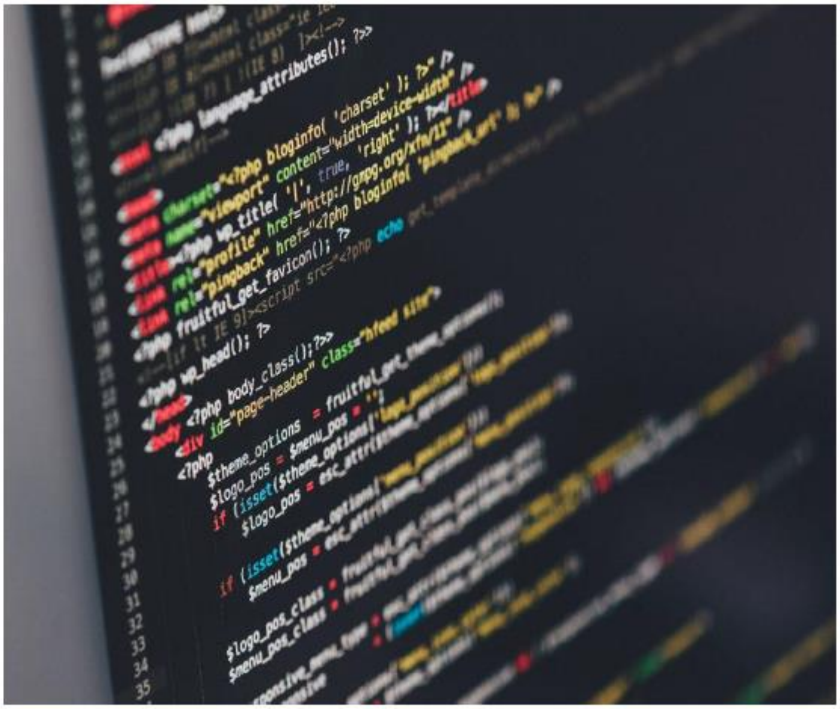


2017 National Seminar and Tabletop Exercise for Institutions of Higher Education

Situation Manual

October 10-11, 2017

THE UNIVERSITY OF UTAH
S.J. QUINNEY
COLLEGE OF LAW

U.S. DEPARTMENT OF HOMELAND SECURITY

CAMPUS RESILIENCE PROGRAM
OFFICE OF ACADEMIC ENGAGEMENT

Handling Instructions

The title of this document is the *2017 National Seminar and Tabletop Exercise for Institutions of Higher Education Situation Manual*. This Situation Manual reflects the information provided to the exercise planning team as of the date of publication and may be modified prior to execution at the direction of the Exercise Director.

This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. This report is FOR DISCUSSION PURPOSES ONLY and should be handled as sensitive information not intended for any other use. Reproduction of this document, in whole or in part, is permissible but should be done with consideration for the sensitivity of its content.

For more information on this exercise, please consult the following point of contact:

Trent Frazier
Executive Director
Department of Homeland Security
Office of Academic Engagement
trent.frazier@hq.dhs.gov

Jennifer Lynch
Emergency Management Specialist
Department of Homeland Security/Federal Emergency Management Agency
National Exercise Division
Jennifer.Lynch@fema.dhs.gov

Cover Photos

http://images.umc.utah.edu/netpub/server.np?find&catalog=catalog&template=detail.np&field=itemid&op=matches&value=487360&site=photobank

https://pixabay.com/en/code-code-editor-coding-computer-1839406/

https://pixabay.com/en/car-police-cars-caravan-sirens-red-1531277/

https://www.fema.gov/media-library/assets/images/128682

http://images.umc.utah.edu/netpub/server.np?find&catalog=catalog&template=detail.np&field=itemid&op=matches&value=497770&site=photobank

http://images.umc.utah.edu/netpub/server.np?find&catalog=catalog&template=detail.np&field=itemid&op=matches&value=14254&site=photobank

https://www.fema.gov/media-library/assets/images/71003

OVERVIEW

Exercise Name	2017 National Seminar and Tabletop Exercise for Institutions of Higher Education
Exercise Date	October 10th – 11th, 2017
Scope	This exercise is a part of a two-day event including seminars/workshops and a tabletop exercise (TTX) geared toward examining issues related to cybersecurity impacting physical infrastructure systems on college and university campuses. The TTX portion of the event consists of a scenario-driven, facilitated discussion and is designed to examine roles, responsibilities, authorities, and capabilities to enhance the resilience of institutions of higher education.
Mission Areas	Response and Recovery
Objectives	1. Identify **common strengths and areas for improvement** when responding to a campus infrastructure breakdown or failure caused by cyber attack that threatens the safety and security of college/university students, including international students, and all faculty and staff. 2. Assess **processes and capabilities to develop timely and appropriate communication** for multiple college and university communities during a critical infrastructure failure to maintain public and institutional confidence, including messaging to: students, faculty and staff, family members, media, alumni, and relevant external business partners. 3. Examine **coordinated public health, mass transportation, and residential life services, as well as continuity of operations planning** related to response and recovery from a physical infrastructure systems failure, for on-campus students, staff, and visitors to campus. 4. Examine and assess plans, protocols, and procedures for colleges and universities to **communicate and collaborate on response and recovery operations with co-jurisdictional law enforcement**, sector-specific organizations, local, state, and federal authorities, as well as private sector partners and other stakeholders. 5. Examine **processes and tools for colleges and universities to automate/expedite communication and comprehension** of threat-relevant information, both internally and with external partners and stakeholders, during the response to and recovery from an incident.
Scenario	The scenario consists of a cyber attack that impacts an institution's physical infrastructure systems.
Sponsors	The DHS Office of Academic Engagement (OAE), the FEMA National Preparedness Directorate (NPD) National Exercises Division (NED), the FEMA-NPD Individual & Community Preparedness Division (ICPD), and the University of Utah S.J. Quinney College of Law
Participating Organizations	Participants are drawn from across the campus community including campus emergency response and law enforcement professionals, campus information technology professionals as well as campus leadership and administration at various colleges and universities from across the country (Refer to ***Appendix B*** for a list of participants).

AGENDA

**National Seminar and Tabletop Exercise for
Institutions of Higher Education**

October 10-11, 2017

The University of Utah S.J. Quinney College of Law
383 South University Street, Salt Lake City, UT 84112

Tuesday, October 10th, 2017

Time	Activity	Presenter/Facilitator	Location
7:30 a.m.	**Check-in opens**		**Lobby**
8:30 a.m.	**Welcome/ Introduction/ Keynote**	**Mr. Trent Frazier** Executive Director, DHS Office of Academic Engagement **President David W. Pershing** University of Utah **Governor Gary R. Herbert** State of Utah	**Moot Court Room**
9:10 a.m.	**Introduction to the Exercise**	**Kevin O'Prey, Ph.D.** NED Exercise Support	
9:15 a.m.	*Break / Transition*		
9:30 a.m.	**1st Seminar / Workshop Session**	**Various Speakers**	**2nd Floor:** Room 2100 **3rd Floor:** Rooms 3609, 3603 **4th Floor:** Room 4603 **6th Floor:** Rooms 6619/6613, 6500, 6623
10:30 a.m.	*Break*		
10:45 a.m.	**Exercise Module 1: Cyber Response**	**Kevin O'Prey, Ph.D.** NED Exercise Support **David Waldman** NED Exercise Support **Brian Smith** NED Exercise Support **James Kish** NED Exercise Support	**6th Floor:** Room 6619/6613 **6th Floor:** Room 6623 **6th Floor:** Rooms Flynn Faculty Room **2nd Floor:** Room 2100

Time	Activity	Presenter/Facilitator	Location
12:15 p.m.	*Lunch*		
1:30 p.m.	**2nd Seminar / Workshop Session**	**Various Speakers**	**2nd Floor:** Room 2100 **3rd Floor:** Rooms 3609, 3603 **4th Floor:** Room 4603 **6th Floor:** Rooms 6619/6613, 6500, 6623
2:30 p.m.	*Break*		
2:45 p.m.	**Exercise Module 2: Emergency Response**	**Kevin O'Prey, Ph.D.** NED Exercise Support	**6th Floor:** Room 6619/6613
		David Waldman NED Exercise Support	**6th Floor:** Room 6623
		Brian Smith NED Exercise Support	**6th Floor:** Rooms Flynn Faculty Room
		James Kish NED Exercise Support	**2nd Floor:** Room 2100
4:15 p.m.	*Break*		
4:20 p.m.	**End of Day Remarks**	**Mr. Trent Frazier** **Robert W. Adler** Jefferson B. and Rita E. Fordham Dean and University Distinguished Professor of Law, S.J. Quinney College of Law, University of Utah	**Moot Court Room**
4:30 p.m.	**Information & Networking Session**		**6th Floor**
5:30 p.m.	**End of Day (Adjourn)**		

Wednesday, October 11th, 2017

Time	Activity	Presenter/Facilitator	Location
8:30 a.m.	**Plenary Session / Announcements**	**Mr. Trent Frazier** **Amos Guiora** Professor & 2017 NTTX Event Chair, University of Utah	**Moot Court Room**
8:45 a.m.	**3rd Seminar / Workshop Session**	**Various Speakers**	**2nd Floor:** Room 2100 **3rd Floor:** Rooms 3609, 3603 **4th Floor:** Room 4603 **6th Floor:** Rooms 6619/6613, 6500, 6623
9:45 a.m.	*Break*		
10:00 a.m.	**Exercise Module 3: Recovery**	**Kevin O'Prey, Ph.D.** NED Exercise Support **David Waldman** NED Exercise Support **Brian Smith** NED Exercise Support **James Kish** NED Exercise Support	**6th Floor:** Room 6619/6613 **6th Floor:** Room 6623 **6th Floor:** Rooms Flynn Faculty Room **2nd Floor:** Room 2100
11:30 a.m.	*Break*		
11:45 a.m.	**Plenary Session / After Action Review**	**Kevin O'Prey, Ph.D.** NED Exercise Support **David Waldman** NED Exercise Support **Brian Smith** NED Exercise Support **James Kish** NED Exercise Support	**Moot Court Room**
12:45 p.m.	**Closing Announcements**	**Mr. Trent Frazier**	**Moot Court Room**
1:00 p.m.	**End of Day (Adjourn)**		

TABLE OF CONTENTS

PARTICIPANT INFORMATION AND GUIDANCE

Exercise Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise portion of the event. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

Facilitators

The Facilitator is responsible for guiding overall exercise play, and ensuring that participant discussions remain focused on the objectives of the exercise during the Modules. They also provide additional information and resolve questions as required. They are responsible for making sure different viewpoints are discussed.

Players

Players are personnel who have an active role in discussing their institution's response and recovery activities during the Exercise. Delegations of players respond to the situation presented based on expert knowledge of response procedures, as well as how they would perform their functions on their respective campus.

Observers

While observers do not directly participate in the exercise, they may view selected segments of the exercise. Observers view the exercise from a designated observation area and must remain within the observation area during the exercise.

Support Staff

The exercise support staff includes individuals who perform administrative and logistical support tasks during the exercise (e.g., registration).

Note-Takers

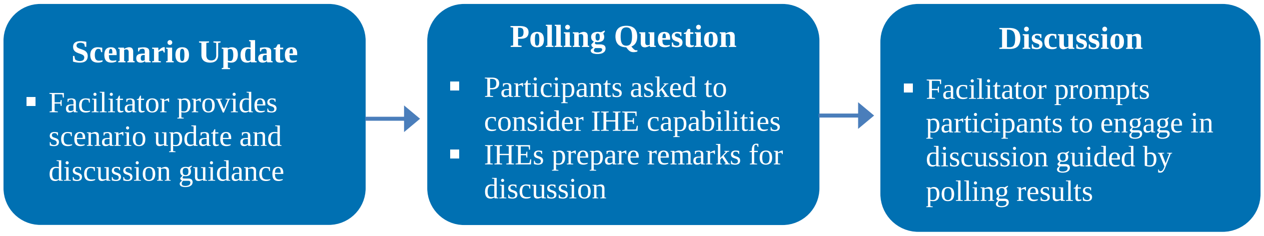
Note-takers will be present during both the Module discussions as well as the Plenary Session to assist with capturing exercise discussions for the Summary Report.

Exercise Structure

The NTTX will consist of three 90-minute exercise modules and three 60-minute seminar sessions. The schedule will alternate between exercise modules and seminar sessions.

Each exercise module consists of three separate activities: a scenario update, polling questions, and group-wide discussions (refer to ***Figure 1***).

Figure 1: Format of Exercise Modules



Scenario Update

- Facilitator provides scenario update and discussion guidance

Polling Question

- Participants asked to consider IHE capabilities
- IHEs prepare remarks for discussion

Discussion

- Facilitator prompts participants to engage in discussion guided by polling results

To begin each Module, the Facilitator will provide a scenario update and general discussion guidance to players. Then each group will be presented with the key topics and associated discussion questions for each Module. Additionally, **IHE delegations will be asked to assess their ability to address each of the issues using handheld polling devices.**

Each institution's assessment will be based on a specific scale which aims to examine the efficacy of each college and university's plans, policies, procedures, and resources relating to each particular issue. This assessment scale is provided in **Figure 2**. The Facilitator will then ask follow-up questions based on the answers provided to further explore key topics addressed in each Module. The results will be consolidated following the completion of all three Modules and will be used to drive discussions during the Plenary Session.

Assessment	Criteria
🟩	My institution can successfully address this issue **without challenges**
🟨	My institution can address this issue, but with **moderate challenges**
🟥	My institution can address this issue, but with **major challenges**
⬛	My institution **does not have the ability** to address this issue

Figure 2: Exercise Assessment Scale

Exercise participants will also be provided a Participant Feedback Form. While key issues and observations from Module discussions will be discussed during the Plenary Session at the conclusion of the exercise, individual players are asked to complete the feedback form to ensure all perspectives on the issues are captured.

The plenary discussion session will be followed by an After Action Review where participants will discuss overall thoughts regarding the exercise. To facilitate the After Action Review discussions, players will also have the ability to answer a variety of questions using handheld polling devices. Answers to polling device questions will be anonymous and non-attributable.

Exercise Guidelines

This exercise will incorporate a scenario-based format that is informed and guided by event objectives. The Modules and questions support achievement of the event objectives by initiating discussions, facilitating decision-making, and examining appropriate response outcomes based on the exercise scenario.

Participants will be acting in their real-world roles in their home institutions when considering the scenario, offering observations and discussing strategic decisions. This approach allows the discussion to focus on situations within a moving timeline and for participants to contribute to the discussion from the perspective of their role in this scenario. The Facilitators will ensure that the scenario moves along at an appropriate pace and that all participants have an opportunity to contribute.

Assumptions and Artificialities

In any exercise, assumptions and artificialities are necessary to complete play in the time allotted and/or to account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to negatively impact their participation.

Assumptions

Assumptions constitute the implied factual foundation for the exercise and, as such, are assumed to be present before the exercise starts. The following assumptions apply to the exercise:

- The exercise scenario is plausible and events occur as they are presented;
- **Players are to respond to the scenario as if events were taking place on their campus**; and,
- Exercise players will use their existing plans, policies, procedures, and resources to conduct response planning and recovery operations.

Artificialities

During this exercise, the following artificialities apply:

- There is no "hidden agenda" nor are there any trick questions; and,
- The scenario assumes certain player actions throughout each of the Modules so players should first discuss the actions stipulated by the scenario; however, players are welcome to engage in "what if" discussions of alternative scenario conditions.

Player Guidelines

The *2017 National Seminar and 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. **Decisions are not precedent-setting and may not reflect your organization's final position on an issue.** The exercise is exploratory and serves to identify issues, as well as multiple options and possible solutions.

To prepare for exercise conduct, players should familiarize themselves with the scenario developments and discussion questions included in this document. There are different sets of discussion questions provided for each Module based on the key issues and concerns that arise during that portion of the scenario. Exercise players should be prepared to speak to some of these major issues and concerns during both the Module discussions and the Plenary Session.

In these discussions as well as during deliberations for each individual delegation, participants will not be expected to address every discussion question presented in this document. Participants will be asked to address the broad, open-ended questions associated with each issue area, and additional questions will be provided for consideration to help prompt thinking and discussion, if needed.

MODULE 1: CYBER RESPONSE

Scenario

September 1, 2017

Your institution has invited a culturally significant religious leader who was recently exiled from his/her country of origin to come speak on your campus. This individual is seeking asylum in the United States and his/her arrival is widely covered by the media. Prior to the event, the political leadership in this individual's country of origin threatens retaliation in response to the event, and specifically calls out your institution for "providing a platform for this individual to spread lies".

Several Weeks Later

Several weeks following the highly publicized speaking event, a supposed leaked document of your institution's records (in the form of an Adobe PDF file) that contains information proving your institution mishandled cases of misconduct is circulated on social media. Multiple individuals employed by your university, as well as students, circulate the PDF file.

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) releases a security alert several days later warning the broader community that a zero-day exploit[1] has been discovered with the ability to compromise systems and exploit a known vulnerability that allows a malicious actor to escalate and maintain privileged access on infected systems.

Tuesday, October 10, 2017

Your institution's IT department receives calls regarding issues with your learning management software; users are experiencing computer issues when logging in to start a session and in some cases their access credentials grant them administrative privileges. Within several hours, data that is housed in the learning management system is either missing or corrupted.

Additionally, several departments, including campus emergency services, report that they have been experiencing degradation in system performance and availability – one of the systems identified in these reports is your campus emergency notification system. That morning, an unauthorized message is pushed out to a large segment of your campus population from an unknown number. The message states "*Emergency Alert: upcoming severe weather affecting university operations. Read more here*". Once individuals click on the hyperlinked message, smartphone browsers connect to a blank webpage which presumably contains malware. The malware causes phones to dial 911 on loop, denying users the ability to end the calls. These looping calls persist until users forcibly shut down their devices.

Around 12:30 PM, your institution is notified by the supervisor at the 911 call-center responsible for managing calls in your area that they are receiving larger than average call volumes from your campus population. According the 911 supervisor, operators are receiving emergency calls that immediately "hang-up" – which they are required to call back to determine if, in fact someone is calling about an emergency. Operators follow up with each call while at the same time responding to legitimate emergency calls.

[1] An exploit directed by using a vulnerability in computer software that is unknown to the vendor of the targeted software. The security flaw is exploited by hackers before the vendor becomes aware and fixes it.

Discussion Questions

Cyber-Incident Planning

1. Does your institution have a formal response plan for each of the types of cyber-incidents described in the scenario?
    a. If so, does your plan contain specific processes and procedures for addressing the types of incidents?
    b. If so, does your plan clearly outline what individuals/positions are involved in the response efforts and how they are expected to coordinate with one another?
    c. If so, do you periodically test your plan and train staff?
    d. If so, does your plan define escalation and prioritization of efforts to manage and coordinate IT, operational, and business recovery?
2. What are your institution's top three priorities at the time of this series of attacks?
    a. Does your institution's response strategy include aligning response efforts with security management and IT engineering initiatives?
3. What resources do your response teams have to address this system/network compromise?
    a. Do these include backup systems?
    b. What resources outside of your institution will you reach out to for assistance?
        i. Do you have formal relationships already established?

Assessment of Impacts

1. Have you identified which systems and networks are most critical for your continued operations?
    a. Does it include identification of critical network nodes and their associated interdependencies?
    b. What risks associated with your university's most critical systems have you identified?
    c. What preventative measures has your institution taken to ensure those systems are protected?
2. How does your organization determine what systems/data/services are affected by the malware?
    a. What technical capabilities does your institution possess?

Event Notification Methods/ Thresholds

1. What critical information must be shared between partners at this point to contain the threat and impacts within the scenario?
    a. What entities within your institution would you coordinate with at this time (e.g., campus leadership, emergency services, etc.)?
    b. What entities outside of your institution would you coordinate with at this time (e.g., law enforcement, third-party providers, etc.)?
2. Do you have plans for ensuring the integrity of your communication capabilities in the event of a compromise?
    a. Do you have secondary communications capabilities in case your primary method to communicate is compromised or unavailable?

MODULE 2: EMERGENCY RESPONSE

Scenario

Later that Day

While your IT department works on addressing the network compromise, your institution is notified that afternoon by the 911 call-center supervisor that the number of dummy 911 calls originating from/around your institution has reached an unsustainable number; this overwhelms the call-center and shuts down their capabilities to respond to legitimate calls. The 911 supervisor states that they suspect this is a telephony denial of services (TDoS) attack.

Your IT department is confident that computers affected by the malware allow malicious actors to acquire credentials from users. By 3:30 PM, an unauthorized user is able to use the admin credentials gained from an infected computer used by a member of the facilities department to access to your campus' industrial control system. With access to your institutions' controls, the outside user begins to manipulate your institution's standard automation processes including the power breakers that control campus electricity, Heating Ventilation and Air Conditioning (HVAC), Key Card Access system, and water.

These systems begin to experience latency and then start to fail. Some campus buildings retain electricity while other lose power immediately. Buildings without power quickly lose water. This disrupts refrigeration in dining halls, campus medical facilities, and laboratories. Additionally, key card access is disabled to many buildings on campus including student dorms.

With HVAC shut down, temperatures rise in classrooms, dorms, medical facilities, research labs, and server rooms. Within a few hours temperatures in classrooms rise from their usual 74 degrees to 92 degrees, too hot for students and faculty. Labs that are normally kept cool to preserve sensitive scientific research heat up to 80 degrees. Server rooms across campus reach temperatures close to 100 degrees due to the heat generated by server nodules; several of your institution's servers melt down.

Moreover, a mass notification is sent out to your campus community containing the following message "*Emergency Alert: Campus is unsafe. Evacuate immediately*." Many students elect to leave campus by foot and seek shelter in restaurants and other establishments off-campus. Many students leave campus by car, causing traffic congestion on the roads surrounding your institution.

Discussion Questions

Response Coordination with Internal and External Stakeholders

1. What is your institution's protocol for establishing incident command during a major disruption affecting campus operations?
    a. How are ongoing cyber incident response efforts integrated into the campus' emergency response efforts?
    b. How are external stakeholders (e.g., local police, hospitals, local utilities) integrated into response efforts?
2. What are your institution's priorities at this stage? How have they changed?
    a. Safety and security priorities?
    b. Cybersecurity priorities?

c. Emergency management priorities?

3. What plans or procedures are in place, if any, for your institution to manage and secure campus environments following this incident?
   a. Does your institution have a plan for the activation of an emergency operations center?
   b. Does your institution have a plan for the evacuation of your campus?
4. What mutual aid agreements or formal relationships exist between your institution and local law enforcement, information sharing and analysis centers (ISACs) and others?

Identifying and Managing Effects of Cascading Impacts

1. What technical capabilities does your institution possess for addressing impacts to your industrial control system?
   a. Do campus systems employ remote diagnostics and maintenance tools to measure the desired outputs or performance of particular systems?
   b. Can systems on your campus operate in manual mode as a backup option?
   c. Does your institution have an understanding of how different domains could potentially be impacted (e.g., some would operates at a degraded state while others would be shut down)?
2. Do you have backup power or uninterruptible power supplies (UPS) in case of an outage?

Continuity (Teaching, Online Curriculum, Research)

1. What continuity plans does your institution have for major disruptions to the following:
   a. The academic mission of your institution?
      i. Does your institution have alternative methods to conduct classes within several days of a disruption?
   b. The student affairs and residential mission of your institution?
      i. What are the implications on student activities and on campus housing services following a disruption?
   c. The research mission of your institution?
      i. How you are going to preserve/protect the experiments in laboratories and the integrity of your research data?
      ii. Are there contingency plans in place to ensure the safety and integrity of sensitive research data?
      iii. Are there plans in place to ensure environmental conditions for research animals in which they are kept are maintained?

Crisis Communications and Public Messaging

1. What coordination activities and communication protocols guide public communications?
   a. How are affected communities notified that assistance is available?
   b. How are students and faculty notified about classes being cancelled?
   c. How are parents notified of the situation?
2. What methods will be used to communicate to the public and the media?
3. What mechanisms will you use to communicate with individuals with language barriers/limitations or those with access and functional needs?

Module 3: Recovery

Scenario

October 11, 2017

Your IT Department is 24 hours into their response efforts and is still working to understand the scope of the impacts to your systems and determine what sensitive personal, research, and financial information may have been compromised. They have gathered enough evidence to conclude that your institution was the target of a malicious and complex cyber-attack – possibly by an advanced persistent threat[2] (APT).

Additionally, while your institution is attempting to recover from the impacts to your networks and systems, your emergency services have been working around the clock to help those affected by the power outages, including the evacuation of patients from on-campus medical facilities.

The Next Few Days

Although your IT response teams are confident that they have successfully blocked the hijacked account that was used to access your industrial control system, they have yet to confirm that there is no malware remaining on those systems at this time. Research faculty are growing increasingly concerned and frustrated over the impacts this event will have on their research projects. Similarly, students and parents are concerned about how this event will impact the remainder of their semester and whether their records or sensitive information has been compromised.

Rumors spread on Twitter claiming that the attack was a result of a malicious insider at your institution. Additionally, individuals in alumni networks are expressing their disappointment with the institution’s efforts, questioning if anything could have been done to prevent this from happening in the first place.

Discussion Questions

Restoring Campus Systems

1. How long can your campus be offline before the school year becomes compromised?
2. In what timeframe do stakeholders and regulatory entities expect campus networks and systems will be restored?
3. Does your institution have recovery procedures in place for IT systems?
    a. What is the process for cleaning systems?
    b. What is the process for bringing systems back online?
4. Do recovery activities include cyber forensics?
    a. What protocols are in place to gather digital evidence? To what end?
    b. Are these activities coordinated with law enforcement entities? Third-party cybersecurity entities?
    c. Does conducting these activities impact the timeline for recovery?

[2] DHS Definition: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Restoring Campus Operations

1. What is the process for establishing your institutions restoration priorities?
   a. Is this described in existing plans?
   b. What coordination efforts must occur with external stakeholders to successfully restore campus infrastructure?
2. Following the restoration of infrastructure systems, how does your institution resume operations? In pre-planned phases?
3. For disrupted services impacting on-campus housing, what plans are in place to accommodate affected individuals?
   a. Are there special considerations for international students or students with access and functional needs?

Post-Incident Communications

1. How will your institution provide and unify all external media messaging and communications following this incident?
   a. What communications channels will your institution use for public messaging?
2. How will your institution handle incoming inquiries and requests for assistance from students, families, faculty, or staff regarding this incident?
   a. How will your institution develop and/or emphasize programs that deliver stress management services to those affected by this incident?
   b. If you have to evacuate the campus for an extended period of time, what do you do with displaced students? Where will they live, how will you feed them, how will you account for them (especially international students)?
3. What actions will your institution take to manage public relations following this incident?
   a. What are your priorities and who are the key target audiences for this messaging?
   b. How will your institution respond to media rumors and inquiries regarding how this incident was managed and handled?

Legal and Financial Considerations

1. How does your organization determine the financial impact of this incident?
   a. To what extent does the institution have capacity to absorb costs?
      i. Do you have insurance policies in place for this?
2. How will your institution handle academic issues (e.g., grade appeals and refund requests from students) that result from this disruption?
3. What are the primary areas of legal liability?
   a. To what extent will the university incur responsibility for grant-funded projects that have been affected (delayed or destroyed)?
   b. How will claims of PII disclosure and liability for impacts be adjudicated?
4. What are your regulatory or reporting responsibilities following this incident?
5. What is the appropriate role of governing boards, university administrators, IT administrators, faculty, and staff in responding to claims?

Appendix A: Exercise Players

Institutions of Higher Education

American Preparatory Academy

Arizona State University-Tempe

Auburn University

Boston University

Brigham Young University-Provo

California State University-Los Angeles

California State University-Northridge

Chapman University

Clark Atlanta University

College of Charleston

Collin County Community College District

Columbia College-Sonora

Cornell University

Dakota State University

Dixie State University

Fashion Institute of Technology

Florida Agricultural and Mechanical University

Florida Atlantic University

George Washington University

Grand Valley State University

Hamilton College

Howard University

Iliff School of Theology

Indiana University-Purdue University-Fort Wayne

Iowa State University

Johnson C Smith University

Los Angeles Community College District

Louisiana State University and Agricultural & Mechanical College

Massachusetts Institute of Technology

Metropolitan Community College-Kansas City

Mississippi State University

Modesto Junior College

Neosho County Community College

Nicholls State University

North Carolina State University at Raleigh

North Central Missouri College

Northeastern Illinois University

Northern Arizona University

Oklahoma State Regents for Higher Education

Pace University-New York

Pennsylvania State University-Main Campus

Pima Community College

Pomona College

Portland State University

Princeton University

Reed College

Rice University

Rochester Institute of Technology

Saint Joseph's University

Salt Lake Community College

Smith College

Snow College

South Texas College

Southern Adventist University

Southern Connecticut State University

Southern Virginia University

Stanford University

SUNY at Albany

SUNY at Binghamton

Syracuse University

Tennessee State University

Texas A & M University-College Station

Texas Christian University

The University of Tennessee-Knoxville

The University of Texas Health Science Center at Houston

Trocaire College

University at Buffalo

University of Alabama at Birmingham

University of Alaska Anchorage

University of Alaska Fairbanks

University of Alaska Southeast

University of Arizona

University of Denver

University of Georgia

University of Houston

University of Idaho

University of Kansas

University of Kentucky

University of Maryland-College Park

University of Massachusetts-Amherst

University of Nevada-Reno

University of New England

University of North Dakota

University of Northern Iowa

University of Oklahoma-Norman Campus

University of St Thomas

University of Utah

University of Virginia-Main Campus

University of Washington-Seattle Campus

University of Wisconsin-Madison

Utah State University

Utah Valley University

Washtenaw Community College

Weber State University

Western Governors University

Wisconsin Lutheran College

Yavapai College

Yosemite Community College District

Organizations and Associations (Observers)

David Suzuki Foundation

Field Innovation Team

Intermedix Corporation

International Association of Campus Law Enforcement Administrators (IACLEA)

Internet2

National Center for Campus Public Safety (NCCPS)

Western Interstate Commission for Higher Education (WICHE)

Research & Education Networking Information Sharing and Analysis Center -- Indiana University Bloomington

University of Akron Main Campus

University of Nebraska at Omaha

Government Partners (Observers)

DHS Federal Emergency Management Agency	DHS Federal Emergency Management Agency (FEMA) National Training and Education Division (NTED)
DHS FEMA	DHS NPPD
DHS National Cybersecurity & Communications Center (NCCIC) National Cyber Exercise & Planning Program (NCEPP)	DHS Immigration & Customs Enforcement (ICE) Student & Exchange Visitor Program (SEVP)
DHS National Protection & Programs Directorate (NPPD) Office of Infrastructure Protection (OIP) Protective Security Coordination Division (PSCD)	DHS National Protection & Programs Directorate (NPPD) Office of Cyber and Infrastructure Analysis (OCIA)
DHS Office of Academic Engagement	DHS Office of Academic Engagement (OAE) Support Team
DHS Office of Intelligence & Analysis (I&A) Field Operations Division (FOD)	DHS United States Secret Service
Exercise Support Team	Federal Bureau of Investigation (FBI)
Federal Emergency Management Agency (FEMA) National Exercise Division (NED)	Federal Emergency Management Agency (FEMA) Region II
FEMA Region VII (CTR)	Naval Postgraduate School (NPS) Center for Homeland Defense & Security (CHDS)
State of Utah - Department of Public Safety	State of Utah - Department of Public Safety - Statewide Information and Analysis Center
State of Utah - Division of Emergency Management	State of Utah, Department of Public Safety
United States Secret Service (USSS)	Utah DPS Statewide Information & Analysis Center

Appendix B: Acronyms

APT	Advanced Persistent Threat
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
HVAC	Heating, Ventilation, and Air Conditioning
ICPD	FEMA-NPD Individual & Community Preparedness Division
ICS	Incident Command System
ISACs	Information Sharing and Coordination Centers
IT	Information Technology
NED	National Exercise Division
NPD	FEMA National Preparedness Directorate
NTTX	National Seminar and Tabletop Exercise
OAE	DHS Office of Academic Engagement
PDF	Portable Document Format
PII	Personally Identifiable Information
TDoS	Telephony Denial of Services
TTX	Tabletop Exercise
UPS	Uninterruptible Power Supplies
US-CERT	Department of Homeland Security's United States Computer Emergency Readiness Team