


National Tabletop Exercise for Institutions of Higher Education

Situation Manual

October 27, 2015

FEMA

EXERCISE OVERVIEW

Exercise Name	National Tabletop Exercise for Institutions of Higher Education (IHEs)
Exercise Dates	October 26-27, 2015
Scope	This is a discussion-based exercise lasting approximately four hours.
Mission Areas	Response and Recovery
Core Capabilities	Planning, Operational Coordination, Intelligence and Information Sharing, Public Information and Warning
Objectives	1. Identify common strengths and areas for improvement when responding to a cyber-incident that threatens the confidentiality, integrity, or availability of university or college information assets, with specific focus on maintaining operational resiliency (academic instruction, essential campus functions, events, and services). 2. Examine processes, policies and procedures specific to cyber incidents or data breaches involving international students, campuses, research, and/or other assets. 3. Assess plans, protocols, and procedures for IHEs to collaborate operationally with sector-specific organizations, federal, state, local, tribal and territorial authorities, as well as private sector cyber incident response services. 4. Examine processes and tools for IHEs to collect and share cyber-related intelligence and/or specific threat information, (both internally and with external partners and stakeholders) to ensure timely and appropriate information reaches those who must act upon it. 5. Assess processes and capabilities to develop timely and appropriate communication for multiple IHE stakeholder communities to include: media, students, faculty and staff, family members and alumni, as well as relevant external business partners.
Threat/Hazard	Cyber-attack.
Scenario	University or college networks are compromised by criminals and/or nation-
Sponsors	Department of Homeland Security/Federal Emergency Management Agency/National Exercise Division, Department of Homeland Security/Science and Technology Directorate, Department of Homeland Security/Office of Academic Engagement
Participating Organizations	Participants are drawn from incident response teams and leadership groups at various Institutions of Higher Education from across the Nation.

Points of Contact

Lauren Kielsmeier
Department of Homeland Security/Office of Academic Engagement
202-282-8162
lauren.kielsmeier@hq.dhs.gov

Douglas Maughan
Department of Homeland Security/Science and Technology Directorate
202-254-6145
douglas.maughan@hq.dhs.gov

Matt Lyttle
Department of Homeland Security/Federal Emergency Management Agency/National Exercise Division
202-786-9664
matthew.lyttle@fema.dhs.gov

Andrew Peterson
Norwich University Applied Research Institutes
802-485-2761
apeters1@norwich.edu

INTRODUCTION

The U.S. Department of Homeland Security/Federal Emergency Management Agency/National Exercise Division, Department of Homeland Security/Science and Technology Directorate and the Department of Homeland Security/Office of Academic Engagement are pleased to sponsor a National Tabletop Exercise for Institutions of Higher Education. This event was designed and made possible through extensive collaboration with federal, state, local and tribal partners as well as key participants from multiple Institutions of Higher Education, the Universities and Colleges Caucus of the International Association of Emergency Managers, the International Association of Campus Law Enforcement Administrators, and the University and College Police Section of the International Association of Chiefs of Police. This Situation Manual provides goals and objectives for the exercise, scenario details, and general issues for discussion during the exercise.

Goal

The Homeland Security Academic Advisory Council recommends that the Department of Homeland Security develop and conduct more exercise activities focused specifically on Institutions of Higher Education. This event has been developed to address that recommendation. This exercise is the second in a series of national campus-based exercises to test and promote campus resilience. In particular, the National Tabletop Exercise for Institutions of Higher Education is meant to promote the White House's all-hazards *Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education* and provide insight into common planning, preparedness, and resilience best practices and shortfalls of the academic community when a significant cyber-incident occurs.

Objectives

The following objectives have been designed for this exercise, each highlighting the Core Capabilities listed in the National Preparedness Goal:

1. **Planning (Continuity).** Identify common strengths and areas for improvement when responding to a cyber-incident that threatens the confidentiality, integrity, or availability of university or college information assets, with specific focus on maintaining operational resiliency (academic instruction, essential campus functions, events, and services).
2. **Planning (Consideration of Global Activities).** Examine processes, policies and procedures specific to cyber incidents or data breaches involving international students, campuses, research, and/or other assets.
3. **Operational Coordination.** Assess plans, protocols, and procedures for IHEs to collaborate operationally with sector-specific organizations, local, state, and federal authorities, and private sector cyber incident response services.
4. **Intelligence and Information Sharing.** Examine processes and tools for IHEs to collect and share cyber-related intelligence and/or specific threat information, (both internally and with external partners and stakeholders) to ensure timely and appropriate information

reaches those who must act upon it.

5. **Public Information and Warning**. Assess processes and capabilities to develop timely and appropriate communication for multiple IHE stakeholder communities to include: media, students, faculty and staff, family members and alumni, as well as external business partners

Format

The National Tabletop Exercise for Institutions of Higher Education is a tabletop exercise consisting of three modules. The first module will feature discussion related to the response to a cyber-attack that has targeted the institution's research and intellectual property. In the second module, participants will be asked to discuss the response and recovery actions required after discovering that the personally identifiable information of students and faculty has also been breached. In the third and final module, teams must consider the potential impact to the institutional business model as evidence indicates that highly sensitive records from the Alumni and Donor Relations databases have been compromised. A facilitator will lead players through plenary discussion of issues raised by the scenario, which will alternate with player-led discussions at their own tables. A separate 30-minute hotwash session will follow.

Participants

Players respond to the scenario presented based on their professional insight, experience, and knowledge of institutional plans, policies, and procedures. Players for this exercise are drawn from key leadership elements and incident response team functions from a wide variety of Institutions of Higher Education. Each institution will be represented by three-to-five players. Representatives from two or more Institutions of Higher Education will be seated at a given table to encourage exchange of ideas.

A **Lead Facilitator** will present the scenario, guide players through plenary discussions, and call upon players to report on discussions held at their tables regarding assigned issues.

Subject-Matter Experts from local, state, and federal agencies will observe the exercise and may be called upon by the Lead Facilitator to describe or clarify their authorities, protocols, or possible response actions.

A **Lead Evaluator** will monitor plenary discussions and collect feedback from players to evaluate whether the exercise has met its objectives and to identify opportunities to improve the preparedness of Institutions of Higher Education and future exercises.

Note-takers at each table will assist the Lead Evaluator in capturing exercise discussions.

Evaluation

The Lead Evaluator will deliver a draft Summary Report to the National Exercise Division in November. The Summary Report will document key discussion points, strengths, and areas for improvement in Institution of Higher Education preparedness and resilience with regard to cyber incident response.

The Summary Report will draw upon direct observations of the Lead Evaluator, notes from the note-takers assigned to each table, Participant Feedback Forms collected following the exercise, and online Pre- and Post-Event Surveys. The Participant Feedback Form allows for input on exercise strengths and areas for improvement as well as comments on the exercise scenario, materials, facilitation, and presentation.

Player Guidelines

The National Tabletop Exercise for Institutions of Higher Education will be held in an open, low-stress, no-fault, and non-attribution environment. Varying viewpoints and disagreements are expected.

Players should respond to the situation presented based on their knowledge and insights related to their respective institution's current resources, plans, and procedures.

Decisions are not precedent-setting and may not reflect your organization's final position on an issue. The exercise is exploratory. The goal is to identify not only issues but also multiple options and possible solutions.

To prepare for exercise conduct, players should familiarize themselves with the scenario developments and discussion questions in this document.

To conserve time for discussions, the Lead Facilitator will present only a very brief summary of scenario developments at each stage of the exercise. Following each scenario summary, the Lead Facilitator will assign an issue area to one or more tables for table-specific discussions. The Lead Facilitator will call on some tables to report to the plenary on their proposed approaches and sense of key challenges.

In deliberations at their tables, participants will not be expected to address every discussion question presented in this document. Participants will be asked to address the broad, open-ended question associated with each issue area. However, more specific questions are provided for consideration to help prompt thinking and discussion, if needed.

Assumptions and Artificialities

The scenario designed for the National Tabletop Exercise for Institutions of Higher Education is presented as a simplified version of a highly complex situation in the interest of achieving exercise objectives. During the exercise, the following assumptions and artificialities apply:

1. Any malware variants, criminal organizations or nation state actors described in the scenario are nondescript and fictitious.
2. This is a high-level discussion-based exercise focused on the strategic response to a cyber-incident. Rather than attempting to recreate the multifarious and highly technical components of an actual cyber-attack, this exercise and supporting scenario are designed to focus on the organization's response action from a leadership perspective. As such, exercise developers have attempted to provide enough relevant detail for participants to make sound business decisions without delving into the specific technical details and forensic activities that would likely be associated with an actual network breach.

MODULE 1: Cyber-Espionage Attack

The following section includes scenario context for National Tabletop Exercise for Institutions of Higher Education discussions regarding the response to a significant cyber incident affecting the institution's network. Discussion questions are also included. Participants should be prepared to address the broad, open-ended questions associated with each issue area. However, more specific questions are provided to help prompt discussion, if needed.

Background Intelligence and Initial Notification of Network Breach

Background

In recent years, malicious cyber actors have targeted universities and colleges with typical cybercrime activities, such as spear phishing students and faculty with university- or college-themed messages, creating fake university or college websites, and infecting computers with malicious software—often in an attempt to gain access to student and faculty e-mail, personally identifiable information (PII), as well as financial records and payment systems.

While malicious cyber actors continue to exploit university and college networks for financial gain, an emerging threat facing Institutions of Higher Education is nation-state actors conducting cyber-espionage. In addition to innovative scientific and medical research, universities and colleges are often involved in sensitive government and private sector research projects. These associations are very appealing to cyber-espionage actors looking to gain access to sensitive research programs to exfiltrate information. University and college networks, which often have multiple levels of connectivity and accessibility to fuel collaboration, may present an easier target for cyber-espionage actors than sensitive government or private industry networks.

Initial Notification of Breach

On Friday, October 30 at 10:10 a.m., your institution's Chief Information Security Officer is contacted by a Special Agent from the Cyber Division of the Federal Bureau of Investigation (FBI). The agent states that a cyber-attack has been launched against your institution network by an outside entity. At this time, the precise duration, scope, and source of the attack are not completely clear.

Working in collaboration with the FBI, the initial investigation quickly reveals the presence of an advanced persistent threat (APT) that appears to be consistent with sophisticated malware that has been previously used by a specific nation-state to access critical institution research data and proprietary information.

By 1:30 p.m. the same day, enough evidence is discovered to determine the attack was initiated at least six months prior, and during the time following, the attackers had free and unlimited access to all networks, databases, servers, and other sensitive resources associated with STEM departments and colleges. While exfiltration of data cannot be confirmed at this time, it is reasonable to assume it has occurred and sensitive information has been compromised.

While the attack appears to specifically target research data within the STEM departments and colleges, a thorough analysis of the entire institution network is underway. This process may take a day or more to complete.

Module 1: Discussion Questions

Operational Coordination

1. Having been alerted by the FBI about this attack, what are your initial concerns and what immediate actions would your institution take to begin response/mitigation actions?

   Specifically, consider the following questions:

   - Does your institution have a formalized cyber-incident response plan?
     - Where is the plan documented, and who has access?
     - Does the plan specifically address this type of incident?
     - How often is the plan reviewed, updated, or exercised?
   - Based on the information you currently have, would you convene an incident response team?
     - If so, what functions would likely be represented, and who would lead the team?
     - How and when would senior leadership of the institution be notified?
   - Do you have sufficient capabilities in-house to investigate and mitigate a significant cyber breach?

Public Information and Warning

2. At what point do you communicate news of the breach to faculty, students, or other institution stakeholders?

   Specifically, consider the following questions:

   - What information do you communicate?
   - Are there or should there be limits on the details that are released to the public?

3. Must notifications be made to governing bodies (Board of Regents/Trustees, chancellor, governor) and what information will you provide?

Planning (Continuity)

4. How might the loss or potential loss of research data or intellectual property impact your institution?

   Specifically, consider the following questions:

   - Was the most sensitive data encrypted, and therefore should be safe?
   - Do you have measures in place to determine if sensitive data has been altered as a result of this attack?
   - How might your institution be impacted by corruption of research databases such that it renders the research inaccessible or unusable?
   - What are your obligations related to research sponsors and/or granting agencies?

5. What types of specific information would be documented relating to your institution's response action? Who would be responsible for this process?
6. In the event the targeted institution networks warrant removal from the internet for a period of days in order to secure and recover systems, what steps would your institution have to take to ensure continuity of essential functions?

   Specifically, consider the following questions:

   - At what point would you elect to take some networks off line? What are the specific triggers or thresholds for such a decision?
   - Is there a business continuity plan in place to provide guidance in such a situation?

Intelligence and Information Sharing

7. How does your institution collect and share threat intelligence that may be useful in mitigating cyber threat risk?

   Specifically, consider the following questions:

   - Are you a member of the Research and Education Network Information Sharing and Analysis Center (REN-ISAC)?
   - Have you developed a relationship with your local FBI field office or other law enforcement agency to help stay informed of current threats?
   - Do any members of your Information Technology staff have standing security clearances that would permit the sharing of classified threat information from the FBI or other law enforcement agencies?

MODULE 2: Student / Faculty PII Breach

The following section includes scenario context for National Tabletop Exercise for Institutions of Higher Education discussions regarding escalation of a cyber-incident affecting the institution's network. Discussion questions are also included. Participants should be prepared to address the broad, open-ended question associated with each issue area. However, more specific questions are provided for consideration to help prompt discussion, if needed.

October 31, 2015: Discovery of Unrelated APT on Network

At 9:20 a.m. Saturday morning, you are informed of a second intrusion that has been detected on the institution network. While investigating the initial breach, a malware variant known to be used by cyber criminals to harvest and exfiltrate personally identifiable information was discovered on several institution computers, to include workstations in the Office of Human Resources, the Office of Enrollment Services, and the International Students and Scholars Office. The source and duration of this attack is currently unknown, and it is unclear if this breach is the result of a separate attack or if it is connected to the previous attack.

By 10:15 a.m. 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. Further examination of web server logs indicates large amounts of data related to students, faculty and staff has been exfiltrated over a period of several months. Evidence suggests the stolen data includes the name, address, date of birth, and social security number of all faculty, staff, and students (domestic and international) from 2005 to present.

At 10:30 a.m., the institution implements its internal communications plan to provide initial notification of the intrusion and its response strategy, including credit monitoring for affected individuals. The notification is sent to all current faculty, staff, and students (domestic and international) via the school's emergency alert system.

By 10:45 a.m., alerted by the institution's internal communications plan, more than 50 F-1 and J-1 engineering students from Country X and Country Y petition to meet with the Academic Dean of the Engineering Department. During the meeting the students inform the administration that they had previously received panicked phone calls and emails from their parents. In all cases, the overseas parent families have been informed, in their native language, that their child is in trouble at the institution and that unless money is sent immediately to a local address, their child's visa will be revoked and they will be deported.

The institution's internal communications made this student group realize that the hackers or affiliates were attempting to use the data to extort money from families outside of the United States.

After investigating, the institution realizes that the theft of student PII included the theft of international students' overseas addresses and phone numbers, which allowed the hackers to contact vulnerable overseas families. Although the investigation is ongoing, it appears that the

Alumni and Donor Relations databases were also targeted by the attackers. At this point however, there is no evidence to indicate that any related records or files contained in those systems have been compromised.

Module 2: Discussion Questions

Public Information and Warning

1. Based on the current information, are you at the point where a public statement should be made to stakeholders or the press?

   Specifically, consider the following questions:

   - What information would you likely disclose, who will speak for your institution, and how will you get your message out (press, website, social media, call center)?
   - Did the institution communicate the hack of student information in a timely fashion? What departments did you coordinate with on the communications?
   - Did the institution's strategic communication crisis plan include messaging for parents? What medium was considered/used? What languages were used?
   - Who on the institution's leadership team informs what government agency of this implication? Is there a need for a standardized communications protocol?
   - Will this incident require formal notifications under applicable law? If so, who must be notified, what is the timeline, and who will make the required notifications?
     - What is the notification requirement and/or notification protocol for potential identity theft victims (faculty/staff, students?)
     - How will you locate former faculty and/or students for whom you may not have current contact information?
2. What law enforcement entities should be contacted?
3. Should foreign embassies be contacted? Who should coordinate this effort? Can US embassies be used as conduits to foreign governments and foreign press?

Planning (Continuity)

2. If you have an established cyber incident response plan, does the plan specifically address this type of incident?
   - Will you call in any additional or different response team members at this point?
3. How might this breach impact essential campus functions, events and services?

   Specifically, consider the following questions:

   - At what point might you elect to take the entire institution network off line? What are the potential triggers or thresholds for such a decision?
   - How would you communicate any potential disruptions to faculty and students?
   - What steps would be required to maintain essential campus functions in the event of a complete network shutdown (i.e. online classes, purchasing, payroll, etc.)?

4. What risks might this breach pose for your brand, and how would you begin to mitigate them?

   Specifically, consider the following questions:

   - Will you release any information to the public at this point?
   - What processes do you have in place to monitor and respond to traditional and social media?
   - What guidance do you issue internally to control external communication?
   - Does your institution have a relationship or an agreement with an external marketing or public relations firm to assist in external communications and/or brand protection?
   - Do you have a contract with a third party to provide victim notification and identification protection services?
   - What types of support or protective services would you make available to data breach victims, and for how long?
   - Due to the uncertainty about whether or not donor information has been breached, should the institution begin discussing plans based on that scenario?

MODULE 3: Extent of Data Breach Realized

The following section includes scenario context for National Tabletop Exercise for Institutions of Higher Education discussions regarding further escalation of a cyber-incident affecting the institution's network. Discussion questions are also included. Participants should be prepared to address the broad, open-ended question associated with each issue area. However, more specific questions are provided for consideration to help prompt discussion, if needed.

November 1, 2015: Discovery of Alumni / Donor Records Exfiltration

By 2:20 p.m. Sunday, a full and thorough analysis of the entire institution network and associated web server logs reveals that the scope of the data breach is even more extensive than previously suspected. Perhaps the most alarming and potentially damaging discovery is that the databases associated with the institution's Alumni and Donor Relations Offices have been completely exfiltrated, compromising individual PII, and a multitude of other highly sensitive details related to hundreds of past donors as well as all active donor prospects.

Module 3: Discussion Questions

Operational Coordination

1. Are there additional response team members who might be called in now?
2. What unique measures or special considerations might your institution take with regard to dealing with a breach of donor information?

Specifically, consider the following questions:

- What is the potential impact if donor information is disclosed or trafficked among cyber criminals? Consider donor PII, donation history, target donation figures, or other sensitive notes, files, and correspondence that may be kept on key alumni and/or donors.
- How might a breach of this magnitude impact your long-range business model?
- At what point do you contact those affected by this breach? What do you communicate, and who will initiate the contact?

3. After resolution of the event, who will run the after action or post mortem session? What changes will there be to compliance and governance?

Public Information and Warning

4. What notification, if any, is made public now?
5. Are there any notifications required by law?
6. What steps would you take to prevent a premature leak of the breach details?

Planning (Continuity)

7. Does the administration have concerns about creating public records (emails, notes, investigative reports, and other related documents) as it works through the crisis? How would administration communicate those concerns to the response team?
8. Does your institution budget in advance for cyber breaches (consider the cost of IT forensics and consultants; legal counsel; call centers, websites and mailings; identity protection and credit-check services; or possible litigation)?
9. Has your institution explored the possibility of acquiring cyber-security insurance?
10. Does your institution regularly utilize commercial penetration testing or other data security services?
11. Do you have a cyber-security attorney on retainer?
12. How might your institution better collect and share threat intelligence that may be useful in preventing a future cyber incident?

END OF MODULE 3
END OF EXERCISE