2019 REN-ISAC Blended Threat Resilience Workshop Series

# Final Findings Report

*May 15, 2020*

REN-ISAC

# Table of Contents

# Foreword

On behalf of the REN-ISAC, thank you for taking the time to read this report. More importantly, thanks to everyone who contributed to the success of the 2019 REN-ISAC Blended Threat Resilience Workshop Series, including our hosts, our planning teams, the REN-ISAC staff, and our partners at Gate 15. While taking on the workshop series may have seemed like a bit of a departure for the REN-ISAC, the workshops, in actuality, took the REN-ISAC back to our roots. The Memo of Understanding between the Trustees of Indiana University and the FBI National Infrastructure Protection Center, established in 2003, articulated that the REN-ISAC "facilitates the exchange of timely, accurate and actionable warning information related to both physical and cyber threats or attacks." The focus on blended threats in the workshops allowed the REN-ISAC to stimulate dialogue and assist organizational planning for response to today's complex threats.

This report is full of actionable information that you, the reader, can apply at your organization–as well as plenty to discover about how the REN-ISAC can continue to provide our members with valuable services and events. As we launch the 2020 workshop series, we take these results as opportunities for improvement.

Best regards,

Kim Milford, Executive Director

REN-ISAC

## Hosts

REN-ISAC would like to thank the six institutions that generously volunteered to host the 2019 Blended Threat Workshops. Without their help, this report would not have been possible.

UNI®

PURDUE
UNIVERSITY®
FORT WAYNE

ACU

NWACC
NorthWest Academic Computing Consortium

YOUNGSTOWN
STATE
UNIVERSITY

UMBC

# Executive Summary

Following from the success of the 2018 Blended Threat Resilience Workshop Series, REN-ISAC and an exercise planning team comprised of REN-ISAC staff, Gate 15 partners, and members designed and developed a new series for 2019. The 2019 scenario focused on a generic state university impacted by an emerging international health threat, eventually resulting in an on-campus outbreak that included a cyber component.

The REN-ISAC—with an outstanding group of partners and hosts—conducted six workshops across the United States: at campuses in Iowa, Indiana, Ohio, Oregon, Texas, and Maryland specifically. All in higher education were welcome to attend, including both REN-ISAC members and non-members. Attendees included subject matter experts from health care, physical security, emergency management, information technology and security, law enforcement, and community partners.

With guidance from the planning team, the 2019 Blended Threat Resilience Workshops examined the serious threat concerns and risks of a health outbreak and associated cybersecurity threats (such as the potential for espionage and the persistence of phishing) to the higher education community. The REN-ISAC strove to facilitate relevant and meaningful discussions regarding organizational preparedness across the various departments, participating institutions, and key partners from the surrounding community. Those discussions inspired a sharing of insights, best practices, issues, and enduring collaborations that culminated in the 16 Best Practices, 18 Areas of Improvement, and four Challenges contained in this report. We hope the information provided enables organizations throughout higher education to enhance their operations, preparedness, and resilience.

**Definition: Workshop**

The HSEEP definition of a Workshop is an informal discussion "employed to build specific products, such as a draft plan or policy."

The workshops' discussions fostered both unique and common ideas, challenges, and successful approaches to health and cyber issues and coordination. Taken together, there is tremendous value for the individual workshop participants—particularly as they have jumped into COVID-19 response—and the broader national conversation with these collective findings.

Throughout the series, workshop observations highlighted the importance of effective collaboration and explored a number of opportunities that may further enhance security and resilience that are specific to higher education institutions, their local partners, across the higher education community, and in partnership with other vital stakeholders. The workshops reiterated and expanded upon some common observations and areas of improvement needed to enhance continued organizational preparedness, some of which echoed related observations from the 2018 series. Many of the observations we reiterated at multiple venues and validated important issues such as:

- The varied complexities regarding continuity of operations and transitioning to remote work locations
- The challenges of safely and securely managing an infected student population
- The perennial challenges of phishing and best practices to educate and arm users
- The importance of having properly documented procedures and back-ups for accessing those procedures
- The value of cross training and organizational depth in preparedness and resilience
- The value in exercising and validating plans and procedures

- Approaching security and resilience with a whole-community approach, integrating communications, risk management, legal, health departments, law enforcement, third parties, and other stakeholders into preparedness and security operations
- Ensuring the safety of first responders and students with proper training and equipment

This report aims to provide valuable insights and considerations derived from the workshop discussions so organizations can learn from these findings and use them to enhance their individual and collective security and preparedness.

Remarkably, as the workshop team prepared the Final Findings Report, our world was confronted with a very real health threat in the global response to COVID-19. Additionally, higher education (and other organizations worldwide) are seeing nefarious cyber criminals launch multiple aggressive campaigns intended to compromise individuals and organizations as simulated in the 2019 workshop scenario. The real-world response to COVID-19 has already and will certainly continue to offer opportunities to reflect on lessons learned, many of which echo the 2019 workshop discussions. For example, several workshop participants brought up the tactical need for staff to work from home and the need to ensure network bandwidth for a remote workforce. Yet there was no direct exploration of the more aggressive stance to proactively close campuses taken by higher education's institutional leaders. The quick move to online services and initiatives that support teaching, learning, and research has been, arguably, one of the most critical life-saving and curve-flattening actions to stop on-campus outbreaks before they occur. Once the current crisis has passed, it will be interesting, even necessary, to examine the 2020 COVID-19 responses to ascertain additional best practices, areas of improvement, and challenges for the future.

## Highlights

The lessons learned during the 2019 workshops helped participants consider and prepare for today's COVID-19 response. While non-participating members have already had to consider many of these issues in their COVID-19 response, the numerous observations and comprehensive analysis in this report can still provide new ideas or improved practices to better support the role of the academy during this time of global crisis.

The observations from this workshop are divided into three categories:

- **Best Practices** – Procedures identified as valuable, or effective.
- **Areas of Improvement** – Opportunities for stakeholders to enhance their security posture.
- **Challenges** – Inherent issues that, in today's threat environment, are unable to be truly eliminated, just mitigated.

The following are some of the key observations gained from many fruitful discussions at the workshops. In order to inform future emergency preparedness efforts stemming from this report, each entry is tied to the appropriate Core Capabilities, as identified in the Federal Emergency Management Agency's (FEMA's) National Preparedness Goal.

The top nine observations are listed below, roughly organized from highest numbers of core capabilities addressed to the lowest. The importance of these highlighted observations and, thus, FEMA's Core Capabilities reflects many of the pivotal issues higher educational institution are currently undergoing. Section 2 goes into detail for all 38 observations.

### *Best Practices*

1. Storing Disaster Recovery Plans Safely and Maintaining Back-Ups
2. Preparing First Responders for a Highly Contagious Disease Outbreak
3. Providing Self-Care Kits to Students
4. Utilizing Social Media to Track Campus Reactions to an Outbreak

### *Areas of Improvement*

1. Exercising and Training on Existing Policies and Procedures Builds Resilience
2. Healthcare Coordination is an Important Consideration While Transitioning Infected Students to Home Counties
3. Improving the Digital Fluency of Campus Populations to Operate Remotely
4. Natural Disasters Affecting the Medical Supply Chain

### *Challenges*

1. Controlling Access to an Integrated Campus

# Section 1: Workshop Series Overview

## Workshop Series Background

The REN-ISAC Blended Threat Resilience Workshop Series began in 2018 out of a desire to increase the higher education community's capability to respond to possible complex and blended threats. To achieve this goal for 2019, the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC) planned and executed a series of six workshops in a diverse set of locations across the United States. As defined by the Homeland Security Exercise and Evaluation Program (HSEEP), workshops are interactive events focused on strategic, policy-oriented issues that result in a product. The primary purpose of this series was to raise awareness of blended threats, allow security professionals from different disciplines to interact, and document the innovations and challenges the higher education community encounters as it navigates complex physical and cybersecurity issues.

For the purposes of this series, the REN-ISAC defines blended threats as a natural, accidental, or purposeful physical or cyber danger that has or indicates the potential for crossover implications to harm life, information, operations, the environment, and/or property. They differ from complex threats, which are two or more separate attacks aimed at the same general or specific target or objective. The key distinction between the two is the crossover component of a blended threat: these types of threats are a growing possibility in today's interconnected world. Cyber and physical emergency response and preparedness efforts are necessary now to prepare for events—from the annoying to the catastrophic—likely to occur in the years to come.

Following the format of REN-ISAC's inaugural 2018 program, the 2019 Blended Threat Workshop Series utilized a realistic and threat-informed scenario focusing on an emerging health threat with a cyber-related incident as described briefly above and throughout this report. Using this scenario to focus the discussion, participants confronted a topical concern that many campuses faced while also speaking to the broader topic of blended threats. REN-ISAC documented these conversations and extrapolated high level observations from each workshop to create two types of reports: six individual workshop reports containing observations from each workshop were created and distributed to participants and this final comprehensive report collating, ranking, and summarizing the series' most relevant observations for public distribution.

## Purpose & Design

### *Scope*

The following is the scope of the workshop series as approved by the 2019 REN-ISAC Blended Threat Resilience Workshop Series planning team:

- *In CY2019, REN-ISAC will lead the development and conduct of six security-focused discussion-based exercises, which are anticipated to be workshop events. These approximately six-hour long exercises are anticipated to be conducted between May and November at six North American locations. Exercise participants are expected to include institution leadership, physical and cybersecurity, emergency management, IT, administration, student affairs, and other key personnel, leaders and/or staff from REN-ISAC and other higher education institutions, as well as other partners and subject matter experts as may be appropriate.*

### *Objectives*

The following are the objectives of the workshop series as approved by the planning team:

- *Provide a forum for higher education organizations to use a complex or blended threat scenario to prompt discussion and share approaches from leaders in the community regarding physical and cybersecurity preparedness, coordination, and response (these exercises will not focus on recovery) to help inform organizational preparedness.*
- *Provide participants an opportunity to interact with one another and discuss issues, concerns, best practices, and other salient points to help inform organizational preparedness.*
- *Provide feedback to members and the broader higher education community on best practices, preparedness gaps, and opportunities for improvement identified through the exercise series to help inform organizational and community security preparedness.*
- *REN-ISAC will provide participants and their organizations a summary of the discussion within 60 days of exercise completion to help inform organizational preparedness.*
- *REN-ISAC will provide participants and their organizations a roll-up summary of the complete 2019 exercise series by 30 Jan 2020 to help inform organizational preparedness.*

### *Scenario*

In the spring of 2019, the planning team developed a sequential four module scenario focused on a campus measles outbreak with subsequent opportunistic cyberattack targeting the affected institution. At the beginning of each module, a situational update from the generic “State University” was presented to attendees, along with supporting media to provide attendees with greater context and immersion. Once complete, a facilitator-led discussion guided attendees through questions pre-selected by the planning team, as well as any raised during the natural flow of conversation to focus attendee discussion on core issues, needs, responses, and challenges. Additionally, there were small-group discussions for certain modules.

The following are summaries of the four modules exercised during the 2019 series. The full text of the 2019 modules can be found in Appendix B: Complete 2019 Scenario and Questions.

### Module One: Eruption

The World Health Organization has announced the emergence of a new strain of vaccine-resistant measles, designated Measles-2, in the Ukraine. While the disease was initially restricted to the Lviv province, a recent international business conference in the provincial capital has raised concerns of international transmission.

### Module Two: The Full Bug

Four weeks later, there have been limited domestic outbreaks of Measles-2 within the United States. The health department for State University discovered a student potentially infected with the disease recently attended a major event hosted on campus where other students and alumni were present. Some event attendees reported measles-like symptoms.

### Module Three: Best of Both Worlds

Two weeks later, the number of Measles-2 infections on campus and in the nearby community has continued to increase, resulting in a higher level of employees’ and students’ absenteeism. State University’s IT department also observed suspicious activity on certain accounts after professors clicked on a link in an email containing a fake Measles-2 themed health alert. The compromised accounts have access to large amounts of sensitive data.

### Module Four: Right Now

Two weeks later, most State University's students and employees are absent due to illness, caring for family members, or concern about the disease. Collaborating government agencies announced that the phishing campaign seen two weeks prior was part of a broader campaign by a nation-state actor targeting research activities. The Department of Justice issued indictments for certain Russian nationals, one of whom is teaching at State University.

# Section 2: Summary of Findings

## Best Practices

- Disaster recovery plans and backups should be available in a wide variety of formats and stored appropriately to be available despite technological limitations commonly experienced during emergencies. (Best Practice 1)
- Preparing equipment and training ahead of time can lead to a successful infectious disease outbreak response on campus. (Best Practice 2)
- Selling or providing self-care kits to students ensures their access to basic supplies in case of illness or natural disaster. (Best Practice 3)
- Social media can be used to track the campus community's questions, concerns, and misconceptions, allowing institutions to proactively respond. (Best Practice 4)
- A self-assessment by an IT department immediately after an event can greatly improve processes and procedures. (Best Practice 5)
- Assign functions in the response plan to roles, instead of people, to give the responding team flexibility to work with the personnel available at that time. (Best Practice 6)
- Continuity records for each position, that are regularly updated and backed up to the cloud, help support effective operations when key members are absent. (Best Practice 7)
- Creating a user engagement program that encourages personal interaction in the user's regular work environment increases participation and improves overall security knowledge. (Best Practice 8)
- Creating a phishing lure database is a low-cost tool that effectively empowers employees and students to defend the institution against cyber threats. (Best Practice 9)
- Providing first responders with sanitized health data from local healthcare systems gives them more time to equip responders appropriately. (Best Practice 10)
- Appointing a dedicated advocate for health and pandemic preparedness helps safeguard the gains that are made during an incident. (Best Practice 11)
- Large surges of information requests can most effectively be handled through preparing various resources before an incident. (Best Practice 12)
- Having a central source of public information, such as a website, facilitates coordination of messaging and speeds public information delivery. (Best Practice 13)
- A properly staffed and funded risk management program that meets regularly allows an institution to effectively track, manage, and mitigate risks. (Best Practice 14)
- Holding regular, quick, informal drills during team meetings is an efficient method to build a culture of preparedness. (Best Practice 15)
- Risk awareness and articulation specific to the institution is vital in prioritizing resources and managing risks. (Best Practice 16)

## Areas of Improvement

- Exercising and drilling emergency response plans gives staff the "muscle memory" to be more effective when an incident occurs. (Area of Improvement 1)
- Validating plans through exercises ensures response effectiveness even when key staff are unavailable. (Area of Improvement 1)

- Plans for the mass relocation of potentially infected students from a quarantined institution could result in cascading burdens for local health systems across an entire region. (Area of Improvement 2)
- During an epidemic, faculty are likely to depend on educational technology systems with which they have limited familiarity to teach remotely. (Area of Improvement 3)
- Training and practical exercises help students and staff acquire the skills to work and learn remotely. (Area of Improvement 3)
- Student employees who are not fully equipped, faculty who are not fully trained, and IT staff not prepared to handle surges in remote needs during an outbreak may hamper operational effectiveness. (Area of Improvement 3)
- Natural disasters can affect critical supply chains, making it even more difficult to respond in the middle of a major incident. (Area of Improvement 4)
- Most IT departments employ students in critical IT positions, and their treatment as employees on one hand and as students on the other must be reconciled by the institution. (Area of Improvement 5)
- Technical service support desks are an important component of campus IT services but reliance on student workers makes it difficult to operate remotely if required. (Area of Improvement 5)
- There is a need for better coordination and processes between IT teams responsible for security. (Area of Improvement 6)
- An incident at multiple institutions may overwhelm the ability for a third-party vendor to provide services for all. (Area of Improvement 7)
- Employee contracts and classifications can restrict IT and Facilities employees from performing vital functions. (Area of Improvement 8)
- Any news of an epidemic is likely to burden an institution’s network resources to an unprecedented level. (Area of Improvement 9)
- While most institutions plan to communicate with local government health departments during a communicable disease outbreak, there is a need for increased communication among neighboring university’s health departments as well. (Area of Improvement 10)
- Understanding the needs of essential employees who must still report to campus during quarantines and providing appropriately for their needs increases their safety. (Area of Improvement 11)
- Preparing for widespread workforce absences due to illness or natural disaster in advance minimizes disruptions when such events occur. (Area of Improvement 12)
- Mitigating attacks against an institution’s public directory can be difficult. (Area of Improvement 13)
- Creating a mass communications service that requires users to opt-out instead of opt-in makes it more effective. (Area of Improvement 14)
- A formal process to approve mass communications requests, with published criteria for the messages, ensures that only critical messages are transmitted and reduces unnecessary requests. (Area of Improvement 15)
- The infrastructure in place to communicate information to the public can quickly be overwhelmed by a major incident. (Area of Improvement 16)
- Planning and coordinating are required when IT teams need to restore systems and law enforcement needs to gather evidence. (Area of Improvement 17)

- While today's flexible work environment routinely involves and depends upon remote execution of duties, there may still be significant barriers to shifting to full-time remote operations. (Area of Improvement 18)

## Challenges

- Protecting campuses integrated into the community can be difficult due to lack of authority over who is present on school property. (Challenge 1)
- Staff, independent of guidance from management, will make decisions regarding their presence or absence based on public information. (Challenge 2)
- The longer or more widespread an epidemic becomes, the higher the risk of staff absences, due to various considerations. (Challenge 2)
- During an epidemic, countering fear, uncertainty, and doubt (FUD) is extremely difficult. (Challenge 3)
- Institutions have limited ability to track and influence the behavior of students that do not live on campus but are often present on campus. (Challenge 4)

# Section 3: Analysis and Observations

## Best Practices

Best Practices are defined here as procedures identified as valuable, or effective. The observations highlighted here were all raised by participants in the six workshops.

### *1.) Storing the Disaster Recovery Plan Safely and Maintaining Back-Ups*

- Disaster recovery plans and backups should be available in a wide variety of formats and stored appropriately to be available despite technological limitations commonly experienced during emergencies.

One participating IT professional emphasized the importance of safely and securely storing incident response plans based on their experience working in an environment where it was difficult to access the electronically stored emergency response plans once the facility lost power. A power outage significantly delayed the institution's response efforts. After that experience, the incident response plan also included a hard copy backup. Other participants discussed their organization's methods for backing up disaster recovery plans, including the use of flash drives or designated alternatives.

It is important to consider the worst-case scenarios when deciding how to store and transmit an organization's emergency plans during incidents. Ensuring the plans are available by a variety of means reduces delays during activation, especially for personnel unfamiliar with the document. Plans should be accessible from more than one storage location or via more than one method to ensure availability when access to a particular service—the internet, a computer, or even power—is unavailable during an emergency. Just as important, staff should be informed and reminded on a regular basis about where to find these backups under those circumstances.

**Core Capabilities:** Planning, Operational Coordination, Risk Management for Protective Programs & Activities, Operational Communications

### *2.) Preparing First Responders for a Highly Contagious Disease Outbreak*

- Preparing equipment and training ahead of time can lead to a successful infectious disease outbreak response on campus.

Leaders from participating health departments and first responders discussed effective preparations for medical and first responder personnel once a disease outbreak is likely to occur. During a potential epidemic in their area of operation, the organization prioritizes protecting their personnel from infection by equipping dispatchers with information about disease symptoms. A dispatcher who takes calls from potentially infected/infectious individuals asks pertinent questions during the call to determine if there is a higher than usual threat of infection. With this information, the dispatcher can warn first responders before they enter a situation with a high risk of infection to don appropriate personal protective equipment (PPE). Responders use easily sanitized vehicles and sanitizable/disposable equipment if patients with highly infectious diseases require transportation.

A successful response to a disease outbreak on campus requires planning, equipment, and training. Leaders should consider optimal methods, from pre-positioning PPE and medical supplies to training dispatchers to check for symptoms, to keep their first responders safe while still serving their campus and community. Training is a key element of this effort. Staff must understand how to properly don and doff PPE and what questions to ask potentially infectious callers. All of this requires the investment of time prior to a potential incident to ensure personnel are proficient and confident, with the “muscle memory” to react properly and safely.

To achieve robust preparation, an important part of the preparedness cycle is organizing and equipping, along with proper training and exercise. Obtaining and positioning protective equipment before a crisis is vital to effective and timely response. As this report is being written, the world is responding to the COVID-19 pandemic and discovering how impactful preparedness—or in some case a lack of preparedness—can be.

**Core Capabilities:** Planning, Operational Coordination, Risk Management for Protection Programs & Activities, Threats & Hazards Identification, Public Health, Healthcare, Emergency Medical Services

### *3.) Providing Self-Care Kits to Students*

- Selling or providing self-care kits to students ensures their access to basic supplies in case of illness or natural disaster.

During a discussion of continuity and resilience early in the scenario (prior to epidemic confirmation) one institution offered a best practice it had implemented: marketing self-care kits to incoming students. For many students, living on campus is the first time they have become fully responsible for their own health and safety, which results in the absence of basic health supplies. At the institution, many students were calling 911 in distress over symptoms that were simply a cold. To mitigate that issue, the institution started selling pre-bundled supplies of useful medicines, first-aid supplies, and basic equipment for natural disasters to students at the start of the academic year.

Selling or providing self-care kits to incoming students allows an institution to ensure students have the basic necessities to handle common diseases or natural disasters. This also emphasizes the importance of personal readiness and responsibility, while simultaneously providing a concrete preparedness and response benefit. New students can be a rewarding yet difficult population to reach with preparedness messaging. They are more liable to start and stick with new habits during this transitional period in their life, yet their attention is occupied by a large number of pressing tasks and new distractions inherent to this major transition. Providing preparedness kits can provide students with a basic level of personal preparedness, allay student concern and anxiety during an epidemic situation, and inspire a solid foundation for health preparedness skills necessary for living on their own.

**Core Capabilities:** Public Information & Warning, Community Resilience, Long-Term Vulnerability Reduction, Environmental Response/Health & Safety

### *4.) Utilizing Social Media to Track Campus Reaction to an Outbreak*

- Social media can be used to track the campus community’s questions, concerns, and misconceptions, allowing institutions to proactively respond.

Some participants emphasized the importance of following social media to track the community’s reaction to a potential outbreak and to counter disinformation. Communications professionals focused on tracking and using social media conversations to better understand questions and concerns from their constituencies. The university’s communications can be customized to address raised concerns and provide necessary information. Similarly, communications professionals can use social media to watch for the spread of rumors and counter disinformation, reducing panic and recommending appropriate preventative actions.

During an ever-changing situation like a disease outbreak, social media can be a powerful tool for situational awareness. Social media managers should consider disease outbreaks as a period of heightened awareness of their social media presence—both for messages directed to them and for relevant conversations about the incident. Communications leaders should further recognize that this conversation not only shapes the university's messaging but also departmental response efforts. For example, health professionals may want to know popular discussion topics, concerns, and other information gleaned from social media to properly address inaccurate information and dispel disinformation, while IT professionals may want to know if there is a sudden trend in people staying home so they can prepare for an increase in remote network traffic.

**Capabilities:** Public Information & Warning, Intelligence & Information Sharing, Situational Assessment, Health & Social Services

### *5.) Conducting Post-Event Self-Assessments*

- A self-assessment by an IT department immediately after an event can greatly improve processes and procedures.

A participating IT professional spoke to the importance of conducting department-level self-assessments (sometimes referred to as after-action assessments, hot washes, or post-mortems) in the immediate aftermath of an event. After each significant security incident, leaders prioritized time to bring together the entire response and management team to ask critical questions, such as "How well did we handle this," "What did we learn," and "What should be changed to respond better in the future?" They found it best to ask these questions while the incident was still fresh in the team's mind so that pertinent information is not lost before returning to steady state operations.

Post-event self-assessments are a valuable tool for improving any team and should be conducted after every major event. Giving employees space to reflect on their response to a real-world incident can improve efficiency and safety by creating a list of useful and specific actions. Leaders should consider building this extra time into current incident response procedures and encourage staff members to speak freely about the successes and failures they encountered. With repetition, self-assessment can be turned into a habit within the organization.

Self-assessments may be done informally or formally. Either way, it is helpful to have an identified "champion" that is responsible for completing the assessment, capturing the findings, and developing action plans. This can be done in a formal after-action report, immediate changes to plans and procedures, or through another system the organization employs. HSEEP offers ideas on the after-action process that are applicable both to exercises and real events.

**Core Capabilities:** Cybersecurity, Planning

### *6.) Assigning Functions to Roles, Not People*

- Assign functions in the response plan to roles, instead of people, to give the responding team flexibility to work with the personnel available at that time.

Participating campus police and IT personnel brought up a major lesson they previously learned: the importance of assigning functions in any emergency plan to roles rather than specific people. After suffering delays and failures when executing plans that emphasized individuals vs. functional roles and responsibilities, participants found value in moving to role-based plans. When assigned to people, an incident response plan's effectiveness begins to degrade as staff change positions, leave, are unavailable, or new staff come on board. Once it becomes time to use the plan, an organization may spend unnecessary time and effort to determine new owners of critical functions within the plan, how to contact them, whether they understand their responsibilities, and other concerns.

Assigning functions to roles gives incident responders the ability to organize the organization's response based on assigned roles and, if the identified position is unavailable, the ability to find successors by searching for a position with similar functions and responsibilities. It is difficult to plan for specific individuals being present during any one incident, especially during health-related incidents where employee absences are a larger risk. Incident response is about completing the tasks that need to be done with the resources at hand and handling personnel should be no different in that regard. A recovery plan should focus on flexibility over exactitude as conditions can be too unpredictable.

**Core Capabilities:** Planning, Operational Coordination, Operational Communication

### *7.) Maintaining a Position-based Continuity Document*

- Continuity records for each position, that are regularly updated and backed up to the cloud, help support effective operations when key members are absent.

During a discussion regarding continuation of departmental operations despite the absence of key employees, one institution shared their current best practice: requiring staff to create and update continuity documents for their position. Each staff member should review their roles and responsibilities, then create a single record delineating the information and procedures necessary to execute basic and critical functions. This record is routinely saved in the institution's backup storage and can be accessed by the appropriate employees when that staff member is out of the office for any reason. Critical passwords, especially those for the network, are treated differently. System administrators must ensure their supervisors have access to critical passwords in case of emergencies. The institution requires an annual update of this collection of information, though employees are encouraged to update it more often.

Maintaining a collection of continuity documents can improve the incident response efficiency and is especially important for essential staff. First and foremost, the record document is a valuable resource that provides context for an employee's regular duties and reduces the risk of critical action failures during absences. In addition, the process of creating and updating the document keeps staff thinking with a continuity-based mindset throughout the year, which can otherwise be difficult to achieve in an institution without a robust preparedness program. However, establishing this practice can take time and resources, as it may require a change in thinking for employees at every level of the enterprise, and its effectiveness could depend on the complexity of each position being documented and the effective maintenance of the documents.

**Core Capabilities:** Planning, Cybersecurity, Risk & Disaster Resilience Assessment

### *8.) Increasing User Engagement in Cybersecurity*

- Creating a user engagement program that encourages personal interaction in the user's regular work environment increases participation and improves overall security knowledge.

One workshop IT department participant discussed its successes in engaging with students and staff about cybersecurity when bringing National Cybersecurity Awareness Month to its university's campus.

Over the course of three years, the department refined an educational series that included lecture sessions, booths on campus, and one-on-one discussions with students. The primary lesson the institution learned was that the best way to target students is to focus less on technical matters and more on being present where students congregate. Booths with IT department staff placed in the main traffic areas on campus were able to draw in and impact more students compared to the "TED Talk"-style approach the department took the first year. The department now offers multiple events to draw students in, from quiz games with candy prizes to free one-on-one scans of their laptops or tablets for common malware and vulnerabilities. The department also learned it is best to build on existing resources and heavily relies on the free handouts and pamphlets that the Federal Government produces for cybersecurity awareness.

Engagement strategies such as these help to make the concept of securing their online presence more real to students. IT and security leaders should consider proactively reaching out to the populations they service, whether students, faculty, or staff, in the locations they work and congregate. This can be done by taking advantage of events like the National Cybersecurity Awareness Month, as well as "World Backup Day," "World Password Day," "National 'Slam the Scam' Day," etc. Being approachable about the risks makes it easier for users to absorb key security lessons. In addition, leaders should not be afraid to continue to experiment and refine these types of initiatives to best fit their on campus audience.

**Core Capabilities:** Cybersecurity, Public Information & Warning, Community Resilience

### *9.) Creating a Phishing Lure Database*

- Creating a phishing lure database is a low-cost tool that effectively empowers employees and students to defend the institution against cyber threats.

A participating institution described its approach to combatting phishing: educating its users through the creation of what it called a "phish tank." This database stores a collection of phishing lures provided to the university's IT department, either through notifications from security tools or user reports. The department then makes the database an available resource for all users. When a user is confronted with a possibly suspicious email, they can quickly search the database to see if a similar lure was already received. The database can also be used as an educational tool to help employees understand how phishing messages look or what phrases might trigger report creation for a legitimate message. The lures are stored in the database as images to reduce the risk of an accidental click.

The "phish tank" concept is a great example of a low-cost tool that IT departments with limited resources can build for their users. It is easy to implement a method to store the images and integrate database maintenance and updates into an analyst's daily workflow. While not a comprehensive solution, the database can assist proactive but less educated users in training themselves to better identify phishing—the most common cyberthreats facing organizations. In the face of limited resources, leaders can consider solutions like this that can be implemented at a low cost and that can provide a tool to enhance threat awareness and empower users.

**Core Capabilities:** Cybersecurity, Threats & Hazards Identification, Community Resilience

### *10.) Providing First Responders Access to Protected Health Data*

- Providing first responders with sanitized health data from local healthcare systems gives them more time to equip responders appropriately.

A participating fire department shared a valuable process for responding to the scenario: connecting the ambulance services' and fire department's databases to share anonymized medical information regarding potential infectious citizens in response areas to enhance firefighters' safety. Created after an epidemic occurred in its area of responsibility, this system allows the local health department to share certain types of information (diseases, infections, etc.) with the fire department, in addition to ambulance services. The data is anonymized when transmitted, simply alerting firefighters responding to an affected address to equip PPE.

Setting up systems that both connect disparate networks and properly navigate legal issues requires effort; however, they provide first responders, such as police officers and firefighters, ample warning before responding to locations with heightened health risks. While hazardous disease infection is, comparatively, a much more subtle threat than others these professionals face while on the job, increasing the time to apply protection protocols and equip the appropriate gear improves their ability to respond safely.

**Core Capabilities:** Planning, Intelligence & Information Sharing, Screening, Search, & Detection, Long-Term Vulnerability Reduction, Environmental Response/Health & Safety, Public Health, Healthcare, Emergency Medical Services

### *11.) Advocating for Disease Resiliency*

- Appointing a dedicated advocate for health and pandemic preparedness helps safeguard the gains that are made during an incident.

One discussion focused on sustaining the energy and commitment necessary to keep an organization prepared for disease outbreaks. In comparison to other types of incidents, serious outbreak occur infrequently; thus, lessons learned from prior outbreaks can be lost in the intervening years.

Organizations often respond to the "right now," which is short-sighted and creates preparedness gaps. When a concern emerges, there is often great short-term interest in mitigating related risks. This was observed in response to the 2013-14 Ebola outbreak and the 2015-16 emergence of Zika in the Americas. Pandemic preparedness is often not prioritized and short-term efforts are not always sustained. Having an advocate allows a consistent champion for this important part of risk management.

To maintain that focus, assigning an advocate within the organization with both the mandate and the energy to keep health and pandemic preparedness a priority is critical. Participants who had an advocate in their organization felt they were better prepared for the workshop scenario than those who did not. An advocate is responsible for keeping momentum towards resilience efforts from falling prey to everyday organizational friction, inertia, and competing priorities for time and resources. By coordinating action between different areas of the organization, an advocate ensures consistent communication and education, keeping the issues and procedures fresh for leadership and staff. The advocate can be an informal position or an additional duty. It requires someone with broad enough job responsibilities to affect change on their own, thus reducing reliance on upper management reporting authority.

**Core Capabilities:** Planning, Risk Management for Protection Programs & Activities, Long-Term Vulnerability Reduction

### *12.) Preparing for Crisis Communications*

- Large surges of information requests can most effectively be handled through preparing various resources before an incident.

Most effectively managing the resources necessary to communicate with the public during a major incident affecting a college campus was another major topic. Whether through phone calls or internet queries, the infrastructure that responders use to handle the event can become overwhelmed as—in addition to students, faculty, and staff—concerned parents, community members, and interested parties outside of the university rush to find information. A secondary impact can be an inadvertent Distributed Denial of Service (DDoS) incident as these parties try to contact the university, impacting systems and networks and further complicating the situation.

Leaders should evaluate their own organization's or department's ability to communicate during an emergency and put appropriate mitigations in place in advance, especially if the rapid increase in volume leads to a DDoS incident. Part of crisis communications is proactively preparing for these surges in phone calls and internet queries to limit their effect on response efforts. An equivalent infrastructure should be in place to handle the increased volume of communication. The discussion largely focused on phone banks, where multiple participants had experience quickly setting them up to respond to a large volume of calls.

One participant detailed how, for major incidents, their institution trains members of the campus crisis team on operating informational phone banks. The core members of the crisis team are able to dictate policy while the extended members receive scripts and can engage with querants. Another participant, who already has an in-house phone bank capability that handles their center's payments and billing, explained how those workers could be quickly re-tasked to receive other types of calls during an emergency.

For all types of crisis communications, pre-scripted templates were held up as a best practice allowing institutions to pivot effortlessly in the face of a rapidly changing situation. Having a generic media release template, preapproved by all critical stakeholders in accordance with preparedness plans, accessible on file for each type of incident designated high priority or high risk makes crisis response a matter of only editing, rather than drafting, editing, and approval. Other strategies are temporarily increasing infrastructure robustness to counter higher bandwidth demands or creating backups of key areas of communication like the school's main webpage.

**Core Capabilities:** Planning, Public Information & Warning, Infrastructure Systems

### *13.) Centralizing Public Communications During a Crisis*

- Having a central source of public information, such as a website, facilitates coordination of messaging and speeds public information delivery.

A participating communications professional emphasized the importance of providing a single source of information when a public incident occurs. A centralized information source, most likely a web page containing all pertinent information related to the emergency, allows the institution to get its message out more coherently and post updates with less delay. A central source also allows the communications department to more easily coordinate the messaging strategy of all departments and utilize templates to save time.

When leaders need to get information to the public quickly and concisely, a single media repository should be considered the primary strategy. However, creating an effective one-stop web page can be challenging in the middle of an incident. To communicate during an incident successfully, this web page should already be in place, with all relevant staff and departments trained to use it. Communications leaders will likely need to coordinate with the IT team to ensure the page can be brought online quickly, as well as withstand a sudden influx of traffic. Overall, investing the time and resources in the university's ability to stand up a comprehensive, single source of information before an incident occurs helps an institution deliver important information in a timely manner when needed.

**Core Capabilities:** Planning, Public Information & Warning

### *14.) Creating a Risk Management Program with Representatives from Critical Departments*

- A properly staffed and funded risk management program that meets regularly allows an institution to effectively track, manage, and mitigate risks.

During a discussion on setting risk prioritization thresholds, one participant detailed their university's practice of holding monthly risk management meetings. The risk management meetings include representatives from critical departments and give institutional leaders a forum to discuss risks that could spread beyond their area of responsibility. These meetings initiate institutional conversations about risk planning and management topics. Because these meetings started for insurance purposes, the risk manager facilitates the discussion, producing the risk analysis, and reporting the results to the board of trustees. The participant felt that, in years past, this consistent process had enabled their school to quickly recognize and begin preparations when a disease outbreak occurred on campus.

A formalized risk management process can provide institutional awareness of potential risks early and manage those risks rigorously. Such an effort requires appropriate resourcing with the staff and funds necessary to create and maintain the process. Dedicated staff provide the expertise necessary to bring in the right subject matter experts for specialized conversations (e.g. active shooter events, quarantines, etc.). While it can take some time to integrate risk management into operations, putting in the effort ahead of time will provide long-term rewards.

**Core Capabilities:** Planning, Risk & Disaster Resilience Assessment

### *15.) Executing Quick and Focused Drills with Teammates*

- Holding regular, quick, informal drills during team meetings is an efficient method to build a culture of preparedness.

While looking at the scenario, one participant observed the benefits of running ad-hoc drills with their team during regular meetings. These drills consist of 15-minute discussions surrounding a specific question, such as "What would happen if this critical server went down?" or "How would we respond if this critical employee was absent?" Meeting participants offer suggestions, allowing a free-flowing discussion that presents an accurate picture of what might occur. These drills can be done as one-off events or scheduled on a regular basis, providing team predictability to understand and articulate their roles and responsibilities.

Whether added to existing team meetings or as separate recurring events, drills are a valuable tool. They allow a team to work through a situation, identify gaps or points of failure, and propose potential solutions to policies and procedures in an informal environment. Regularly executing drills further creates a culture of preparedness, reinforces training, provides opportunities for learning and improvement, and builds habits that reinforce lessons learned into daily duties. Informal drills can be easier to introduce to a team's workflow than other resilience-building measures, and leaders can tailor them on the fly to fit immediate or long-term needs.

**Definition: Drill**

The HSEEP definition of a Drill is "a coordinated, supervised activity usually employed to validate a specific function or capability in a single agency or organization."

**Core Capabilities:** Planning, Risk & Disaster Resilience Assessment, Operations Coordination

### *16.) Prioritizing Threats and Risks to the Organization*

- Risk awareness and articulation specific to the institution is vital in prioritizing resources and managing risks.

An important topic of discussion focused on how institutions could both manage and prioritize threats and the associated risks so that organizational resources can be properly allotted when deciding threat preparation tactics.

One participating risk manager explained how their campus security department handled this challenge both through creating a common operating picture and briefing leadership on the most critical threats and risks. Their pipeline begins with a world-event tracking system that allows their analysts to track professors at conferences, students studying abroad, and other off-campus travel. With this situational awareness, the risk manager provides a daily brief to the police chief, who is responsible for reporting threats to campus leaders. The chief can pass issues of concern to leadership, empowering relevant departments to find solutions.

**Definition: Risk**

The 2010 DHS Risk Lexicon definition of a Risk is a "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences."

Whether the organization has a well-resourced or more ad-hoc risk management program, the fundamentals remain the same for all institutions, knowing where to spend limited time and resources depends on knowing the threat landscape and the most consequential risks facing the organization. Scanning the environment while identifying risks and priorities is a task likely performed on an informal basis by key personnel in security-focused departments. Formalizing that process, even with limited resources, reduces dependency on specific employees and ensures capability continuity when personnel changes. It also provides leaders with a better sense of risk management and decision making, whether in preparation for an incident or during one.

**Definition: Threat**

The 2010 DHS Risk Lexicon definition of a Threat is a "natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property."

**Core Capabilities:** Planning, Cybersecurity, Threats & Hazards Identification

## Areas of Improvement

Areas of Improvement are defined here as opportunities for stakeholders to enhance their security posture. The observations highlighted here were all raised by participants in the six workshops.

### *1.) Exercising and Training on Existing Policies and Procedures Builds Resilience*

- Exercising and drilling emergency response plans gives staff the "muscle memory" to be more effective when an incident occurs.
- Validating plans through exercises ensures response effectiveness even when key staff are unavailable.

A participating risk management professional emphasized the importance of practice and exercise in building institutional resilience. While plans are a critical component of preparedness, they do not reach their full potential until people in the organization are trained to the point of being able to execute the plan's components by rote. Staff must rely on this "muscle memory" during the initial confusion and anxiety of a disaster or major incident. It is impossible to create a document that covers every type of incident. Therefore, organizations should build plans with flexibility in mind, and incident-specific details incorporated in the plans directly or via supporting documentation, e.g. linked standard operating procedures.

A participating healthcare professional shared an experience that, to them, emphasized the importance of staff executing drills of existing plans. The professional's organization had a comprehensive collection of checklists, worksheets, and plans covering what to do with certain patients during an Ebola outbreak. However, those procedures were only effective at certain times of day, as the professional found out when they had to process a patient at 2:00 a.m. Key personnel were absent and important tests could not be conducted, leaving the patient unattended for an extended period of time.

For effective preparedness, plans must be validated through exercises ahead of actual incident response. This validation must consider not only operations during fully staffed hours but also under minimally staffed timeframes, such as evenings, weekends, and holidays. Leaders should dedicate time to all aspects of preparedness, including planning, training, and exercising. When faced with an untested plan, leaders should consider setting aside staff time to exercise the plan. Since there is limited time in any staff member's daily schedule for exercising, the primary focus should be on exercising key functions and processes within a plan. Even 15 to 30-minute drills targeting a single activity within the plan will highlight areas of strength or improvement and lead to more effective procedures. Practicing these actions also helps improve a team's response posture by developing the muscle memory staff needs during an incident.

**Core Capabilities:** Planning, Operational Coordination, Cybersecurity, On-scene Security, Protection, & Law Enforcement, Operational Communications, Health & Social Services

### *2.) Coordinating Healthcare While Transitioning Infected Students to Home Counties is an Important Consideration*

- Plans for the mass relocation of potentially infected students from a quarantined institution could result in cascading burdens for local health systems across an entire region.

One participating healthcare professional noted that, if an institution's administration decided to evacuate the campus, managing the transition of already-infected students from the university's healthcare system to local healthcare systems could result in significant challenges. A less populated county with few dedicated health services resources may suddenly experience the need to care for a disproportionately large number of infected or at-risk students, straining existing resources. This challenge is not just a sudden burden for a local health system but may cascade well beyond the institution's local community. If an entire campus had to be evacuated and infected students were spread widely across the region the institution serves, it could create a large and complex problem for one or more states.

To avoid or mitigate this risk, university healthcare professionals should consider patient transfer procedures to handle the evacuation of students from campus for health reasons. Health departments and government authorities located near the campus should maintain close communications and coordinate activities. Maintaining communication with the students' hometown health authorities is critical for management of their move back home. Bringing in the relevant state agencies to coordinate this migration may be a powerful force multiplier.

**Core Capabilities:** Planning, Operational Coordination, Environmental Response/Health & Safety, Mass Care Services, Operational Communications, Public Health, Healthcare, & Emergency Medical Services

### *3.) Improving the Digital Fluency of Campus Populations to Operate Remotely*

- During an epidemic, faculty are likely to depend on educational technology systems with which they have limited familiarity to teach remotely.
- Training and practical exercises help students and staff acquire the skills to work and learn remotely.
- Student employees who are not fully equipped, faculty who are not fully trained, and IT staff not prepared to handle surges in remote needs during an outbreak may hamper operational effectiveness.

At multiple workshops, participants discussed concerns relating to remote work and learning. Some departments, specifically IT and the communications teams, use student workers to interface with the campus population, either to solve technical issues in person or to communicate through social media. Despite the importance of these roles during a disease outbreak, these student positions often do not have the option to work remotely like full-time employees may be instructed to do

Other participating IT professionals were concerned about their faculty's ability to quickly transition from classroom-based learning to remote-based learning. While some institutions have remote educational technology capabilities, most faculty are not fully trained or proficient on them. Institutions attempting to transition to remote learning during a crisis could create additional confusion and challenges.

Participants raised two major concerns for IT professionals during these discussions. The first category was ensuring adequate system hardware and bandwidth to handle a surge in demand. Many participants calculated resources needed for remote work or learning to handle the average expected network burden, but they had not considered simulations or exercises to determine if adequate resources handled a spike in demand. The second category focused on the expanded user population the scenario created. Not all staff, faculty, or students use the remote work or learning solutions at their institution during normal operations. For some universities, the percentage of users can be very low. Moving many untrained users onto remote systems requires a massive effort to increase their digital fluency and occupies staff resources with creating educational materials, conducting outreach, and fielding support calls.

Remote capabilities can be an important component of an institution's response to a disease outbreak, as well as other incidents. Leaders should consider preparing the community in its use of remote services before an incident occurs. Personnel performing mission critical tasks, even part-time and temporary employees, should be allowed to work remotely during emergencies. Training faculty to teach online would be valuable in advance of an incident. Most importantly, IT departments should consider the surge of untrained faculty required to use new tools or existing tools in new ways during an outbreak. This surge could overwhelm unprepared teams, especially those also suffering from staff absences. IT departments should focus on ensuring they have the hardware and bandwidth to handle larger-than-average usage, fielding significant volumes of calls from new users, and handling classes with unusual requirements, such as labs.

**Core Capabilities:** Planning, Access Control & Identity Verification, Cybersecurity, Community Resilience, Infrastructure Systems, Logistics & Supply Chain Management

### *4.) Natural Disasters Affecting the Medical Supply Chain*

- Natural disasters can affect critical supply chains, making it even more difficult to respond in the middle of a major incident.

A participating fire department shared their issues acquiring certain medical supplies after Hurricane Maria in 2018. Like many organizations, they had to work under limits on purchasing IV solutions in the immediate aftermath of the storm. Factories located in Puerto Rico were taken offline due to the damage. As a result, suppliers informed the department that purchases were restricted to one box of solution every two weeks, creating concerns for responding to medical calls. Due to the interconnected and international nature of today's supply chain, natural disasters in other parts of the world may affect the availability of important medical items and other critical dependencies.

### Supply Chain & Covid-19

DHS CISA has issued the following recommendations:

- Assess your organization's supply chain for potential impacts from disruption of transport logistics and international manufacturing slowdowns resulting from COVID-19.
- Discuss with those suppliers any challenges they may be facing or may expect to face due to the ongoing situation.
- Identify potential alternate sources of supply, substitute products, and/or conservation measures to mitigate disruptions.
- Communicate with key customers to keep them informed of any issues you have identified and the steps you are taking to mitigate them.

This is a difficult situation for institutions, as it is inherent to the difficulties of today's globalized and specialized economy. Barring a unified call for manufacturers to change practices and build greater redundancy into the global supply chain, there is no simple fix. However, institutions can identify critical supply dependencies and develop redundant acquisition methods to work without those supplies when availability is limited. Building the capability to function in this limited manner can be accomplished through stakeholder meetings, workshops, and tabletop exercises.

**Core Capabilities:** Supply Chain Integrity & Security, Environmental Response/Health & Safety, Public Health, Healthcare, & Emergency Medical Services, Health & Social Services

### 5.) *Managing Critical Student Employees During an Outbreak*

- Most IT departments employ students in critical IT positions, and their treatment as employees on one hand and as students on the other must be reconciled by the institution.
- Technical service support desks are an important component of campus IT services but reliance on student workers makes it difficult to operate remotely if required.

For IT departments, the first line of their public presence consists of campus help desks, which are primarily staffed by student employees. During an outbreak, student behavior maybe be restricted in different ways than employee behavior. For example, if an institution restricts students from class attendance while requiring employees' physical presence, what are the rules for student employees? This becomes an especially important question when those students are on the front lines during a major incident, e.g. answering phone calls and handling an increased volume of technical issues due to remote work. Not all participants were certain their department could scale their response capability if student resources were affected.

Many participating institutions employ a large number of student workers at their service desks. An epidemic situation potentially impacts the service continuity of support desks. To protect students on campus, the safest option during an outbreak may be to require remote work. However, most institutions require student service desk jobs to be on-site. Changing the infrastructure and processes to facilitate remote work could be challenging for institutions. While it may be possible to bring in additional resources from nearby or partnered schools to fill gaps, many participants articulated that it could be a challenge to integrate those resources quickly. Campus work study programs are primarily intended to help students gain practical experience; however, these student positions are still essential to an institution's response activities. IT departments should analyze the roles assigned to students to determine their critical functions during incidents. These roles may fall under the umbrella of "essential personnel" and, therefore, required to stay on campus for major incidents. Leaders should ensure that their student employees understand whether they have a role in the university's incident response or continuity plans and, if so, what is expected from them. Student employees can be critical employees and, as critical employees, they also need to be supported by an organization's emergency plans.

**Core Capabilities:** Planning, Operational Coordination, Cybersecurity, Infrastructure Systems

### 6.) *Reducing Response Time through Better Coordination and Improved Processes*

- There is a need for better coordination and processes between IT teams responsible for security.

A participating IT professional articulated a concern found to slow overall response to daily cyber incidents. When handling security alerts involving phishing, their team responds on a scale measured within minutes; however, the overall time to remediate these alerts remains high when solutions require actions by another IT team with slower response requirements. This disconnect between multiple teams speaks to a gap in coordination that frustrates institutional response. Coordination can be a political conversation and demonstrates where IT security risks have moved beyond being a purely technical matter.

This observation creates an opportunity for leadership, peer engagement, and coordination to bolster organizational readiness. IT security leaders should consider how other departments affect the security team's responsiveness. Opportunities exist to educate peers on the importance of cybersecurity and coordinate with them to better protect the university. Finding these opportunities requires knowledge of the team's processes, workflow, and potential points of failure. An action as simple as the email team providing temporary access to email controls could facilitate a successful response in an emergency.

**Core Capabilities:** Planning, Operational Coordination, Cybersecurity

### *7.) Mitigating Potentially Overburdened Local Third-Party Vendors during a Major Incident*

- An incident at multiple institutions may overwhelm the ability for a third-party vendor to provide services for all.

One unexamined potential point of failure is that multiple institutions in the same vicinity could overburden local vendors when affected by the same incident. Many participants' departments signed agreements with third parties in the community to provide backup services in case of an emergency, causing a surge in demand or availability restrictions on key providers. Since participants did not know how many other local organizations signed similar agreements with those same businesses, this could lead to a potential situation where, if a large number of that business's customers are impacted, a local resource could become overloaded attempting to fulfill multiple contracts. Consequently, the service provider could be unable to provide full service to everyone.

Countering this issue requires finding and mitigating critical points of failure in the local vendor community where an institution operates. Neighboring universities will need to cooperate to determine if they depend on the same businesses and, if so, work with the vendor to ensure contractual obligations. This discussion can become a potential foundation for joint workshops or exercises between organizations: first, to reduce potential points of failure and, second, test the effectiveness of current plans in potential points of failure.

**Core Capabilities:** Planning, Supply Chain Integrity & Security

### *8.) Adapting Emergency Plans to Employees Under Different Contracts/Policies*

- Employee contracts and classifications can restrict IT and Facilities employees from performing vital functions.

One participating institution shared concerns that workers' union contracts complicate its incident response. Specifically, the union consists of both IT and Facilities employees and is required to offer the same benefits to all members, including the option for remote work. During a disease outbreak, it is safer to remove as many employees as possible, including IT professionals, from potentially infectious campus sites. On the other hand, it is necessary for Facilities staff to remain on campus to perform essential functions until the outbreak is over (or under reasonable control). The participants were unaware if agreements with the union contained exceptions to these policies for emergency scenarios. If not, there could be delays in the school's response. Another participating institution had a similar concern with regards to remote work and its two different, contract-based classes of employees.

Employment contracts and policies can potentially hinder response efforts. Leaders should consider assessing potential conflicts and challenges that relate to organizational emergency plans before an incident. Leaders, legal counsel, emergency managers, and employee representatives should jointly exercise their plans to discover any critical contractual conflicts. These stakeholders can work together to solve issues equitably before an incident instead of during the incident. While each institution's legal position is different, amendments or addendums to contracts could be a powerful tool for the necessary flexibility to respond effectively to a major incident while keeping work protections, policies, and contracts in place.

**Core Capabilities:** Planning, Operational Coordination, Infrastructure Systems, Cybersecurity

### *9.) Sudden Network Burdens Could Overwhelm Resources*

- Any news of an epidemic is likely to burden an institution's network resources to an unprecedented level.

One participant noted that faculty, staff, students, parents, and other constituents are likely to change their online behavior at the onset of an epidemic, drastically increasing the load on the institution's network infrastructure for a variety of reasons:

- Many faculty may teach their classes remotely
- Parents may be searching for information from the institution
- Campus dorm residents restricted to sheltering in place will increase their use of the internet

These behavioral changes can overload the network's capacity and require extra attention from IT staff, especially if these actions create an inadvertent denial of service.

In these situations, IT staff must plan for tools and processes to increase availability or mitigate traffic load in advance. For example, tracking network usage baselines during periods of regular traffic can give operators an early warning system when those baselines change significantly. IT departments can employ network usage criteria as a rubric to determine the success of preventative measures. Popular streaming apps like Pandora, Spotify, or Netflix take up significant amounts of bandwidth during normal operating conditions. By understanding bandwidth restriction and balancing needs, the organization can prioritize high-value educational and research traffic, potentially restricting access to high volume entertainment streaming services. Teams can show agility when network congestion slows availability by preparing and planning for these events in advance, reducing network load without restricting critical services.

Any variety of high-visibility incidents can spur behavioral changes that tax critical online resources, as observed in the 2018 REN-ISAC Exercise Series based on a hostile event scenario. Leaders should build these expectations into their infrastructure as early as possible, even during service procurement. High levels of robustness built into systems allows for flexibility when confronted with the unexpected.

**Core Capabilities:** Cybersecurity, Infrastructure Systems

### *10.) Coordinating with Local Government Health Departments and Neighboring Universities' Student Health Departments*

- While most institutions plan to communicate with local government health departments during a communicable disease outbreak, there is a need for increased communication among neighboring university's health departments as well.

Participants brought up gaps in the ways they communicate with their local health departments and neighboring institutions during an outbreak. If an outbreak of an infectious disease is discovered on-campus, medical professionals at campus clinics are uniformly prepared to inform their county-level healthcare systems. However, most are not prepared to also inform their neighboring institutions, instead assuming the county-level system will do so, which might not always occur. Participants proposed gathering a list of campus health clinic contacts for all local schools and maintaining a forum for them to coordinate among themselves and the local health department. Institutions could be kept aware of health concerns in regional campuses while the local health department could use the information to provide direct assistance in providing state resources for afflicted schools.

Health leaders at institutions should consider how to best leverage their local health system to coordinate university response to health threats at a regional level. As discussed above, these departments can be invaluable for information sharing and requesting state or local resources during an incident. Building that relationship in conjunction with neighboring schools ahead of an outbreak reaps great benefit during the response phase. It can also serve as a foundation for more long-term coordination among local schools, such as mailing lists or coordinated training and drills.

**Core Capabilities:** Planning, Intelligence & Information Sharing, Public Health, Healthcare, Emergency Medical Services

### *11.)Supporting Employees During a Quarantine*

- Understanding the needs of essential employees who must still report to campus during quarantines and providing appropriately for their needs increases their safety.

A major theme of discussion was how best to support essential or critical employees, e.g. those who must be physically present for work even during major incidents such as a quarantine. Participants had prior experience with staff logistics during natural disasters, such as major blizzards, and provided relevant lessons learned. During one large snowstorm, an institution worked with a local venue to ensure essential employees could park their cars in heated, covered parking to prevent engines from freezing. The same care could be taken during a health event to prioritize employee safety. Participating health professionals suggested essential staff be subject to more stringent vaccination requirements, similar to those demanded of nurses or medical staff. Communication was another important aspect of protecting essential employees, with managers noting the importance of quick refreshers on established policies that would apply to the incident, e.g. sanitary guidelines and leave of absence requirements.

It is vital for leadership to prepare ahead of time to support essential employees during a quarantine, natural disaster, or other major incident. Understanding employees' needs when operating in a high-risk situation can be difficult. Prior discussion regarding the concerns, difficulties, and other potential issues experienced during such situations is key. These concerns can be discovered through exercises and practice involving incident response stakeholders. Solutions mitigating these concerns for essential employees could then be implemented before an emergency occurs.

**Core Capabilities:** Planning, Operational Coordination, Physical Protective Measures

### *12.)Preparing for Workforce Absences*

- Preparing for widespread workforce absences due to illness or natural disaster in advance minimizes disruptions when such events occur.

A major theme of discussion was handling expected workforce absences during an epidemic situation. The discussion included the importance of adequate preparation for this eventuality, such as ensuring documentation of staff duties for cross-training or to be used by others during absences. Prioritization was another important investment area. By ranking the criticality of responsibilities or essential functions, an institution can more easily determine what efforts can be paused, allowing staff time to contribute to critical and essential functions. The discussion included potential options for handling workforce absences in the middle of a crisis, such as enhancing staff by securing employees from other departments, or even other organizations, to backfill a diminished team. One example was temporarily reassigning nursing school staff, who are also required to keep up with their vaccinations, to the campus health team.

Overall, the participants agreed that it is better to prepare for reduced staff operations before an incident than to attempt to do so during one. Managers should consider hosting candid and open discussions with their teams about their critical tasks, both as individuals and as a group, and how to best support those tasks during periods of reduced resources, e.g. epidemics, natural disasters. Those discussions can inspire the creation of useful procedures, such as prioritization lists and documentation guidelines, reducing the burden on staff when an incident occurs. Many government agencies, such as FEMA and Health and Human Services (HHS), provide and collect useful continuity of operations planning resources and provide good starting point.

**Core Capabilities:** Planning, Operational Coordination, Operational Communications

### *13.) Protecting the Public Directory from Exploitation*

- Mitigating attacks against an institution's public directory can be difficult.

The vulnerability of an institutions' public directories may contribute to phishing attacks. Protecting the school's public directory is vital in reducing the risk of online targeting of students and staff. Participants discussed potential methods to make it harder for attackers to take advantage of this vulnerable asset. Most IT departments preferred obfuscation as the main tactic. This includes techniques such as implementing a captcha system to prevent hostile programs from accessing the directory, requiring a user to fill out a web form before receiving directory information, or generating random one-time emails to initially contact a person on entry. However, some IT professionals noted they have experienced organizational and cultural barriers when proposing these ideas, as some universities manage their directories at the departmental level and others consider the value of openness to outweigh the risk of exploitation.

Public directories are a useful tool in an academic environment, but they are also vulnerabilities that must be properly protected. IT professionals should consider informally testing their institution's directory, if public, and create a list of ways that attackers can exploit it to individually target students, faculty, and staff. Then, depending on how the directory is administered, the proper stakeholders can be brought in to analyze and discuss potential mitigations that would be acceptable to the stakeholders.

**Definition: Obfuscation**

The Trend Micro definition of Obfuscation is "the process of concealing something important, valuable, or critical." Obfuscation can be utilized by attackers or defenders.

**Core Capabilities:** Cybersecurity, Threats & Hazards Identification, Infrastructure Systems

### *14.) Registering Users in Mass Communications Services*

- Creating a mass communications service that requires users to opt-out instead of opt-in makes it more effective.

Organizations generally have two main options for registering users in mass communications services: requiring students, faculty, staff, alumni, parents, contractors, or any other interested party to opt-in to emergency notifications or automatic registration of users requiring them to opt-out of the emergency notifications. Since many institutions see very low registration rates when utilizing the first method, most participants preferred the second method, defaulting users into the system and make leaving an option that requires deliberate user action.

The modern college campus is an integrated collection of facilities. Managing all people present on an institution's property during a rapidly changing, major incident is a complex problem. Mass communications services help mitigate this concern by giving the administration immediate access to those most impacted by an event. However, these services are only effective if the majority of those who would be affected by a campus-wide incident are registered by the system. A system that automatically adds users and allows them to opt-out should typically lead to higher effective communication rates.

**Core Capabilities:** Public Information & Warning

### *15.) Formalizing Mass Communications Requests*

- A formal process to approve mass communications requests, with published criteria for the messages, ensures that only critical messages are transmitted and reduces unnecessary requests.

One area of workshop focus is the importance of and the processes supporting mass communications. One participating university police department managed a mass communication system for the campus and provided a description of how their staff operates the service. The department's priority is to utilize the system for only the most critical or time-sensitive messages to the campus, while declining or delaying lower priority requests. However, there is currently no formal criteria or threshold that defines what messages are important, making the process somewhat subjective, potentially inconsistent, and an ad hoc affair.

Creating a formalized criteria and process for what types of messages can be sent using an institution's mass communications service and who approves the messages allows leaders to better understand what constitutes an emergency and follow clear steps for the use of mass communications. This can reduce the number of lower priority requests during an emergency, as the process can be published in advance to help set campus expectations. Those involved with emergency management should consider gathering information on the current use of their institution's mass communications service and explore which types of incidents are best served by the system while not overloading it. These conversations can set expectations and be used to establish guidelines and procedures.

**Core Capabilities:** Public Information & Warning

### *16.) Planning for Surges of Public Information Requests During Incidents*

- The infrastructure in place to communicate information to the public can quickly be overwhelmed by a major incident.

One participating university police department identified concerns regarding incident management. While its first responders demonstrated the capability to surge in response to major events on campus, the department found it difficult to do the same for its public communications. As a public incident evolves, parents, alumni, and other concerned individuals will likely try to find information, departments do not always have the resources to handle an increased number of communications requests. The police department has addressed this issue on an ad hoc basis, depending on the institution's communications and IT departments to relieve some of the burden, but has not been able to find a sustainable solution.

Communications are a critical component of incident management. It can significantly reduce concerns, reducing staff time in answering individual questions, and promote greater, accurate education that leads to reasonable behavior by constituents. During an incident, many departments prioritize responding to, mitigating, and resolving the main problem over managing communications. Leaders should consider how their response plans might limit their staffs' ability to handle a sudden increase in volume because effectively communicating with the public should be every department's responsibility. If possible, consider utilizing temporary employees to fill gaps until the incident is over. These employees could come from other departments on campus, other campuses, or even other schools if a mutual aid agreement has been signed.

**Core Capabilities:** Planning, Public Information & Warning

### *17.) Conflict between Remediation Requirements and Legal Requirements*

- Planning and coordinating are required when IT teams need to restore systems and law enforcement needs to gather evidence.

During the final module involving a possible FBI investigation, one participant highlighted competing needs between responders trying to bring the network online and law enforcement trying to conduct investigation forensics. Due to various legal requirements, actions taken to restore the common network services can create complications—e.g. the deletion of critical evidentiary dates—for investigations and legal analysis. This can be further complicated during an outbreak or other emergency situation where key personnel are absent, as the chances of a legal error increase.

The incident response teams should bring in a legal representative as early as possible for situations that could potentially result in an investigation or legal case. Ideally, the incident response team would consult General Counsel when planning and preparing to ensure the IT and legal departments can work together to find the right balance between service restoration and investigative response. This further ensures that, even if key personnel are absent due to sickness or vacation, remaining employees have a well-researched foundation to provide coverage during a crisis. Another option is involving General Counsel in preparedness efforts, including the development of incident response plans and procedures. This ensures the consideration of complex legal issues in preparation, exercises, and incidents.

**Core Capabilities:** Planning, Operational Coordination, Forensics & Attribution, Cybersecurity, Threats & Hazards Identification

### *18.) Managing the Complexity in Shifting from Campus-based Operations to Remote Operations*

- While today's flexible work environment routinely involves and depends upon remote execution of duties, there may still be significant barriers to shifting to full-time remote operations.

One concern raised (reflected in multiple observations herein) is the difficulty of transitioning from an on-site to a remote staff population. There are many potential pitfalls that could occur during such a change in operations, and leaders are concerned about their departments' ability to identify and mitigate these risks in a timely manner. This includes logistical issues such as educating staff, managing student employees, and ensuring infrastructure scaling to handle network load, as well as cybersecurity issues such as ensuring the confidentiality, integrity, and availability of data being sent remotely. Encountering these problems without adequate planning could lead to significant delays in incident response, frustrating interconnected efforts, and increased risk for the institution and those they serve.

To avoid the pitfalls from such a massive shift, leaders need to invest time in preparatory activities and gain a nuanced understanding of the transition to remote work. A high-level working group will likely be necessary to allow relevant stakeholders to understand and review the steps involved in the process and identify areas of concern. Staff should create plans to address the areas of concern and exercise the plans to ensure adequate response, especially during a fast-paced incident such as a natural disaster or disease outbreak. The current outbreak of Covid-19 presents an opportunity for institutions perform a thorough after-action review process to analyze response efforts and provide the foundation for future incident management.

**Core Capabilities:** Planning, Operational Coordination, Cybersecurity, Long-Term Vulnerability Reduction, Operational Communications

## Challenges

Challenges are defined here as inherent issues that, in today's threat environment, are unable to be truly eliminated but may be mitigated. The observations highlighted here were all raised by participants in the six workshops.

### *1.) Controlling Access to an Integrated Campus*

- Protecting campuses integrated into the community can be difficult due to lack of authority over who is present on school property.

A participating school whose campus is largely integrated into a metropolitan area emphasized the difficulty of controlling access to its campus even in emergency situations. A large, public park runs through the middle of campus. During a prior measles outbreak that prompted the institution to declare an emergency, the administration found protecting the park visitors from the potential risk of infection challenging. For schools whose facilities are embedded into the local community, it might be impossible to truly control who is present on or near their property.

**Core Capabilities:** Access Control & Identity Verification, Long-term Vulnerability Reduction

### *2.) Managing Personnel Making the Unilateral Decision to Not Report to Work*

- Staff, independent of guidance from management, will make decisions regarding their presence or absence based on public information.
- The longer or more widespread an epidemic becomes, the higher the risk of staff absences, due to various considerations.

One underlying concern was that individual employees are likely to make their own determination of whether it is safe to come to work. Illness, caring for others, health concerns, and other challenges may impact employee's independent decision whether to report to a potentially infected campus before management or the administration makes that decision and provides guidance. Critical staff may be absent, both for daily operations and for incident response. Even if provided guidance, some personnel may not attend work due to concern for their health or the health of their loved ones, especially if there is public unease over the outbreak. Clear guidance that sets employee expectations at the start of an incident, as well as cross-training of team members, can partially mitigate this risk; however, institutions should consider independent decisions by employees as part of any disease response plans.

**Core Capabilities:** Planning, Operational Coordination

### *3.) Health FUD and Preparing for Possible Panic During an Epidemic*

- During an epidemic, countering fear, uncertainty, and doubt (FUD) is extremely difficult.

Managing an institution's communications in the face of a publicized epidemic on campus is difficult, especially where FUD is likely to emerge. There is no avoiding the potential panic and irrational responses that such an announcement produces, only methods to mitigate and reduce. The university has important recommendations, such as when to (and not to) physically go to university health centers if community members health centers believe they are infected during an epidemic. Institutional information authorities must educate students, staff, and parents on trusted information sources during the epidemic and provide enough information to ensure the community reduces the risk of infections through their actions.

**Core Capabilities:** Public Information & Warning

### *4.) Managing the Movement of Non-Residential Students During an Outbreak*

- Institutions have limited ability to track and influence the behavior of students that do not live on campus but are often present on campus.

One challenge raised was the management of non-residential students, especially in institutions with a large percentage of commuter students who attend classes on campus but live elsewhere. Unlike students in residential facilities, whose actions can be more easily tracked and influenced, the mobility of non-residential students is harder to regulate. An infected student has an impact on campus health regardless of where they reside, but there is little awareness about non-residents' medical status. The institution has fewer tools to change their behavior if non-resident students are infected. Beyond university provided education and outreach, institutions must depend largely on that student's own community health infrastructure to counter an outbreak. Students studying abroad in high risk areas present similar but specific challenges, as discussed at many of the workshops.

**Core Capabilities:** Planning, Public Information & Warning, Situational Assessment, Health & Social Services, Access Control & Identity Verification

## Section 4: Conclusion

The 2019 REN-ISAC Blended Threat Resilience Workshop Series successfully achieved the individual and collective exercise objectives and created valuable dialogue among participants, including higher education, critical health, and security professionals. The exercise highlighted Best Practices, Areas of Improvement, and Challenges that can be further explored and developed to bolster higher education security preparedness, response, coordination, and resilience. These observations can benefit schools at the individual, community, and national levels.

During a seven month period, the REN-ISAC successfully facilitated meaningful discussions that preceded a similar, but much larger, real world event in the COVID-19 pandemic. Unexpectedly, this series had an added benefit of enabling the attending organizations to start thinking about the issues they would soon have to manage in real-time, including continuity, remote access, cyber-scams, and managing with limited resources.

Among the outcomes from the workshop series, REN-ISAC aimed to identify best practices, preparedness gaps, opportunities for improvement, and other security and resilience considerations. The workshop discussions allowed for the sharing of insights, experiences, issues, and enduring challenges that have helped to enhance the REN-ISAC's and participating organizations' understanding of the higher education security environment.

This report strives to share those valuable ideas and considerations to higher education and partner organizations dealing with today's complex and blended threat environment. The workshop findings can provide perspective on the ongoing challenges and rapidly changing needs of the 2020 global pandemic. Taken together with in-progress or after-action assessments of their real-world response, organizations have a tremendous opportunity to bolster preparedness and operational activities. As isolated measles and mumps outbreaks in 2019 and the COVID-19 pandemic in 2020 have shown, health threats are a persistent and potentially rapidly evolving reality, as are the opportunistic attacks criminals will execute even—or perhaps especially—in the face of life-threatening disruptions.

REN-ISAC thanks all of the participating institutions in Iowa, Indiana, Ohio, Oregon, Texas, and Maryland that candidly shared their experiences and valuable perspective in this national, crowdsourced report intended to inform and bolster the higher education community's collective security, preparedness, and resilience.

# Appendix A: Acronyms

- CDC – Centers for Disease Control and Prevention
- CISA – Cybersecurity and Infrastructure Security Agency
- DDoS – Distributed Denial of Service
- DHS – U.S. Department of Homeland Security
- DOE – U.S. Department of Education
- DOJ – U.S. Department of Justice
- DOL – U.S. Department of Labor
- FEMA – Federal Emergency Management Agency
- FUD – Fear, Uncertainty, and Doubt
- HHS – U.S. Department of Health and Human Services
- HSEEP – Homeland Security Exercise and Evaluation Program
- IT – Information Technology
- PPE – Personal Protective Equipment
- REN-ISAC – Research and Education Networks Information Sharing and Analysis Center
- UNESCO – United Nations Educational, Scientific, and Cultural Organization
- WHO – World Health Organization

# Appendix B: Complete 2019 Scenario and Questions

*Note: [T] is used as a substitute value for the date the workshop occurred. All dates in each module are based around [T].*

*Note: This appendix contains the final version of the scenario, refined after execution at multiple workshops.*

## Module One: Eruption

### Scenario

It is [T-8 Weeks], and the World Health Organization (WHO) has released a global alert announcing the emergence of a new strain of measles, discovered to be immune to most conventional measles vaccines, designated Measles-2. This variant emerged in the Ukraine, specifically the Lviv province. First reported on [T-20 Weeks], it had been previously thought to be contained to the rural areas of the region. 21,864 cases were confirmed and reported to the WHO between [T-20 Weeks] and [T-12 Weeks]. 108 of those cases were fatal, mostly among young children and the elderly.

However, from [T-10 Weeks] to [T-9 Weeks], approximately 400 European, American, and Asian business professionals resided at the Grand Golden Hotel in Lviv during an international information technology and security conference. During the conference, several food servers, reception event staff, and event hotel guests presented measles-like symptoms and were later confirmed to have contracted Measles-2. At the end of the week, around 40% of the conference guests had preliminary symptoms of the disease. The WHO was notified of this series of events by the Ukrainian government on [T-8 Weeks, 2 Days].

On the heels of the announcement, the international media is reporting that Measles-2 cases have emerged in the home countries of some conference attendees.

### Questions

1. How would you anticipate gaining initial awareness of this potential hazard?
2. Organizationally, who is responsible for monitoring such threats?
    a. How do they monitor such information?
    b. How is it shared/discussed within your organization?
    c. Is there a process to assess and respond to health threats?
3. Would your institution respond in any way to the situation as it developed within Ukraine? Would that change as it emerges domestically?
4. At what point does a health threat become a concern to your organization?
5. What types of activity would you anticipate being involved with at this time?
    a. Would you be discussing this development within your organization?
    b. Would you be coordinating with anyone externally?
    c. Do you have plans and procedures for responding to emerging or imminent health threats?

# Module Two: The Full Bug

## Scenario

It is [T-4 Weeks]. Since the initial announcement by the WHO, the Centers for Disease Control and Prevention (CDC) released its own health alert. The agency also activated its Emergency Operations Center and issued a set of interim guidelines on Measles-2 for state and local health departments. Two weeks ago, the first domestic cases of Measles-2 were discovered, motivating the CDC to issue additional guidelines and a health alert notice for travelers to the United States from the Ukraine.

Until recently, these cases have remained confined to small outbreaks in regions with low measles vaccination rates. However, State University's campus health center has discovered a student experiencing Measles-2-like symptoms after returning from time at home with family in New York City, where one of these outbreaks is occurring. This student informed medical staff that they recently attended [relevant major campus event] where a large number of students and alumni were present. Since this disclosure, the university has discovered that approximately [1%-5%] of event attendees have reported Measles-2-like symptoms. Absences among both students and staff have risen sharply with the release of this information, and smaller departments are concerned about personnel shortages.

## Questions

1. What are your biggest concerns and challenges at this time?
2. With news of large-scale infections at the [relevant event], what is your communications plan?
    a. Who is involved in developing the institution's communications?
    b. What populations will you target?
    c. Who is responsible for communicating to different populations?
    d. What is your message?

## Small Group Discussions

1. Will your operations change due to the infections and enduring threat?
    a. What are the thresholds for modifying, or even suspending, class or work schedules due to the outbreak?
    b. Would you implement business continuity plans at this point?
    c. Are there other operational considerations that need to be considered?
2. How will your departments be impacted by the personnel shortages?
    a. Which departments are the most critical to operations?
    b. What do they need to be functional?
    c. Are there any gaps or issues you can identify?

# Module Three: Best of Both Worlds

## Scenario

It is [T-2 Weeks]. Over the last two weeks, the number of Measles-2 infections on campus and in the nearby community have continued to increase. This has had an effect on campus operations as significant numbers of students and employees are calling in sick or taking vacation time to care for sick family members. The IT and emergency management departments have been especially impacted by the loss of essential personnel.

Today State University's IT department reported the potential for a data breach after observing suspicious activity related to school accounts used by teaching staff associated with the university, including with the university's hospital. It is believed these accounts were compromised two days ago during a phishing campaign that targeted the university. The lure email contained an attachment claiming to be an updated health alert issued by the government. It is difficult to determine what data has been exfiltrated. However, since the staff members were both medical professionals and professors, the compromised accounts had access to large amounts of sensitive data.

## Questions

1. How would you anticipate responding to such an incident under "normal" circumstances and fully staffed?
2. Do you have continuity plans and would they support this situation?
3. Do you have Memorandums of Agreement/Understanding in place with other institutions or organizations?

## Small Group Discussions

1. People
    a. Which positions' absences would make it more difficult or impossible to respond properly?
    b. Are there vital functions that may be impacted?
2. Response
    a. What would you need to effectively (or more effectively) respond in this situation?
    b. Is there equipment, training, external resources (Memorandums of Understanding, vendors) that can support a more effective response?

## Module Four: Right Now

### Scenario

It is [T] and it has been a month and a half since the outbreak of Measles-2 began in the United States and State University's campus health center and hospital has filled 100% of their bed capacity. The majority of students and teachers are not showing up for classes and every university department has been impacted, with essential staff absent due to the outbreak. Beyond those that are sick, many are also out due to caring for infected family members, local school closures, or fear of exposure.

Today, DHS Cybersecurity and Infrastructure Security Agency (CISA), working in partnership with the Department of Justice (DOJ), REN-ISAC, other higher education institutions, and private sector security entities, has announced that the phishing campaign seen two weeks ago was part of a broader campaign by a suspected nation-state actor targeting research activities in both higher education and the private sector. CISA has also issued an alert containing technical details, mitigations, and additional resources regarding the campaign. At the same press conference, the DOJ issued indictments for multiple Russian nationals. This list includes Russian citizens currently residing in America, one of which is an assistant professor and researcher at State University.

### Questions

1. After being informed that a past cyber-attack was potentially committed by an Advanced Persistent Threat actor, what actions would you take?
    a. How credible would the intelligence have to be to take action?
2. What would you want to know from government and peer institutions?
3. What would you expect internal actions to be?
    a. What security actions would you be taking?
    b. What would you need from others at your institution?
    c. What internal communications would be occurring?
    d. What, how, and with who would you be communicating externally?

### Small Group Discussions

1. Pandemic Planning – Planning (See Appendix D: Resources – FEMA Commercial Facilities Pandemic Influenza Guides)
2. Pandemic Planning – Facilities (See Appendix D: Resources – FEMA Commercial Facilities Pandemic Influenza Guides)

## Appendix C: Combined Observations

For this summary report, similar observations from multiple venues have been combined into one observation for ease of reference. In order to respect each discussion conducted during the workshops, the chart below identifies the sources of each observation.

[1] Observation Type:

- AoI: Area of Improvement
- BP: Best Practice
- CH: Challenge

[2] Original Venue:

- UNI: University of Northern Iowa
- PUFW: Purdue University Fort Wayne
- YSU: Youngstown State University
- NWACC: NorthWest Academic Computing Consortium
- ACU: Abilene Christian University
- UMBC: University of Maryland Baltimore County

[3] Core Capabilities (FEMA):

- Distinct critical elements necessary to meet the National Preparedness Goal.
- Essential for the execution of each Mission Area.
- Developed and sustained through the combined efforts of the whole community.

*Note: Venue indicates the venue(s) where the discussion occurred, not the institution(s) that discussed the observation.*

| Observation | Type[1] | Original Venue[2] | Core Capabilities[3] |
|---|---|---|---|
| **Storing the Disaster Recovery Plan Safely and Maintaining Back-Ups** | BP | • UNI | Planning,<br>Operational Coordination, Risk Management for Protective Programs & Activities,<br>Operational Communications |
| **Preparing First Responders for a Highly Contagious Disease Outbreak** | BP | • ACU | Planning,<br>Operational Coordination, Risk Management for Protection Programs & Activities,<br>Threats & Hazards Identification,<br>Public Health,<br>Healthcare,<br>Emergency Medical Services |

| | | | |
|---|---|---|---|
| **Providing Self-Care Kits to Students** | BP | • PUFW | Public Information & Warning, Community Resilience, Long-Term Vulnerability Reduction, Environmental Response/Health & Safety |
| **Utilizing Social Media to Track Campus Reaction to an Outbreak** | BP | • UMBC | Public Information & Warning, Intelligence & Information Sharing, Situational Assessment, Health & Social Services |
| **Conducting Post-Event Self-Assessments** | BP | • ACU | Cybersecurity, Planning |
| **Assigning Functions to Roles, Not People** | BP | • UNI | Planning, Operational Coordination, Operational Communication |
| **Maintaining a Positioned-based Continuity Document** | BP | • YSU | Planning, Cybersecurity, Risk & Disaster Resilience Assessment |
| **Increasing User Engagement in Cybersecurity** | BP | • NWACC | Cybersecurity, Public Information & Warning, Community Resilience |
| **Creating a Phishing Lure Database** | BP | • NWACC | Cybersecurity, Threats & Hazards Identification, Community Resilience |
| **Providing First Responders Access to Protected Health Data** | BP | • PUFW | Planning, Intelligence & Information Sharing, Screening, Search, & Detection, Long-Term Vulnerability Reduction, Environmental Response/Health and Safety, Public Health, Healthcare, Emergency Medical Services |
| **Advocating for Disease Resiliency** | BP | • PUFW | Planning, Risk Management for Protection Programs & Activities, Long-Term Vulnerability Reduction |
| **Preparing for Crisis Communications** | BP | • YSU | Planning, Public Information & Warning, Infrastructure Systems |
| **Centralizing Public Communications During a Crisis** | BP | • ACU | Planning, Public Information & Warning |

| | | | |
|---|---|---|---|
| **Creating a Risk Management Program with Representatives from Critical Departments** | BP | • YSU | Planning, Risk & Disaster Resilience Assessment |
| **Executing Quick and Focused Drills with Teammates** | BP | • YSU | Planning,<br>Risk & Disaster Resilience Assessment,<br>Operations Coordination |
| **Prioritizing Threats and Risks to the Organization** | BP | • NWACC | Planning,<br>Cybersecurity,<br>Threats & Hazards Identification |
| **Exercising and Training on Existing Policies and Procedures Builds Resilience** | AoI | • NWACC<br>• UMBC | Planning,<br>Operational Coordination,<br>Cybersecurity,<br>On-scene Security, Protection, & Law Enforcement, Operational Communications,<br>Health & Social Services |
| **Coordinating Healthcare While Transitioning Infected Students to Home Counties is an Important Consideration** | AoI | • UNI | Planning,<br>Operational Coordination,<br>Environmental Response/Health & Safety, Mass Care Services,<br>Operational Communications,<br>Public Health,<br>Healthcare, &<br>Emergency Medical Services. |
| **Improving the Digital Fluency of Campus Populations to Operate Remotely** | AoI | • UNI<br>• YSU<br>• UMBC | Planning,<br>Access Control & Identity Verification,<br>Cybersecurity,<br>Community Resilience, Infrastructure Systems, Logistics & Supply Chain Management |
| **Natural Disasters Affecting the Medical Supply Chain** | AoI | • PUFW | Supply Chain Integrity & Security,<br>Environmental Response/Health & Safety, Public Health,<br>Healthcare,<br>Emergency Medical Services, Health & Social Services |
| **Managing Critical Student Employees During an Outbreak** | AoI | • UNI<br>• YSU | Planning, Operational Coordination, Cybersecurity, Infrastructure Systems |
| **Reducing Response Time through Better Coordination and Improved Processes** | AoI | • UMBC | Planning,<br>Operational Coordination,<br>Cybersecurity |

| | | | |
|---|---|---|---|
| **Mitigating Potentially Overburdened Local Third-Party Vendors during a Major Incident** | AoI | • YSU | Planning, Supply Chain Integrity & Security |
| **Adapting Emergency Plans to Employees Under Different Contracts/Policies** | AoI | • YSU | Planning, Operational Coordination, Infrastructure Systems, Cybersecurity |
| **Sudden Network Burdens Could Overwhelm Resources** | AoI | • UNI | Cybersecurity,<br>Infrastructure Systems |
| **Coordinating with Local Government Health Departments and Neighboring Universities' Student Health Departments** | AoI | • ACU | Planning,<br>Intelligence & Information Sharing,<br>Public Health,<br>Healthcare,<br>Emergency Medical Services |
| **Supporting Employees During a Quarantine** | AoI | • PUFW | Planning,<br>Operational Coordination, Physical Protective Measures |
| **Preparing for Workforce Absences** | | • PUFW | Planning, Operational Coordination, Operational Communications |
| **Protecting the Public Directory from Exploitation** | AoI | • NWACC | Cybersecurity,<br>Threats & Hazards Identification,<br>Infrastructure Systems |
| **Registering Users in Mass Communications Services** | AoI | • NWACC | Public Information & Warning |
| **Formalizing Mass Communications Requests** | AoI | • ACU | Public Information & Warning |
| **Planning for Surges of Public Information Requests During Incidents** | | • ACU | Planning,<br>Public Information & Warning |
| **Conflict between Remediation Requirements and Legal Requirements** | AoI | • UMBC | Planning,<br>Operational Coordination, Forensics & Attribution, Cybersecurity,<br>Threats & Hazards Identification |
| **Managing the Complexity in Shifting from Campus-based Operations to Remote Operations** | AoI | • n/a | Planning,<br>Operational Coordination,<br>Cybersecurity,<br>Long-Term Vulnerability Reduction,<br>Operational Communications |

| | | | |
|---|---|---|---|
| **Controlling Access to an Integrated Campus** | Ch | • NWACC | Access Control & Identity Verification, Long-term Vulnerability Reduction |
| **Managing Personnel Making the Unilateral Decision to Not Report to Work** | Ch | • UNI<br>• YSU | Planning<br>Operational Coordination |
| **Health FUD and Preparing for Possible Panic During an Epidemic** | Ch | • UNI | Public Information & Warning |
| **Managing the Movement of Non-Residential Students During an Outbreak** | Ch | • UMBC | Planning, Public Information & Warning, Situational Assessment, Health & Social Services, Access Control & Identity Verification |

# Appendix D: Resources

## General Resources

- Epidemic/Pandemic Resources, DHS
- Ready Pandemic Resources, Ready.gov
- Commercial Facilities Pandemic Influenza Guides, FEMA
- Core Capability Development Sheets, FEMA
- Emergency Management Institute (EMI), FEMA
    - FEMA EMI IS-100.C Introduction to the Incident Command System
    - FEMA EMI IS-200.HCA: Applying ICS to Healthcare Organizations
    - FEMA EMI Higher Education-specific Courses
- Continuity of Operations Resources, FEMA
- Continuity of Operations Topic Collection, HHS
- Health Alerts and Emergencies, CDC
- US-CERT Alerts, CISA
- OSHA Guidance on Preparing Workplaces for an Influenza Pandemic, DOL
- Fusion Center Locations and Contact Information, DHS
- Protective Security Advisor Program, DHS
- S.1379 - Pandemic and All-Hazards Preparedness and Advancing Innovation Act of 2019 (signed into law on 24 June 2019; White House Statement)

## COVID-19 Specific Resources

### Health Resources

- Coronavirus Disease 2019 (COVID-19), CDC
- Coronavirus Disease (COVID-19) Outbreak, WHO
- Coronavirus COVID-19 Global Cases, Johns Hopkins CSSE
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), CISA
- COVID-19 and the American Workplace, DOL

### Information Security Resources

- Network Security Perspective on Coronavirus Preparedness, SANS Technology Institute
- SANS Security Awareness Work-From-Home Deployment Kit, SANS Technology Institute
- COVID-19 Security Resource Library, National Cyber Security Alliance
- COVID-19 Resource Page, Educause
- Maintaining IT Services During a Health Incident, REN-ISAC

### Higher Education Resources

- Interim Guidance for Administrators of US Institutions of Higher Education, CDC
- Addressing Biological Hazards That May Impact Students, Staff, and Visitors, DOE
- COVID-19 Educational Disruption and Response, UNESCO
- Distance Learning Solutions, UNESCO