ensure consistency.

Answer Key:

- **Option A (Correct):** A liaison team ensures timely and consistent messaging tailored to external needs.
- **Option B:** Directly sharing internal updates could include irrelevant or overly technical details.
- **Option C:** Only communicating operational timelines risks losing trust and transparency.
- **Option D:** Standard templates may oversimplify information, reducing communication effectiveness.

Question 18: IT Personnel
Facilitator: How can you provide updates about system restoration progress without introducing unnecessary panic or confusion among non-technical teams?

Action Steps:

- **A:** Use progress meters and simple visuals to illustrate which systems are back online and which remain affected.
- **B:** Avoid giving granular updates to reduce the risk of miscommunication.
- **C:** Share only technical logs and timelines with leadership, leaving broader communication to them.
- **D:** Present the updates only during larger group meetings to avoid repetitive questions.

Answer Key:

- **Option A (Correct):** Progress visuals convey clear, digestible updates suitable for non-technical teams.
- **Option B:** Avoiding granular updates may leave gaps in understanding.
- **Option C:** Delegating broader communication risks creates delays in addressing team concerns.
- **Option D:** Limiting updates to larger meetings can miss opportunities for clarification.

Question 19: Cybersecurity Specialist (CCS)
Facilitator: How can you communicate complex threat intelligence and mitigation strategies to internal teams with varying technical expertise?

Action Steps:

- **A:** Focus only on real-time updates and delay technical briefings until after full mitigation.
- **B:** Provide a single comprehensive report to all teams for consistency.
- **C:** Limit communication about specific strategies to IT and leadership teams only.
- **D:** Use tiered communication strategies that tailor the level of detail to each audience's expertise.

Answer Key:

- **Option A:** Delaying technical briefings risks hampering immediate understanding and response.
- **Option B:** Comprehensive reports may confuse non-technical teams.
- **Option C:** Excluding teams from updates hampers overall coordination.
- **Option D (Correct):** Tailored messaging ensures relevance and comprehension for each audience.

Question 20: Scientific Representative
Facilitator: How can you ensure updates are communicated in a way that prioritizes urgency but avoids panic among farmworkers?

Action Steps:

- **A:** Directly update all farmworkers via general messages to avoid delays in action.
- **B:** Use a hierarchical communication system where team leaders cascade clear, actionable updates.
- **C:** Share only urgent updates to prevent information overload.
- **D:** Focus on providing detailed updates only to management to streamline decision-making.

Answer Key:

- **Option A:** General messages to all workers may create confusion without context.

- **Option B (Correct):** A hierarchical system ensures timely and clear communication while maintaining order.
- **Option C:** Limiting updates to urgent situations can lead to missed preparations.
- **Option D:** Restricting updates to management risks delays in worker-level actions.

Question 21: Regular Employee Representative
Facilitator: How can employees effectively raise concerns or report unusual activity without overwhelming communication channels?

Action Steps:

- **A:** Establish a schedule for reporting issues only at specific times during the day.
- **B:** Set up a designated communication channel for employee input on issues.
- **C:** Instruct employees to use their personal discretion in deciding which issues to escalate.
- **D:** Require all employees to report directly to supervisors, avoiding direct communication with IT.

Answer Key:

- **Option A:** Time-limited reporting could delay critical observations.
- **Option B (Correct):** A dedicated channel reports issues systematically and efficiently.
- **Option C:** Leaving discretion to employees may result in inconsistent reporting.
- **Option D:** Restricting communication to supervisors may introduce delays and bottlenecks.

Question 22: Finance Representative
Facilitator: How should you balance communicating financial risks to leadership with maintaining trust and reassurance among external stakeholders?

Action Steps:

- **A:** Prioritize internal discussions about financial risks and communicate mitigated risks to external stakeholders.
- **B:** Share the same detailed financial impact analysis with both internal and external audiences.
- **C:** Delay communicating financial risks externally until mitigation strategies are fully implemented.
- **D:** Avoid sharing detailed financial information with external stakeholders, focusing only on high-level reassurances.

Answer Key:

- **Option A (Correct):** Sharing mitigated risks externally reassures stakeholders while managing internal transparency.

- **Option B:** Equal detail for both audiences may lead to external stakeholders overreacting.
- **Option C:** Delayed communication risks eroding trust with partners.
- **Option D:** Overly vague reassurances can come across as evasive and harm trust.

Question 23: Legal Advisor
Facilitator: How can you communicate regulatory and legal compliance efforts effectively to both internal teams and external authorities?

Action Steps:

- **A:** Avoid discussing compliance updates during the incident to prevent distracting the response teams.
- **B:** Share the same detailed compliance updates with all parties for consistency.
- **C:** Focus communications solely on external authorities to avoid overburdening internal teams.
- **D:** Use clear summaries to inform internal teams about compliance actions and timelines while providing detailed updates to authorities.

Answer Key:

- **Option A:** Avoiding compliance discussions undermines timely and informed action.
- **Option B:** Equal detail for all may overwhelm internal teams unnecessarily.
- **Option C:** Omitting internal updates risks disjointed compliance efforts.
- **Option D (Correct):** Summaries for internal teams ensure clarity and alignment, while detailed updates to authorities maintain transparency.

Question 22: ALL PARTICIPANTS

Facilitator: Reflecting on the challenges faced during this phase, what improvements should be made to the farm or research facility's communication and coordination strategies to enhance incident response?

Facilitator: Reflecting on the challenges faced during this phase, what improvements should be made to the farm or research facility's communication and coordination strategies to enhance incident response?

Action Steps:

- **A:** Practice handling incidents together to improve communication.
- **B:** Keep doing things the same way as before.
- **C:** Create a clear team to manage all communication during incidents.
- **D:** Set simple rules for how and when to share updates.

Allow time for participants to choose an option.

Answer Key:

Option A: Practicing together is helpful but needs proper systems in place for lasting impact.
Option B: Keeping things the same doesn't help improve the response.
Option C (Correct): A clear communication team makes it easier to coordinate and avoid confusion.
Option D: Clear rules are useful but can't replace the need for a dedicated team.

Hotwash (10 minutes)

Facilitator: Thank you for your participation in today's tabletop exercise. Let's take a few minutes to reflect on our performance and discuss key takeaways from this simulation.

- What communication gaps or issues surfaced during the exercise, and what steps can we take to address them effectively?
- What are the top three improvements we can make to strengthen both our technical response and overall operational resilience?
- How well did we manage to isolate and contain the ransomware attack, and were there any significant delays or obstacles encountered?

Facilitator: Today's exercise underlined the critical role the farm or research facility plays in mitigating disruptions during an attack. By refining our communication frameworks, improving interdepartmental coordination, and ensuring more resilient continuity plans, we can strengthen farms and research facilities' readiness for future challenges. The insights shared here today will shape actionable strategies moving forward. Thank you again for your dedication and teamwork.