



Facilitator Guide  
[Insert Date]

Department of Homeland Security

Exercise Starter Kit

Sponsor Logo

Cyber Breach Tabletop Exercise

# Facilitator Guide

[**Planner Note:** The purpose of this Facilitator Guide is to provide a baseline exercise document for facilitators to use in the delivery of the Cyber Breach Tabletop Exercise. The sample content contained in this document can be tailored as necessary to meet the desired goals and outcomes for the exercise by filling in all bracketed content that is highlighted in red. This document is to be used in tandem with the Cyber Breach Exercise Conduct Briefing and Situation Manual so any changes made to this document will also need to be aligned with those documents.]

This document is for the use of the exercise facilitator and should not be given to exercise players. It gives the approximate time of delivery for each slide, limited talking points, and possible supplemental questions or issues to raise in discussions if needed. The lead exercise planner and the exercise planning team are responsible for tailoring this document, as appropriate.

|  |  |  |  |
| --- | --- | --- | --- |
| **Slide #** | **Time** | **Slide Title/Content** | **Facilitator Notes** |
| **WELCOME AND INTRODUCTIONS,** [Insert time – Insert Time] (~ 5 minutes) |  |  |  |
| **[#]** | **[Insert Time]** | **Welcome and Introductions** | *When participants are ready:*   * Introduce yourself as the facilitator and provide a brief explanation of the facilitator’s role during the exercise * Introduce the topic of the exercise: a cyber breach targeting critical institutional data and information   Introduce any additional speakers and allow time for welcoming remarks |
| **[#]** | **[Insert Time]** | **Administrative Remarks** | *Provide brief administrative remarks.* |
| **[#]** | **[Insert Time]** | **Exercise Schedule** | *Briefly review the exercise schedule with participants.* |
| **EXERCISE OVERVIEW**, [Insert Time – Insert Time] (~ 10 minutes) |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Slide #** | **Time** | **Slide Title/Content** | **Facilitator Notes** |
| **[#]** | **[Insert Time]** | **Exercise Overview** | *Provide a brief background on the exercise:*   * This Cyber Breach Tabletop Exercise (TTX) is made available through the Department of Homeland Security’s (DHS) Exercise Starter Kits, and was developed as part of a collaborative effort between DHS and the Federal Emergency Management Agency (FEMA), National Exercise Division (NED)   *Provide an overview of the purpose of the exercise:*   * Each Exercise Starter Kit aims to support practitioners and senior leaders from the academic community in assessing emergency plans, policies, and procedures while also enhancing overall campus resilience * This specific Exercise Starter Kit aims to provide the opportunity to examine response and recovery operations related to a cyber breach   The materials used during this exercise were provided as templates and were tailored by the exercise planning team to meet the desired goals for this exercise |
| **[#]** | **[Insert Time]** | **Exercise Overview (cont.)** | *Provide an overview of the scope of the exercise.* |
| **[#]** | **[Insert Time]** | **Exercise**  **Objectives** | *Review the exercise objectives:*   1. Operational Coordination 2. Cybersecurity 3. Situational Awareness   Public Information and Warning |

|  |  |  |  |
| --- | --- | --- | --- |
| **Slide #** | **Time** | **Slide Title/Content** | **Facilitator Notes** |
| **[#]** | **[Insert Time]** | **Participant Roles and Responsibilities** | *Briefly review the roles and responsibilities of different types of participants in the exercise.* |
| **[#]** | **[Insert Time]** | **Participating Organizations** | *Briefly review the organizations participating in the exercise.* |
| **[#]** | **[Insert Time]** | **Exercise Guidelines** | *Briefly review the exercise guidelines.* |
| **[#]** | **[Insert Time]** | **Assumptions and Artificialities** | *Note that in any exercise there are certain assumptions and artificialities that participants must accept as being true. Briefly review these assumptions and artificialities.* |
|  |  |  | **STARTEX** |
| **MODULE 1: INITIAL RESPONSE** [Insert Time – Insert Time] (~ 60 minutes) |  |  |  |
| **[#]** | **[Insert Time]** | **Module 1: Background** | *Announce that this is the Start of the Exercise and that you will now transition into Module 1.*  *Review the scenario background information:*   * In recent years, malicious cyber actors have targeted colleges and universities with cybercrime activities and some institutions have experienced acts of cyber espionage * College and university networks may present an easier target due to multiple levels of connectivity and accessibility   Institutions may be at higher risk due to a lack of cyber security awareness among students, faculty, and staff |
| **[#]** | **[Insert Time]** | **Module 1: Scenario Overview** | *Review the exercise scenario:*   * **[Insert Date and Time]**   + A Special Agent with the FBI Cyber Division warns your institution’s Chief Information Security Officer that a cyber attack has been launched against your institution by an outside entity   + Currently the precise duration, scope, and source of the attack is unclear   A collaborative investigation with the FBI reveals the presence of an advanced persistent threat (APT) that appears to be consistent with sophisticated malware used in other university attacks to access critical institutional and proprietary information |
| **[#]** | **[Insert Time]** | **Module 1: Scenario Overview (cont.)** | *Review the exercise scenario:*   * **[Insert Date and Time + 4 Hours]**   + Within a few hours, evidence determines the attack was initiated three months prior, providing attackers with unlimited access to networks, databases, servers, and other sensitive resources associated with various departments and colleges   + While exfiltration of data cannot be confirmed, it is reasonable to assume that sensitive information has been compromised   While PII seems to be the initial target of the attack, a thorough analysis will take a few days to complete |
| **[#]** | **[Insert Time]** | **Module 1: Discussion Questions (1/4)** | *Explain to participants that they will now be engaging in the facilitated discussions portion of Module 1. Review the following exercise discussion questions with participants, then begin engaging and facilitating conversations for [insert number] minutes. Repeat this at the beginning of each set of discussion questions* |
| **[#]** | **[Insert Time]** | **Module 1: Discussion Questions (1/4)**  **(continued)** | **Operational Coordination**   1. What plans, policies, and procedures does your institution have in place to respond to the effects of a data breach? 2. What are your institution’s initial priorities?   [Facilitator Note: If there are any conflicting priorities, ask how participants would de-conflict them]   1. How would your institution establish a command structure to coordinate your immediate response efforts?    * Who are your key internal and external stakeholders and how would your institution incorporate them into this command structure?   [Facilitator Note: Prompt participants to identify specific offices or departments]   * + How can your institution coordinate with private and public partners to ensure a unified response effort?   [Facilitator Note: Ask participants if they follow the Incident Command System]   1. What resource gaps could limit your institution’s ability to respond to a cyber attack?  * What community resources and aid agreements could compensate for these resource gaps?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 1: Discussion Questions (2/4)** | **Cybersecurity**   1. Does your institution have a formalized cyber incident response plan?  * Does your plan clearly outline what individuals/positions are involved in response efforts and how they are expected to coordinate with one another? * Do you periodically test your plan and train staff? * Does your institution currently have cyber insurance? If so, at what point would you notify your provider of a potential breach? If not, what other financial plans do you have in place to offset the potential costs of this type of incident?   [Facilitator Note: If an institution does not have a formalized cyber incident response plan, ask participants if any other plans contain relevant guidance for a cyber event] |
| **[#]** | **[Insert Time]** | **Module 1: Discussion Questions (2/4)**  **(continued)** | 1. Does your institution’s response strategy outline how to align broader response efforts with ongoing security management and IT efforts? 2. What steps will your institution take to verify the likelihood of a data breach resulting in the release of PII?  * How does your institution determine what systems/data/services may have been breached?  1. What measures are in place to protect confidential, personal, financial, and academic information concerning students, faculty, staff, and alumni from a potential cyber incident?  * Are these existing protective measures, or measures that would be implemented following a cyber incident?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 1: Discussion Questions (3/4)** | **Situational Assessment**   1. How does your institution collect, verify, and analyze information immediately following awareness of, or notification of a cyber incident?   [Facilitator Note: Ask who within the institution is responsible for leading this effort]   1. How do you conduct initial decision-making and offer decision-making recommendations to senior leadership?   [Facilitator Note: Ask participants who would be considered the “lead” for this type of cyber incident]   1. Do you have identified information requirements that support leadership decision-making processes (e.g., type of cyber incident, scope of incident, numbers of individuals impacted, implementation of cyber response plan)?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 1: Discussion Questions (4/4)** | **Public Information and Warning**   1. What plans, policies, and procedures does your institution have in place to guide communications with potentially affected parties at this time?   [Facilitator Note: Follow-up with participants with a question about how aware personnel across the institution is aware of these plans, policies, and procedures] |
| **[#]** | **[Insert Time]** | **Module 1: Discussion Questions (4/4)**  **(continued)** | * What internal and external stakeholders are you engaging? * What information would you release and how? * How does your institution use pre-scripted or automated messaging that would expedite critical communications?   [Facilitator Note: Ask participants how often these pre-scripted messages are reviewed and updated]   1. What individual, office, or department coordinates and delivers your institution’s messaging? 2. How will your institution use social media platforms in support of incident communications and messaging? 3. At this point in the scenario, would your institution notify non-affected members of the campus community? 4. [Insert additional discussion questions]   *Announce that we will now be transitioning to a 10-minute break.* |
| **BREAK:** [Insert Time – Insert Time] (~ 10 minutes) |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Slide #** | **Time** | **Slide Title/Content** | **Facilitator Notes** |
| **MODULE 2: EXTENDED RESPONSE** [Insert Time – Insert Time] (~ 60 minutes) |  |  |  |
| **[#]** | **[Insert Time]** | **Module 2: Scenario Overview** | *Announce that you will now transition into Module 2.*  *Review the exercise scenario:*   * **[Insert Date and Time + 12 Hours]**   + A second intrusion has been detected on your institution’s network   + While investigating the initial breach, a malware variant used by cyber criminals to harvest PII was discovered on several computers within your Office of Human Resources, the Admissions and Registration Offices, and the Financial Aid and Scholarship Offices * **[Insert Date and Time + 24 Hours]**   A detailed review of internal logging systems indicates stolen employee login credentials may have been used to access databases containing both student and faculty records |
| **[#]** | **[Insert Time]** | **Module 2: Scenario Overview)**  **(continued)** | * + Further examination reveals larger amounts of data has been exfiltrated over the past few month, including the name, address, date of birth, and social security number for students, faculty, and staff from 2012 to present   This information includes both domestic and international students |
| **[#]** | **[Insert Time]** | **Module 2: Scenario Overview (cont.)** | *Review the exercise scenario:*   * **[Insert Date and Time + 36 Hours]**   + Local news outlets begin contacting your institution’s public affairs office indicating that they have received reports of a potential data breach at your institution   + Reports claim that the personal information of hundreds of students, faculty, and staff have been stolen   Concerned students and parents begin inundating your institution with questions about their information as well as the extent of the potential breach |
| **[#]** | **[Insert Time]** | **Module 2: Discussion Questions (1/4)** | *Explain to participants that they will now be engaging in the facilitated discussions portion of Module 2.*  **Operational Coordination**   1. What plans, policies, and procedures does your institution have in place to guide response efforts at this point?  * What are your mid-term response priorities?   [Facilitator Note: The emphasis of this question should be how priorities have changed compared to Module 1]   1. How would your institution maintain an effective command structure to coordinate cyber response efforts?  * Who are the key decision-makers at this point?   What are their specific roles and responsibilities? |
| **[#]** | **[Insert Time]** | **Module 2: Discussion Questions (1/4)**  **(continued)** | 1. How do key decision-makers collect information on system damages and critical needs? 2. What resources are currently available to support response efforts?  * What plans, agreements, and contingency contracts are in place to address potential system issues?  1. Who are the key external stakeholders that would support response efforts?  * How would your institution coordinate and communicate with these stakeholders?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 2: Discussion Questions (2/4)** | **Cybersecurity**   1. What tools are in place to prevent the remote extraction of information from a network by unauthorized users?  * Who is responsible for assisting the security of the network? * How often are security tests completed?   [Facilitator Note: Ask participants if these tests are conducted on a routine/continuous basis]   1. Do you currently possess sufficient capabilities in-house to investigate and mitigate a potential incident of this type?  * If not, what stakeholders would you engage to address capability gaps?  1. What types of impacts could your institution expect from the potential loss of PII?  * At this point, do you envision any financial and legal consequences?   [Facilitator Note: Note to participants that this could vary between participants depending on the type of PII that is lost]   1. What plans, policies, and procedures exist to ensure students, faculty, and staff engage in information security best practices?  * Who determines these organizational best practices? * How are students, faculty and staff educated about these practices?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 2: Discussion Questions (3/4)** | **Situational Assessment**   1. Have your information needs changed during this phase of the response?  * How are you collecting critical information at this time? * Who do you receive this information from and who do you disseminate this information to? * How are you analyzing and disseminating this information?   Facilitator Note: Ask participants if there is a central hub for accessing information and if everyone has access to that information source]   1. What are the processes for communication and coordination between internal and external partners to support any emerging needs or response requirements? 2. Are there identified reporting requirements for internal stakeholders? For external partners? For leadership and key decision makers?  * What, if any, federal, state, or local reporting requirements must you comply with if impacted by a cyber incident? * Who within your institution is responsible for fulfilling these reporting requirements?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 2: Discussion Questions (4/4)** | **Public Information and Warning**   1. At this point in the scenario, how would your institution be communicating with potentially affected as well as non-affected parties?  * What would your messaging priorities be at this point? * How would your institution ensure messaging is consistent and coordinated throughout the response period? * Who is responsible for delivering this messaging? * How does this messaging accommodate international students and families as well as students with access and functional needs?  1. How does your institution ensure timely and accurate situational updates for external stakeholders (e.g. media) throughout the response period?  * Who is responsible for delivering these updates?   What sort of information is your institution releasing at this point? |
| **[#]** | **[Insert Time]** | **Module 2: Discussion Questions (4/4)**  **(continued)** | [Facilitator Note: The emphasis of these questions should be on how messages are tailored to different audiences]   1. Does your institution have a crisis communications plan or other means of communicating with all stakeholders in case of a disruption or corruption of standard communications?  * How and when does your institution activate its crisis communications plan?  1. [Insert additional discussion questions]   *Announce that we will now be transitioning to a 10-minute break.* |
| **BREAK: [Insert Time – Insert Time] (~ 10 minutes)** |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Slide #** | **Time** | **Slide Title/Content** | **Facilitator Notes** |
| **MODULE 3: SHORT-TERM RECOVERY [Insert Time – Insert Time] (~ 60 minutes)** |  |  |  |
| **[#]** | **[Insert Time]** | **Module 3: Scenario Overview** | *Announce that you will now transition into Module 3.*  *Review the exercise scenario:*   * **[Insert Date and Time + 7 Days]**   + A full analysis of your entire network and associated server logs reveals that the extent of the breach is more extensive than originally suspected; the breach may now include health-related data as well as donor information   + Students, faculty, and staff are expressing concerns regarding their information and are requesting guidance from your institution about what they are doing to protect their personal data   Media outlets continue to report on the breach and begin to feature critical reports on how your institution handled the situation |
| **[#]** | **[Insert Time]** | **Module 3: Discussion Questions (1/4)** | *Explain to participants that they will now be engaging in the facilitated discussions portion of Module 3.*  **Operational Coordination**  How does your institution coordinate the transition from response to short-term recovery efforts? |
| **[#]** | **[Insert Time]** | **Module 3: Discussion Questions (1/4)**  **(continued)** | [Facilitator Note: Note to participants that some of these efforts could overlap and be conducted concurrently. Ask participants if they envision any conflicting priorities]   1. What plans, policies, and procedures guide your institution’s recovery process?  * Who is responsible for coordinating short- and long-term recovery efforts? * What are your institution’s priorities for short-term recovery?   [Facilitator Note: Ask participants to think about their broader recovery goals]   1. What resource gaps could limit your institution’s ability to meet these priorities?  * What community resources or aid agreements could compensate for those gaps?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 3: Discussion Questions (2/4)** | **Cybersecurity**   1. What partnerships does your institution have to support recovery efforts (e.g. cyber insurance) in the aftermath of a cyber incident?  * If none, how would your institution formalize partnerships with the necessary stakeholders? * Who at your institution would be responsible for coordinating these efforts?   [Facilitator Note: Ensure that the focus of this question is on cyber related stakeholders]   1. What are your institution’s plans for the recovery and restoration of critical systems and data that have been compromised as a result of a cyber incident? 2. What strategies would be implemented to mitigate potential negative impacts resulting from stolen and/or leaked PII?  * If you have an established cyber incident response plan, how does it provide guidance for this type of incident recovery?  1. What future cybersecurity measures could you implement to develop more secure systems and protect critical institutional data from a future breach?   [Facilitator Note: Be sure to prompt participants to provide specific examples of these measures]  [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 3: Discussion Questions (3/4)** | **Situational Assessment**   1. What critical decisions would need to be made at this point to inform recovery efforts?  * What are the long-term financial implications of a breach of this nature for your institution?   [Facilitator Note: Ask participants to consider both internal and external financial implications]   1. What legal obligations exist, if any, that may affect how intelligence and information is processed and communicated following a cyber incident?  * How are these legal obligations accounted for in overall recovery efforts? * What stakeholders would likely be involved in this information sharing?  1. Following this type of incident, what decisions or actions would you take to maintain public and institutional confidence?  * What internal or external partners would be engaged in this process? * What leadership decisions would support this process?   [Insert additional discussion questions] |
| **[#]** | **[Insert Time]** | **Module 3: Discussion Questions (4/4)** | **Public Information and Warning**   1. How does your institution ensure consistent, coordinated messaging throughout the recovery period?  * How does your institution’s communications strategy transition from response-oriented to recovery-oriented messaging? * Who is responsible for monitoring and managing inquiries from students, faculty, staff, and alumni? * How does this messaging accommodate international audiences as well as those with access and functional needs?  1. How does your institution provide external stakeholders (e.g. media) with timely updates concerning recovery efforts?   [Facilitator Note: Ask participants how they would account for communicating recovery goals and priorities to these stakeholders] |
| **[#]** | **[Insert Time]** | **Module 3: Discussion Questions (4/4)**  **(continued)** | 1. How would you maintain overall brand reputation for an incident involving a cyber breach?  * How would potentially false or misleading information be handled? * How would potentially sensitive or classified information be handled?   [Facilitator Note: Ask participants if anyone at their campus has the necessary qualifications to handle and process classified information]   1. How are students, faculty, and staff briefed on protective actions and measures to prevent future cyber incidents? 2. [Insert additional discussion questions]   *Announce that this is the End of the Exercise and that you will now transition to a brief 15-minute hot wash.* |
|  |  |  | **ENDEX** |
| **HOT WASH, [Insert Time – Insert Time] (~ 15 minutes)** |  |  |  |
| **[#]** | **[Insert Time]** | **Hot Wash Overview** | *Review the purpose of the Hot Wash noting that it is an opportunity for participants to provide candid feedback on their overall performance as well as the overall delivery of the exercise* |
| **CLOSING REMARKS, [Insert time – Insert Time] (~ 10 minutes)** |  |  |  |
| **[#]** | **[Insert Time]** | **Closing Remarks** | *Thank players for their participation in the exercise. Introduce any additional speakers who will provide closing remarks.* |
| **ADJOURN, [Insert Time]** |  |  |  |