Hosting a Successful Cyber Breach Tabletop Exercise

A tabletop exercise is a cost-effective way to validate emergency response plans and system outage procedures (e.g., cyber breach incident response plan). During these exercises, leadership teams and employees with key emergency response roles come together to review hypothetical crisis situations (in a step-by-step, stress-free manner).

Exercises can be facilitated by internal or external experts and can run anywhere from two to eight hours, depending on the participants and the objectives.

Why run a Tabletop Exercise

Tabletop exercises can help organizations assess the adequacy of current procedures and policies, identify the strengths and deficiencies of their crisis response plans and define the roles and responsibilities of the crisis team. They are used to prepare relevant emergency response teams and leadership, as well as to educate healthcare board members around emergency response protocol. While exercises do take some planning to define key objectives, ensure credible scenarios, and be risk based they do not have to be complicated to stage.

With the increase in cyber breaches across the sector, tabletop exercises are a necessary and powerful tool for healthcare organizations.

At a minimum, organizations should run cyber breach tabletop exercises with executive leadership teams annually. The exercise can also be run with cyber breach response teams and other functional teams as required.

Key Elements of a Cyber Breach Tabletop Exercise

1. **Clearly-defined objectives and expected outcomes**
2. **A cyber breach scenario or example that is frequently experienced by the industry**
3. **An engaging exercise structure for tabletop participants**
4. **An engaging facilitator**
5. **The right group of stakeholders and participants**
6. **Well-documented responses**

Key Elements of a Cyber Breach Tabletop Exercise

EXPLAINED

1. Clearly-defined objectives and expected outcomes

Example of Objectives:

i. Gain a clear understanding of a cyber breach incident

ii. Review existing cyber breach response plan to identify gaps and opportunities for improvement

iii. Define roles and responsibilities of cyber breach response team members

iv. Understand emergency communication procedures and escalation paths (e.g., CEO will notify Board Chair, Board Chair will notify board members)

v. Review and talk through response plans in a stress-free and safe environment

Example of Expected Outcomes:

i. Clearly defined gaps and improvement ideas

ii. List of external or additional resource requirements

2. A cyber breach scenario or example that is frequently experienced by the industry

Pull from available cyber breach examples in the media or that peer healthcare organizations have experienced. You want the scenarios to be current and relevant. Ensure you keep this scenario well hidden from the participants of the tabletop exercise. The element of surprise is vital to the success of a tabletop exercise.

Sample cyber breach scenario: *Through a phishing email, a cybercriminal targets one of the hospital's Information Technology staff members who has system administrative privileges. The cybercriminal gains access to the network, compromises Personal Health Information (PHI) and installs ransomware on the hospital's computers.*

3. An engaging exercise structure for tabletop participants

Exercise structure can be presented using multimedia (e.g., PowerPoint, videos, etc.). The exercise structure should include:

- Cyber threat definition, examples and other details to educate the participants of the importance of cyber threats
- Description of events as they unfold from Day 1 to event resolution day, in a step-by-step and contemporary manner. Here is a sample description:

i. *Day 1, 10:00 a.m.: A system administrator from the Information Technology (IT) Department receives an email from the personal email account of a Finance department employee. The email states the Finance employee recently noticed some security notifications on their payroll vendor's website and recommends that the system administrator review the notification. The system administrator clicks on the link in the email and is re-directed to what appears to be the vendor's website. The website contained a generic warning of a ransomware variant. The IT employee does not believe the email to be suspicious.*

ii. *Day 4, 12:30 p.m.: Your IT staff conducts a routine review of intrusion detection system logs and discovers unusual traffic on your organization's printer ports. There is a significant amount of data leaving the printer ports and going to external IP addresses.*

4. An engaging facilitator

A facilitator should be knowledgeable and experienced enough to facilitate the group discussion by pausing and posing the right questions to the participants, at the right time. Sample questions may include:

- *What concerns do you have? How would you rate the severity of this event? Would this event need escalation?*
- *Who (if anyone) should be informed? By whom?*
- *What actions should be taken? By whom?*

5. The right group of stakeholders and participants

To reap the benefits accordingly, the right group of participants should be engaged based on the topic of the exercise. A cyber breach tabletop exercise should involve the following representatives, at minimum:

- Incident Manager
- Information Technology or Infrastructure Lead
- Chief Information Security Officer and Chief Information Officer
- Human Resources
- Communications/Media
- Privacy Officer
- Risk Manager
- All other executive leaders (CEO, VPs, etc.)
- Clinical leadership (as required)
- Scribe (Document! Document! Document!)
- Any other appropriate roles from the Incident Management System Team (e.g. Logistics)
- Board members (optional)
- Legal counsel (optional)

6. Well-documented responses

Your scribe should document the answers to the facilitator's questions and gaps appropriately. Below is a sample of a completed Facilitation Questionnaire (following the scenarios presented above in part 3).

What concerns do you have?	Who should be informed?	What actions would you take?
• Potential cyber breach • How did the IT system administrator not identify the phishing email? • Did the system administrator use the elevated account when they clicked the phishing link? • Potential data breach or data exfiltration	• Internal cyber security lead • IT leadership/management • CIO • Cyber security firm • VPs and CEO • Privacy Officer	• Take the printer offline • Look at all system activities and logs to identify potential anomalies • Look back at the printer logs to gage when the anomalies started • Contact Security Operations Centre (internal/external)

Discussion Questions for Cyber Security Teams

When running a tabletop exercise with the team responsible for cyber security, create discussion questions to ensure the important topics are covered. Sample discussion questions include:

- Do you have appropriate internal resources to handle such events?
- Do you know (and can you access) the contact details of external resources that may help resolve such events?
- Do you have defined roles for handling cyber security incidents?
- Do you have the necessary escalation path and decision-making criteria for paying the ransom?
- Do you have an identified individual, or group of individuals, responsible for external communications and media relations? Do you have scripts developed?
- What impact will a breach of Personal Health Information have on your organization? On patients/clients?
- What preventative processes and activities have you employed to ensure that these types of breaches do not occur at your organization?

How HIROC Can Help

As your proactive safety partner, HIROC shares knowledge and scales lessons learned across the healthcare system.

HIROC held two virtual risk management clinics in 2021, which included a total of three facilitated cyber security tabletop exercises. These exercises were built on real-life cyber breach incidents observed in the healthcare space. Hundreds of Subscriber participants with representation from IT leadership, healthcare leadership, Risk Managers, Privacy Officers and Chief Information Officers participated in the clinics. To access recordings from the 2021 sessions, email riskmanagement@hiroc.com.

Stay tuned for more Subscriber-exclusive workshops in 2022 that can help your teams prepare and practice.

Tabletop exercises do require planning and resources to ensure success. While they are valuable for all emergency planning, running tabletop exercises focused on cyber breach is critical for healthcare organizations.

If your organization is looking for assistance in putting together a cyber breach tabletop exercise or developing educational resources for staff, please do not hesitate to reach out to us at riskmanagement@hiroc.com.

Finally, for more information on best practices, download HIROC's Cyber Risk Management Guide, and Cyber Security Crisis Communications Guide.

External Resources

- Ransomware Playbook, Canadian Centre for Cyber Security, November 2021, https://cyber.gc.ca/sites/default/files/2021-12/itsm00099-ransomware-playbook-2021-final3-en.pdf
- CISA Tabletop Exercises Packages, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/cisa-tabletop-exercises-packages
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, National Institution for Standards and Technology, 2006, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

Kopiha Nathan
is HIROC's Privacy and Compliance Officer.

Reach out to her at knathan@hiroc.com.

Pre-Exercise Outline for Tabletop Exercise Organizers*

The following editable template will help tabletop exercise organizers identify key information prior to preparing and presenting a detailed exercise.

<Enter the Exercise Name: (e.g. Ransomware Attack)>	
Exercise Date, Time, and Location	Exercise Date Time (e.g. 9:00 a.m. – 12:00 p.m.) Exercise Location
Scope of the Exercise	<Identify what's in scope for the exercise. (e.g., Ransomware attack at hospital site A, facilitated exercise for senior leadership team.)>
Participants and Audience	<Identify the key participants for the exercise and their roles. If you will allow participants to observe the exercise, identify the audience here.>
Purpose/Objective of the Exercise	<Define the purpose/objective of the exercise. Example: 1) Educate senior leadership team about elements of cyber breach response. 2) Examine the current cyber breach communication procedures and solutions. 3) Validate the cyber breach response plan and identify changes and gaps. 4) Identify internal and external partners that should be involved in, or informed of, cyber breach response.>
Reference Materials	<List all reference materials. (e.g., Cyber breach response plan, communication plan, contact information for key internal and external stakeholders, vendors and authorities.)>
Threat Under Review	<Clearly identify the threat being evaluated. Always focus on one threat at a time. (e.g., Ransomware attack, phishing attack resulting in misdirected funds, etc.)>
High-Level Scenario Description	< Without going into detail, describe the cyber breach scenario in a few sentences.>
Exercise Sponsor	<Include a senior leadership sponsor. Having a senior leadership sponsor is key to running a tabletop exercise and ensuring follow-up activities have the necessary resources.>
Participating Organizations	<If you plan to include external vendors, partners or stakeholders in the exercise, identify them here. (e.g., Hospital association, insurer, IT provider, etc.)>

*This template was adopted from the Tabletop Exercises Packages, developed by the Cybersecurity & Infrastructure Security Agency (CISA). CISA is part of the Department of Homeland Security of the United States Government.

Topics to Discuss	<Identify topics that should be addressed during the exercise and questions tabletop participants should address. Example: 1) Identify what internal and external notifications are required (e.g. patients, families, staff members, Board Chair, insurance provider, community, etc.) to be sent within the following time window from discovering the breach: a) Minutes b) One hour c) 4-5 hours d) One day e) Two days f) Ongoing until full recovery of the systems 2) Identify the internal/external key technology partners that will: a) Contain the breach b) Provide forensic analysis c) Restore systems that have been taken down 3) Decisions regarding ransom payment: a) Who is responsible for making this decision? b) What are our decision-making criteria for paying ransom? c) What are the ramifications if we decide to pay? d) What outside partners/entities do you need to contact or seek approval from if we decide to pay?>
Other Notes	
Case Example	<Identify a case example that you can present to exercise participants so that they understand the subject and the potential impact the incident in review can have on an organization.>

Detailed Description of the Exercise Event	<Build out the scenario with time-based descriptions of the event. Example: Day 1, 1 p.m.: A staff member logging in to open a Word document from a shared drive notices that the file did not have the MS Word logo and looked different. The staff member couldn't open the file by double-clicking the file. The staff member sends an IT helpdesk ticket. Day 1, 3 p.m.: An IT helpdesk technician notices that there are an increased number of tickets about Microsoft files that staff are unable to open from the shared drive. Day 1, 3:10 p.m.: A team meeting is called with all IT helpdesk staff and the IT team lead to discuss the current issue with Microsoft files. The team decides to contact Microsoft helpdesk and a Cyber Security Specialist to investigate the issue. Day 1. 5pm: A ransomware warning appears on a staff member's computer. Continue building out the scenario.>

Once the above outlines are created, prepare a PowerPoint slide deck with appropriate visual aids.