Campus Resilience Program
Exercise Starter Kit

Cyber Breach Tabletop Exercise

Exercise Conduct Briefing

[Insert Date]

FEMA

Sponsor Logo

Office of
Academic
Engagement

READ FIRST

- The purpose of this Exercise Conduct Briefing is to provide a baseline exercise document that institutions of higher education can use to assess their emergency plans, policies, and procedures
- The sample content contained in this document can be tailored as necessary by filling in all [bracketed content that is highlighted in red]
- To insert the sponsoring organization’s logo, navigate to the “View” menu and select “Slide Master”
- This briefing is to be used in tandem with the Cyber Breach Situation Manual and Facilitator Guide so any changes made to this briefing will need to be aligned with those documents

****Delete slide prior to conduct****

Welcome and Introductions

[Name]

[Title]

[Department/Agency/Organization]

[Name]

[Title]

[Department/Agency/Organization]

Sponsor Logo

Administrative Remarks

- Cell phone etiquette
- Evacuation procedures
- Restroom locations

FEMA

Sponsor Logo

Office of Academic Engagement

Exercise Schedule

Activity	Time
[Welcome and Introductions]	[00:00 a.m.]
[Exercise Overview]	[00:00 a.m.]
Module 1: Initial Response	[00:00 a.m.]
Break	[00:00 a.m.]
Module 2: Extended Response	[00:00 p.m.]
Break	[00:00 p.m.]
Module 3: Short-Term Recovery	[00:00 p.m.]
[Exercise Hot Wash]	[00:00 p.m.]
[Closing Remarks]	[00:00 p.m.]

Exercise Overview

Exercise Overview

Background:

- This Tabletop Exercise (TTX) is made available through the Campus Resilience (CR) Program Exercise Starter Kits
- 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

Purpose:

- This specific Exercise Starter Kit will provide the opportunity to examine response and recovery operations related to cyber breach targeted against institutional data

Exercise Overview (cont.)

Scope:

- This [insert duration]-TTX is divided into three Modules:
  - **Module 1** will examine immediate response operations four hours following the initial notification of a cyber breach
  - **Module 2** will examine extended response operations up to 36 hours following the notification of a cyber breach
  - **Module 3** will examine short-term recovery operations seven days following the notification of a cyber breach
- Each Module will consist of two activities:
  1. **Scenario Overview:** Each Module will contain a detailed overview of the scenario
  2. **Facilitated Discussions:** Participants will engage in facilitated discussions surrounding a set of discussion questions

FEMA

Sponsor Logo

Office of Academic Engagement

READ FIRST

- The exercise objectives contained in the following slide(s) are provided as sample objectives
- These can be tailored as appropriate to align with the overarching goals and desired outcomes for the exercise
- Please note that changes made to these objectives will need to be reflected in the associated Facilitator Guide and Situation Manual for this scenario

****Delete slide prior to conduct****

Exercise Objectives

1. **Operational Coordination:** Assess the ability to establish an effective command structure that integrates all critical stakeholders to ensure campus and community resources are used efficiently to respond to and recover from a cyber incident
2. **Cybersecurity:** Evaluate existing capabilities to protect and restore electronic systems, networks, information, and services from damage, unauthorized use, and exploitation during a cyber incident
3. **Situational Awareness:** Examine the ability to provide timely and relevant information regarding the cyber incident to critical campus and community decision-makers
4. **Public Information and Warning:** Assess the ability to deliver coordinated, actionable, and timely information to critical partners and stakeholders when faced with a cyber incident targeting institutional operations

Sponsor Logo

Participant Roles and Responsibilities

- **Facilitator:** Provides situation updates and facilitates discussions
- **Players:** Respond to the situation presented based on current plans, policies, and procedures
- **Observers:** Visit or view selected segments of the exercise without directly engaging in exercise discussions
- **Support Staff:** Performs administrative and logistical support during the exercise (e.g., registration)
- [Insert additional participant roles as appropriate]

Participating Organizations

- [Insert Participating Organization]
  - [Insert Participating Sub-Organization]
- [Insert Participating Organization]
  - [Insert Participating Sub-Organization]
- [Insert Participating Organization]
  - [Insert Participating Sub-Organization]

Exercise Guidelines

- This exercise is being conducted in an **open, low-stress, no-fault environment**; varying viewpoints, even disagreements, are expected
- Act in real-world roles for your institution or organization when considering the scenario
- Decisions are **not precedent-setting**; this is an open discussion
- The focus should be on **identifying suggestions and recommended actions** for improving preparedness, response, and recovery efforts
- [Insert any additional guidelines that may be relevant to the exercise]

Assumptions and Artificialities

- The exercise **scenario is plausible** and events occur as they are presented
- Players will use **existing plans, policies, procedures, and resources** to guide responses
- There is **no "hidden agenda"** nor are there any trick questions
- The scenario assumes certain player actions as it moves through each phase; players should first discuss the actions stipulated by the scenario
- Players are welcome to engage in **"what if" discussions** of alternative scenario conditions
- [Insert any additional assumptions or artificialities that may be relevant to the exercise]

Sponsor Logo

Start of Exercise

Module 1: Initial Response

Module 1: Background

- In recent years, malicious cyber actors have targeted colleges and universities with cybercrime activities
- An additional emerging threat facing institutions of higher education includes cyber espionage in an attempt to gain access to scientific and medical research as well as potentially sensitive government and private-sector research information
- College and university networks may present an easier target for cyber espionage actors due to multiple levels of connectivity and accessibility
- Furthermore, they present an easier target due to lower cyber security awareness among students, faculty, and staff

Module 1: Scenario Overview

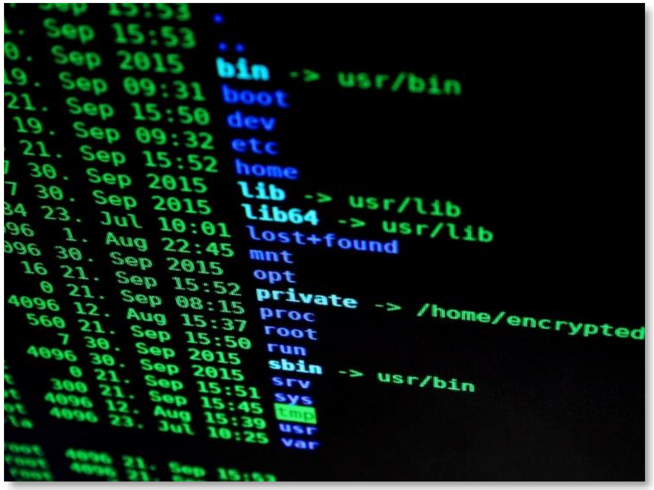
[Insert Date and Time]

- Your institution’s Chief Information Security Officer is contacted by a Special Agent from the Cyber Division at the FBI
- The agent states that a cyber attack has been launched against your institution’s network by an outside entity and currently the duration, scope, and source of the attack is not clear
- An initial investigation reveals the presence of an advanced persistent threat (APT) that appears to be consistent with malware known to be associated with other university attacks

Module 1: Scenario Overview (cont.)

[Insert Date and Time + 4 Hours]

- By this time, 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
- A thorough analysis of the entire institution network has been initiated but may take a day or more to complete



```
   1. Sep 15:53  .
   0. Sep 2015   ..
  19. Sep 09:31  bin -> usr/bin
  21. Sep 15:50  boot
  19. Sep 09:32  dev
  21. Sep 15:52  etc
  30. Sep 2015   home
7 30. Sep 2015   lib -> usr/lib
34 23. Jul 10:01 lib64 -> usr/lib
96  1. Aug 22:45 lost+found
096 30. Sep 2015 mnt
16 21. Sep 15:52 opt
 0 21. Sep 08:15 private -> /home/encrypted
4096 12. Aug 15:37 proc
560 21. Sep 15:50 root
  7 30. Sep 2015 run
4096 30. Sep 2015 sbin -> usr/bin
  0 21. Sep 15:51 srv
300 21. Sep 15:45 sys
4096 12. Aug 15:39 tmp
4096 23. Jul 10:25 usr
                   var
```

Module 1: Discussion Questions (1/4)

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?
3. How would your institution establish a command structure to coordinate your immediate response efforts?
4. What resource gaps could limit your institution’s ability to respond to a cyber attack?
5. [Insert additional discussion questions as appropriate]

Module 1: Discussion Questions (2/4)

Cybersecurity

1. Does your institution have a formalized cyber incident response plan?
2. Does your institution's response strategy outline how to align broader response efforts with ongoing security management and IT efforts?
3. What steps will your institution take to verify the likelihood of a data breach resulting in the release of PII?
4. What measures are in place to protect confidential, personal, financial, and academic information concerning students, faculty, staff, and alumni from a potential cyber incident?
5. [Insert additional discussion questions as appropriate]

FEMA

Sponsor Logo

Office of Academic Engagement

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?
2. How do you conduct initial decision-making and offer decision-making recommendations to senior leadership?
3. 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)?
4. [Insert additional discussion questions as appropriate]

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?
2. What individual, office, or department coordinates and delivers your institution's messaging?
3. How will your institution use social media platforms in support of incident communications and messaging?
4. At this point in the scenario, would your institution notify non-affected members of the campus community?
5. [Insert additional discussion questions as appropriate]

FEMA

Sponsor Logo

Office of Academic Engagement

Break

Module 2: Extended Response

Module 2: Scenario Overview

[Insert Date and Time + 12 Hours]

- A second intrusion has been detected on your institution's network
- During the investigation, a malware variant used to exfiltrate personally identifiable information was discovered on several computers in the 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
- Data appears to have been exfiltrated over several months

FEMA

Sponsor Logo

Office of Academic Engagement

Module 2: Scenario Overview (cont.)

[Insert Date and Time + 36 Hours]

- Local news outlets begin contacting your public affairs office in response to reports that a data breach has occurred at your institution
- Reporters note that they have heard that the personal information of hundreds of students, faculty, and staff has been stolen and are requesting more information on the situation
- Students and parents begin contacting your IT department expressing concerns over their personal information

Module 2: Discussion Questions (1/4)

Operational Coordination

1. What plans, policies, and procedures does your institution have in place to guide response efforts at this point?
2. How would your institution maintain an effective command structure to coordinate cyber response efforts?
3. How do key decision-makers collect information on system damages and critical needs?
4. What resources are currently available to support response efforts?
5. Who are the key external stakeholders that would support response efforts?
6. [Insert additional discussion questions as appropriate]

FEMA

Sponsor Logo

Office of Academic Engagement

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?
2. Do you currently possess sufficient capabilities in-house to investigate and mitigate a potential incident of this type?
3. What types of impacts could your institution expect from the potential loss of PII?
4. What plans, policies, and procedures exist to ensure students, faculty, and staff engage in information security best practices?
5. [Insert additional discussion questions as appropriate]

Module 2: Discussion Questions (3/4)

Situational Assessment

1. Have your information needs changed during this phase of the response?
2. What are the processes for communication and coordination between internal and external partners to support any emerging needs or response requirements?
3. Are there identified reporting requirements for internal stakeholders? For external partners? For leadership and key decision-makers?
4. [Insert additional discussion questions as appropriate]

FEMA

Sponsor Logo

Office of Academic Engagement

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?
2. How does your institution ensure timely and accurate situational updates for external stakeholders (e.g., media) throughout the response period?
3. 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?
4. [Insert additional discussion questions as appropriate]

FEMA

Sponsor Logo

Office of Academic Engagement

Break

Module 3: Short-Term Recovery

Module 3: Scenario Overview

[Insert Date and Time + 7 Days]

- A full analysis of the entire network reveals that the scope of the data breach is more extensive than previously suspected
- Health-related data and donor information appears to have also been compromised
- Students, faculty, and staff express concerns over their personal information and inquire about what your institution is doing to protect their data
- Media outlets reporting on the breach highlight stories criticizing the way your institution handled the situation

Module 3: Discussion Questions (1/4)

Operational Coordination

1. How does your institution coordinate the transition from response to short-term recovery efforts?
2. What plans, policies, and procedures guide your institution's recovery process?
3. What resource gaps could limit your institution's ability to meet these priorities?
4. [Insert additional discussion questions as appropriate]

FEMA

Sponsor Logo

Office of Academic Engagement

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?
2. 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 related incident?
3. What strategies would be implemented to mitigate potential negative impacts resulting from stolen and/or leaked PII?
4. What future cybersecurity measures could you implement to develop more secure systems and protect critical institutional data from a future breach?
5. [Insert additional discussion questions as appropriate]

Module 3: Discussion Questions (3/4)

Situational Assessment

1. What critical decisions would need to be made at this point to inform recovery efforts?
2. What legal obligations exist, if any, that may affect how intelligence and information is processed and communicated following a cyber related incident?
3. Following this type of incident, what decisions or actions would you take to maintain public and institutional confidence?
4. [Insert additional discussion questions as appropriate]

Module 3: Discussion Questions (4/4)

Public Information and Warning

1. How does your institution ensure consistent, coordinated public messaging throughout the recovery period?
2. How does your institution provide external stakeholders (e.g., media) with timely updates concerning recovery efforts?
3. How would you maintain overall brand reputation for an incident involving a cyber breach?
4. How are students, faculty, and staff briefed on protective actions and measures to prevent future cyber incidents?
5. [Insert additional discussion questions as appropriate]

End of Exercise

Exercise Hot Wash

Hot Wash Overview

- This Hot Wash aims to capture the following information based on observations made throughout the exercise:
  - Overall strengths
  - Overall areas for improvement
  - Major takeaways and action items

Closing Remarks

[Name]

[Title]

[Department/Agency/Organization]

[Name]

[Title]

[Department/Agency/Organization]

FEMA

Sponsor Logo

Office of
Academic
Engagement

Adjournment

Campus Resilience Program
Exercise Starter Kit

Cyber Breach Tabletop Exercise

Exercise Conduct Briefing

[Insert Date]

FEMA

Sponsor Logo

Office of
Academic
Engagement