2018 REN-ISAC Blended Threat Resilience Workshop Series

Final Findings Report

July 31, 2019

TLP: WHITE

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 2018 REN-ISAC Blended Threat Resilience Workshop Series, including our hosts, our planning teams, the REN-ISAC Board, 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 2019 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 hosted the 2018 workshop series workshops. Without their help, this report would not have been possible.

Executive Summary

From May to October 2018, REN-ISAC led the development and implementation of six analogous workshops across the United States as part of the 2018 REN-ISAC Blended Threat Resilience Workshop Series. These exercises occurred in Indiana, Arizona, North Carolina, Oregon, Massachusetts, and Florida and involved member and non-member institutions, higher education organizations, and other private and public sector partners involved in higher education security.

Recognizing the changing threat landscape and the risk implications technology has across higher education, REN-ISAC sought to facilitate meaningful discussion regarding security preparedness outside the silos of physical and cyber security, beyond traditional emergency management, and outside the walls of a single institution—all in order to glean valuable insights and to inform and enhance the individual and collective security and preparedness of the research and education community across the United States and throughout the broader REN-ISAC membership.

By all measurements, the 2018 REN-ISAC Blended Threat Resilience Workshop Series was a success. The 13 Best Practices, 18 Areas of Improvement, and 7 Challenges identified in this report provide valuable lessons learned through both discussion and real-world experiences that the entire community of higher education and partner organizations can learn from, discuss, and apply in a variety of ways to enhance their preparedness and operations.

The events' composition allowed for open and effective conversation among the participants and provided insights into the complexities of higher education security preparedness, response, and coordination. The workshop discussions provided new ideas, successes, and complications, as well as enhanced REN-ISAC's and participating organizations' understanding of the higher education security environment. Taken together, there has been tremendous value in the national conversation and the collective findings.

Throughout the series, workshop observations addressed the importance of effective collaboration and explored a number of opportunities that may further enhance security and resilience across the higher education community, and in partnership with vital stakeholders. The workshops reiterated and expanded upon some common observations and areas of improvement organizations need to enhance as part of their continued organizational security preparedness. Many of the observations were recurring at multiple venues and validated important issues such as:

- A comprehensive campus speaker approval process
- Preauthorized procurement procedures in place before an incident occurs
- Identifying and protecting of critical facilities
- Increased IT security's involvement in the response to physical incidents
- Opportunities in better connecting higher education with broader security and emergency management organizations
- The value in exercising and validating plans and procedures
- The challenge of protests occurring whether or not school approves controversial event
- The increasing complexities surrounding media, social media and managing "The Story"

This report aims to provide valuable insights and considerations to the research and education community so that organizations can learn from these findings and use them to enhance their individual and collective security and preparedness in this evolving threat environment.

Workshop Series Background

The REN-ISAC Blended Threat Resilience Workshop Series began out of a desire to increase the capability of the higher education community to respond to the possibility of blended threats. In order to achieve this goal, the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC) planned and executed six workshops in a diverse series 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 and result in a product. The primary purpose of this series was to raise awareness of the blended threats concept, to allow security professionals from different disciplines to interact, and to document the innovations and challenges the higher education community is encountering as it navigates complex security issues.

For the purposes of this series, REN-ISAC defines blended threats as a natural, accidental, or purposeful physical or cyber danger that has or indicates the potential to have crossover implications and harm life, information, operations, the environment, and/or property. This type of threat is a growing possibility in today's interconnected world. Cyber and physical emergency response and preparedness efforts need to begin now in order to be ready for likely incidents—from the annoying to the catastrophic—in the years to come.

REN-ISAC's inaugural 2018 program utilized a realistic and threat-informed scenario based on a hypothetical, controversial speaking event and cyber incident. By using this topic to focus the discussion, participating professionals could confront a topical concern that many campuses are facing while also speaking to the broader topic of blended threats. REN-ISAC documented these conversations and extrapolated high level observations from each event in order to create two types of reports. First, six individual workshop reports were created for participants of the six events, containing observations from the workshop they attended. Second, the series report (this document) contains the most relevant observations from across the entire series, collated and merged based on importance and relevance.

Highlights

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 possibly enhance their security posture.
- **Challenges** – Inherent issues that, in today's threat environment, are unable to be truly eliminated, just mitigated.

Section 2 goes into further detail for each observation. Appendix C: Combined Observations contains a list of which observations were merged due to being present at multiple 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.

Best Practices

1. A Comprehensive Campus Speaker Approval Process
2. Multi-Year, Multi-Stakeholder Meetings and Exercises
3. Proactive Management of Protest Groups On-Campus
4. Full IT Support to the Emergency Operations Center

5. Preauthorized Procurement Procedures in Place Before an Incident Occurs
6. Contact with and Learning from Other Institutions with Experience
7. Memorandums of Understanding to Defer Cyber Risk
8. Fusion Center Integration with the Education Sector
9. Incident Response Staff Rotation
10. Event Coordinator as Primary Security Coordinator
11. Resilience Provided by Redundant Communications Methods
12. Third-Parties to Enhance Communications Capacity During and After Critical Incidents
13. Mutual Awareness of Scheduled Events

Areas of Improvement

1. Exercising and Validating Plans
2. Conducting Institution-Wide After-Action Reviews in the Aftermath of Major Incidents
3. Determining Thresholds for Cutting Off Critical Network Resources
4. Increasing IT Security's Involvement in the Response to Physical Incidents
5. Streamlining Emergency Responders' Access to Internal Campus Resources
6. Providing Cyber Defenders with a Broader Threat Context
7. Using Social Media and Email Monitoring to Improve Awareness, Planning, and Response
8. REN-ISAC Providing Social Media Awareness Resources
9. Connecting to Broader Security and Emergency Management Organizations
10. Requesting Threat Assessments from Local Law Enforcement
11. Improving the Process to Provide Law Enforcement with Pertinent Evidence after Violent Events
12. Involving Students in the Emergency Response Process
13. Identifying and Communicating Organizational Information Requirements
14. Reducing Alert Fatigue
15. Cost of Security
16. Reducing Duplication of Effort
17. Reluctance to Share Information about Cyber-Attacks

Challenges

1. Protests May Occur Regardless of Controversial Event Approval
2. Deciding on Appropriate Law Enforcement Presence at High Risk Events
3. Managing Insider Threat
4. The Rapid Pace of Media, Social Media, and "The Story"
5. Media Sensitivity to Cyberattacks
6. Protest Organization Moving to Private Channels
7. Split Attention During Crises

Section 1: Workshop Series Overview

Purpose & Design

Scope

The following is the scope of the 2018 workshop series as approved by the 2018 REN-ISAC Blended Threat Resilience Workshop Series Planning Team:

In CY2018, REN-ISAC will lead the development of six physical security-focused discussion-based exercises, which will be workshop events. These exercises will be conducted between May – October at six geographically diverse locations around the domestic United States, and to be approximately six-hours each. Exercise participants are expected to be lead physical security and emergency management personnel and / or their 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 physical security scenario to prompt discussion and share approaches from leaders in the community regarding physical security preparedness and response (these exercises will not focus on recovery) to help inform organizational physical security preparedness.*
- *Provide participants an opportunity to interact with one another and discuss issues, concerns, best practices, and other salient points to help inform organizational physical security 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 physical 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 physical security preparedness.*
- *REN-ISAC will provide participants and their organizations a roll-up summary of the complete 2018 exercise series by 30 Nov 2018 to help inform organizational physical security preparedness.*

Scenario

During the planning process, the planning team developed the following scenario, which was executed in five parts. At the beginning of each module, a situational update about a controversial speaker applying to speak at the mock university (along with supporting media) was presented to attendees. Once complete, there was a discussion section guided by the lead facilitator, using both questions pre-selected by the planning team and those that surfaced during the natural flow of conversation. The five modules were sequential and built on the base scenario

There are two modules in the scenario that were vignettes. Vignettes are modules that have two or more variants that can be substituted for each other. These variants covered the same emergency preparedness themes but utilized different situations. Modules Three and Five were vignettes. Each had two variants.

The following are summaries of the five modules and vignettes exercised during the 2018 series. The full text of the 2018 modules, the vignettes, and associated questions can be found in Appendix B: 2018 Scenario and Questions.

Module One: Twist and Shout

A week prior to the date of Module One, REN University, the fictitious university used throughout the entire scenario, received an application from a controversial speaker to use the campus's facilities for a speech and reception. On the date of Module One, six months before the speech, REN University announced the existence of the event. The university's statement gathered local and national media attention and there were activist groups who quickly stated their intent to support or oppose the speech.

Module Two: Power to the People

On the date of Module Two, one month before the speech, REN University tracked multiple Facebook events created by local and national groups to support or oppose the speech. It appeared likely a large number of protestors from out of state would be on campus. In addition, REN University became aware of a cyber activist group threatening to target campus networks.

Module Three: Revolution – Vignette One

On the date of Module Three, two weeks before the speech, REN University became aware of a "target list" on Pastebin containing sensitive information on professors, students, and staff. This list had been distributed on specific activist websites and forums alongside concerning language involving those on the list.

Module Three: Revolution – Vignette Two

On the date of Module Three, two weeks before the speech, REN University became aware of potentially concerning network activity. A university cybersecurity vendor has alerted the institution of concerning social media conversations suggesting hacktivists have conducted reconnaissance against the school's network. University analysts have also reported suspicious network activity that could have been a trial distributed denial of service attack.

Module Four: Come Together

On the date of Module Four, the day of the speech, the event occurred as planned. REN University's campus was crowded with a larger number of protestors than expected. Before and during the speech, there were reports of violence between protestors and counter-protestors, both near the facility where the speech was held and at other locations on campus.

Module Five: Something – Vignette One

On the date of Module Five, the day of the speech, a vehicular ramming attack occurred on REN University's campus after the speech finished. A car rammed into a large crowd crossing a road on campus, resulting in a dozen injuries, some life threatening. The driver of the car escaped the scene but was apprehended by police. National media coverage was at the preliminary stage during the module, with many inaccurate pieces of information being reported.

Module Five: Something – Vignette Two

On the date of Module Five, the day of the speech, an improvised explosive device detonated on campus after the speech finished. It was located in a trashcan on a well-traveled pathway between the

venue and the main parking lot. Over a dozen were injured, some to a critical degree. National media coverage was only at the preliminary stages during this module, with many inaccurate pieces of information being reported.

Section 2: Analysis & Observations

Best Practices

Best Practices are defined as procedures identified as valuable, or effective.

1.) A Comprehensive Campus Speaker Approval Process

- Institutions can gain better intelligence on the risk of an event by integrating emergency management into the speaker approval process.
- A single, online form that automates the process of notifying the correct stakeholders involved in event-application approval reduces the chance of not recognizing a potentially controversial application.

A topic covered in multiple workshops was how schools process applications for speakers and other events. Controversial speakers have increasingly drawn the attention of the national news media, as well as potentially violent protesters and counter-protesters. In response, participants' institutions have been investing time in refining their speaker approval process. Multiple schools explained how they had incorporated a threat assessment into the steps required to host an event on campus. Some schools required the assessment for every event above a certain defined threshold. Other schools placed the responsibility for deciding the need for an assessment on a specific university official, most often from the student affairs department.

In an attempt to automate this procedure, one participating institution detailed how it built an event registration process, focusing on the checks and balances necessary to handle the concerns of a potentially controversial event application. The university has a standard online form that anyone interested in hosting an on-campus event is required to fill out. Depending on the information provided, the application is automatically emailed to the appropriate stakeholders to review the request. For example, the institution's police department always reviews an event request for security concerns, while student life only becomes involved if the form indicates that a student or student-run organization is planning the event. It has taken years to refine the process of ensuring these emails are sent to the appropriate groups based on the specific information entered into the form. While there are still occasional unsanctioned events on campus, this system has reduced the burden of event management for all involved according to participants.

Unifying and strengthening the approval process for campus-associated events gives schools an earlier awareness of the activities hosted on their campus and the potential consequences that could result. This lengthens the amount of time and resources the school can spend preparing for a potentially dangerous event, improving the overall quality and effectiveness of the response. Using a single online portal streamlines applications for any entity interested in planning an on-campus event and allows the appropriate departments to quickly become aware of any potential issues and address them within a reasonable amount of time. One challenge identified with automating the approval process is that this transition requires an investment of time and resources, as well as ongoing cooperation between the information technology (IT) and emergency management departments. Once an institution is acclimated to using the portal, it can be a powerful tool to manage the varied activities that occur on a college campus.

Core Capabilities: This observation speaks to the Planning; Intelligence and Information Sharing; Threats and Hazards Identification; and On-scene Security, Protection, and Law Enforcement capabilities.

2.) Multi-Year, Multi-Stakeholder Meetings and Exercises

- Creating and maintaining relationships, both internal and external to the organization, ahead of an incident is necessary for an effective, coordinated response.
- Committing to a multi-year exercise process with critical stakeholders creates a venue for training involved organizations to work together smoothly.

At two separate workshops, participants praised the value of their relationships with other groups – whether departments at their institution, third-party vendors, or homeland security partners. These relationships enhanced their ability to respond to the workshops' scenario and were deliberately built before any potential incidents that required cooperation on response efforts. Emergency managers especially stressed the usefulness of reaching out to the many departments within their own schools to cooperate on capabilities or to ensure all leaders were within a unified communications loop. Local police and government officials brought up multi-year, multi-stakeholder meetings to discuss or exercise preparedness plans with stakeholders in the community as another important best practice.

As emphasized by the first principle in the DHS slogan Connect, Plan, Train, Report – a part of effective Hometown Security – connections with the community can give colleges a wealth of capabilities when organizing incident response. These connections tend to be built on individual, informal relationships; however, to make sure they are maintained over the long term, participants need to effectively build them into organizational resilience processes. Attention should be given to codifying that organization as an important partner and maintaining a point of contact's information so that any new personnel can continue where a prior staff member left off. Having these procedures in place reduces the risk of a critical connection being lost due to a turnover. Such a partnership benefits all involved through the sharing of information, supplies, and assistance that can be integrated into the institution's response plans and accounted for to offset future security investments.

While a multi-year exercise program with external stakeholders can be a complicated initiative to begin, existing resources are available to help institutions that want to commit to this path. For instance, the DHS encourages any business or organization to connect, plan, train, and report to prepare for incidents as a part of developing hometown security and local partnerships. DHS's HSEEP guidance provides a set of guidelines for an institution to follow from beginning foundational efforts to continued execution of a fully matured program. A multi-year training and exercise plan can help align core capabilities and objectives development in a deliberate, progressive process and help partners work towards enhancing security and preparedness over a reasonable period of time.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; Risk Management for Protection Programs and Activities; Long-Term Vulnerability Reduction; and Operational Communications capabilities.

3.) Proactive Management of Protest Groups On-Campus

- An institution should create and follow a deliberate process for messaging protest groups in order to prevent violence.
- Administration-supported teams of university staff can act as liaisons to protest organizers, providing a conduit between protestors and the administration and law enforcement.

One of the participants in the workshop series represented a sporting venue that neighbored a host institution. Representatives emphasized the importance of managing protestors deliberately and

offered multiple best practices that they utilized with protestors that move between their property and the university's. In order to have better communications, the venue embeds a staff member with each organized protest and counter-protest group. The groups are informed that the staff member is there to ensure the group's safety as much as the safety of those attending the event that is being protested. Any safety and security guidance, such as outlining the safest areas to stand or the evacuation route in case of emergency, is communicated through this trusted staff member. This information includes any security updates issued by management. This staff member is trained to act appropriately with the group, always assuming they are on camera and representing the venue. Police representatives do not join the staff member unless a certain threshold of violence has been reached and the police on scene have taken over security.

During another workshop, an institution discussed their great success in formalizing the above maxims by creating what it calls "protest teams," a group of staff members who are trained to coordinate with and assist those planning and conducting protests on campus. Each team consists of representatives from multiple campus organizations, including housing, student affairs, and other key stakeholders, who are trained by the team captain in relevant university policies, de-escalation, and further critical techniques. The primary purpose of the protest team is to get involved with the protest group as early as possible and begin discussing both the group's goals and the school's protest policies and procedures, all with the intention of helping the protestors accomplish their mission in the safest manner possible. These teams do not exist in a vacuum and are a fully integrated component of the campus police department's protest response protocols. When there is no observed potential for violence, they are expected to be the institution's face at protests, with law enforcement standing by to support. Only if and when the potential for violence appears, does the police department take the lead to minimize risks to protest team members.

For an institution interested in a measured and deliberate escalation policy regarding protests, adopting the protest team concept can be a useful and effective component of that policy. They occupy an important middle ground between any informal contact the administration might have with a protest group and a formal police contact that might make some groups defensive. A formal protest team gives the institution a formal channel to educate, communicate, and coordinate with groups that could otherwise be potentially unreceptive to the campus police department. However, taking this step does require investment in training and equipping staff for the role. Liaisons will need skills to represent the university correctly and knowledge of the proper stakeholders to communicate with in case the protest group has questions or if an issue emerges.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; Intelligence and Information Sharing; and Threats and Hazards Identification capabilities.

4.) Full IT Support to the Emergency Operations Center

- The technical needs of a temporary Emergency Operations Center should be managed by a full IT team, similar to any established department.

One workshop participant noted an important lesson their institution learned: the need for providing full IT support to an emergency operations center (EOC) they stood up alongside government partners during their response to a potentially violent security event. The university treated the event similar to a significant IT project, with procurement money and hours set aside specifically for the EOC. The incident managers had a number they could call regarding any technical issue, and there were technical staff on-

site for IT emergencies. This redundancy was helpful at multiple points during the event, especially when diagnosing a sudden drop in bandwidth the EOC experienced at the eleventh hour as it began to process video streams from the campus and surrounding areas.

Providing full IT support to emergency response operations is one of the most fundamental ways IT departments can cooperate with their physical security and emergency management peers and bridge the cyber-physical security divide. Instituting this procedure does not require a university to add new capabilities. Instead, it can use existing capabilities and enhanced collaboration to better serve the campus. This is an approach that acknowledges each team's expertise in their respective areas and frees the other to do what they do best, all while confronting a quickly changing situation.

Core Capabilities: This observation speaks to the Operational Coordination; Cybersecurity; Risk Management for Protection Programs and Activities; and Operational Communications capabilities.

5.) Preauthorized Procurement Procedures in Place Before an Incident Occurs

- Preauthorization of funds to respond to an event gives incident responders more freedom and speed to procure what is needed to quickly solve the problem.

Sparked by a discussion of the Distributed Denial of Service (DDoS) attack introduced in one of the variants of Module 3, multiple workshop participants explained the plans their institutions have put into place to facilitate emergency purchases during a rapidly changing incident. One discussed approach involved utilizing emergency declarations issued by the President's office, giving the IT department the flexibility needed to procure any equipment or services necessary to respond to an incident. There should also be a representative from the business affairs division on every incident response team to ensure the division is aware of any changes in how responders are using their budgets.

Another tactic is to build procurement preauthorization into the disaster recovery plan. The IT disaster recovery plan sets tiers of response with corresponding, preauthorized procurement budgets. Any manager of an IT incident response group is authorized to declare an emergency and set the tier level. This method streamlines the procurement process and allows IT personnel to respond quickly with the necessary equipment and services.

To best support incident responders, institutions should plan ahead of time how to utilize their funds during a disaster. The ability to quickly allow access to funds without typical procurement restrictions gives staff the discretion to act quickly to reduce the impact of the emergency. In order to streamline procedures during an emergency, multiple stakeholders need to come together to explore available resources, determine the likely needs, and set proper procedures in place. The investment of time in planning and granting of procurement authority to IT managers will be repaid by the agility given to the response team to more rapidly reduce impacts to the organization.

Core Capabilities: This observation speaks to the Logistics and Supply Chain Management; Planning; and Cybersecurity capabilities.

6.) Contact with and Learning from Other Institutions with Experience

- Other institutions who have gone through similar events and challenges are valuable sources of information and generally open to assisting their peers.

As part of preparing for a major incident, multiple participants at one workshop promoted the idea of reaching out to sister institutions who have had prior experience with similar events. One of the universities present detailed its experience sending a team to a campus which had recently undergone a series of protests similar to what it was expecting to host in the near future. As part of this visit, staff members from the institution, including law enforcement representatives, sat down with their peers to discuss lessons learned and best practices they could take back and incorporate into their own response plans. There was significant value gained from both the information obtained and contacts developed during this visit.

As universities prepare for events that may strain their capabilities or experience, they should consider reaching out to other school administrations who have undergone similar events. It can be difficult to find the right contact for arranging a meeting, but information sharing organizations—including REN-ISAC, state fusion centers, and informal professional communities—are all good resources to begin that search. Once contacted, in many cases, these institutions are usually happy to pass along their knowledge and help support their peers, an action that enriches the security of the education sector as a whole.

Core Capabilities: This observation speaks to the Planning; Threats and Hazards Identification; and Situational Assessment capabilities.

7.) Memorandums of Understanding to Defer Cyber Risk

- Memorandums of understanding uniting groups of institutions managing cyber risk can rapidly allow incident responders to bring in additional resources from other institutions during major incidents.

At multiple workshops, participants mentioned their organization's use of memorandums of understanding (MOU) to help manage and defer cyber risks during serious security incidents, whether those incidents were denial of service attacks or observed data exfiltration attempts. These MOUs give participants' institutions the ability to rapidly call upon other universities' security operations personnel, network bandwidth, or other cybersecurity capabilities as necessary and allow the school to be more efficient with its resources while effectively planning and managing surge capabilities without incurring exorbitant costs. For example, an institution can depend on other schools to provide remote staffing as its IT department surges to respond and recover rather than having to pay for a large number of cybersecurity personnel during a complex cyber incident. Once the event is over, personnel are returned to their host institution and operations revert to a steady state.

The creation of a useful MOU requires careful thought by those involved. The document represents an investment of time and commitment; signatories agree to it before a disaster is in order to foster a quicker and more comprehensive response when a disaster occurs. A university exploring an MOU should first consider the vulnerabilities their organization faces. Next, they must consider if they have the resources to mitigate the disaster if these vulnerabilities are exploited. Acquiring the resources it lacks should be prioritized as the organization begins the MOU negotiation process, determining which resources it can provide to other signatories. While MOUs are typically signed after a long negotiation between two or more schools, there have also been efforts towards establishing a standardized, national-level MOU to help lower the threshold of entry for institutions with less resources to dedicate to this process.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; Cybersecurity; Risk Management for Protection Programs and Activities; and Long Term Vulnerability Reduction capabilities.

8.) Fusion Center Integration with the Education Sector

- Maintaining a strong relationship within a trusted local information sharing organization builds communities to counter larger threats.

When discussing how to become aware of the threats raised in the workshop's scenario, one workshop participant noted how important it is for university campuses to invest the time and resources in building an integrated relationship with their local fusion center or other state or local government information sharing organization. The institutions participating in that workshop displayed a high level of trust in their local fusion center due to a history of timely intelligence and joint cooperation. Information sharing organizations come to depend on this trust as they form the core of a preparedness-focused community that institutions can use to coordinate against regional threats. Not all regions of the country have strong ties to their local intelligence sharing organization, and without this relationship, it becomes difficult for the information sharing entity to reach out to the research and education community. Outreach and education from both information sharing organizations and satisfied customers is necessary to counter this trend.

Core Capabilities: This observation speaks to the Public Information and Warning; Information Sharing; Cybersecurity; and Threats and Hazards Identification capabilities.

9.) Incident Response Staff Rotation

- Command center staff should be managed appropriately during long-term incident response in order to prevent burnout and other consequences.

When discussing how to manage the protestors wounded by the improvised explosive device attack introduced in one of the variants of Module 5 of the scenario, workshop participants noted the importance of managing the sudden surge of incident responders that would result. In the immediate aftermath of the attack, responders will be required to fully treat the wounded, manage the evacuation of the campus, process a crowded crime scene, and other tasks, all of which need to be supported by IT. Additional personnel will be needed for longer than the expected during the heightened activity of the event. Often a large number of command center staff and first responders will show up immediately as news of the attack filters out to the community. If an incident lasts several days, assigning personnel to shifts and rotating them out regularly ensures there is no initial surplus of personnel or risk of overwork during the critical first few days after a deadly event.

It is vital to avoid wasting resources when handling an event that has created or extended a period of heightened activity, especially when an incident command center is part of the response. Procedures should be able to absorb new personnel into existing command structures. Managers should know how many additional bodies they can accommodate, so the rest can be sent home for the next shift. Institutions need to be ready for the consequences of this surge in attention and should plan appropriately.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; Risk Management for Protection Programs and Activities; On-Scene Security, Protection, and Law Enforcement; and Situational Assessment capabilities.

10.) Event Coordinator as Primary Security Coordinator

- The institution's event planner is in the best position to serve as primary security coordinator for controversial speaking events.

One workshop came to the consensus that the best position to coordinate the security response to a controversial speaking event appears to be the school's event coordinator. This role is in the best position to understand all that is occurring in relation to the event. For some schools, this may already be a role the event coordinator is assigned. For other schools, it may be a new set of duties given only if they are targeted by a controversial speaker event. It allows for security to be planned into the speech from the beginning and many government agencies are turning to event coordinators first if a school asks for preparedness assistance.

Core Capabilities: This observation speaks to the Planning and Operational Coordination capabilities.

11.) Resilience Provided by Redundant Communications Methods

- Having multiple communications methods and fallbacks provides a significant amount of resilience during a natural disaster or other large emergency.

When listing the priorities of IT departments during a recent natural disaster, maintaining communications was often mentioned as the highest priority. No matter what school, the administration had to get its message out to multiple audiences. Participants observed that their institution's use of redundant communications methods allowed them to maintain communications over the course of the storm and its aftermath. Voice-Over-IP, cellular service, landline phones, the schools' websites, and social media were all mentioned as common methods IT staff helped to keep up. Some of these systems failed for some, though it was different for each participating school. In some areas, older technology failed. In other areas, newer technology failed. Furthermore, many schools had backup options for each of these communications methods, such as failing over to a mirrored emergency management web page during spikes of traffic or the use of micro cellphone towers. Some schools used programs available to emergency responders to build out this robustness, such as the Government Emergency Telecommunication Service (GETS) or Wireless Priority Service (WPS) managed by the Department of Homeland Security (DHS). These programs allow for calls into affected areas to be prioritized by communications companies, a critical asset for campuses with hospitals or other branches assisting in emergency response efforts.

Layering communications methods allows a university to be confident that it can get its message out in a timely manner, whether that is information about the campus's current status or emergency tips for students. Institutions should consider both the number of methods currently used in their organizations and the number of backup systems and procedures in place for each of those methods. Investing resources to increase the number of both methods and back-up systems strengthens the administration's position to control its response when a catastrophic disaster occurs.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; and Operational Communications capabilities.

12.) Third-Parties to Enhance Communications Capacity During and After Critical Incidents (2)

- Third-party services can handle network traffic surges due to a rapid increase in searches for more information on well-publicized incidents, thus mitigating network degradation and possible disruption of service due to increased traffic.

When discussing the violent events introduced in Module 5 of the scenario, one university participating in the workshop series shared a challenge it experienced in the immediate aftermath of a similar event that occurred near its campus. Once the violent event was reported in the media, the university's webpage suddenly experienced a large increase in traffic as interested parties, such as parents searching for news about their children and local media outlets looking for information, navigated to the site. The surge in traffic was enough to take the site offline entirely, causing, in effect, an unintended distributed denial of service incident. Once it realized the risk, the school took steps to reduce the chance of a similar shutdown happening in the future, but that workshop's participants noted that this was a common pattern after tragedies or other newsworthy events and the risk should be prepared for.

At another workshop, multiple participating institutions highlighted their successful use of third-party call centers and internet providers to handle increased volume during past well-publicized events. They emphasized how important it was that their universities had such services on retainer before the incidents happened, commenting that otherwise it would have been difficult to arrange assistance once the service-denying levels of traffic occurred.

One of the important items noted with regards to third-party call centers was the niche they occupy. These centers work best when given a prewritten script and answers. This means the best use of their time is providing the school's statement, receiving information in the aftermath of a chaotic situation, and preventing a busy signal during a spike in attention.

Integrating third-party companies into an institution's response plan gives an institution the flexibility to sustain service capacity under the rare conditions that occur during and after major incidents on or near campus. However, prior research and preparation is necessary to properly obtain this capability. Contracts need to be negotiated and signed, while both IT and emergency management departments have to discuss how to integrate a new service during emergencies and exercise alongside the contractors.

Core Capabilities: This observation speaks to the Planning; Cybersecurity; and Intelligence and Information Sharing capabilities.

13.) Mutual Awareness of Scheduled Events

- Regularly sending a list of university-hosted events to the local police department allows the department to be aware of potential security issues ahead of time.
- For events, providing first responder agencies a map of the facility where events are to be hosted helps potential responders prepare for a timely response in the event of an emergency.

One suggestion offered by a local police department during a workshop was a best practice it observed from other entertainment venues in the community. On a scheduled basis, other venues will send the police department a list of all upcoming events they are hosting. These lists can be consolidated and shared back with local security organizations. At the most basic level, these lists are similar to a public calendar that would be sent out to a venue's mailing list. However, what the department highlighted as

being especially helpful was certain venues attached maps of the rooms where each event would be held. This information is then forwarded to the department's SWAT team and bomb squad to use, either in determining if there is a potential threat to the venue beforehand, which could result in further joint planning, or to have on hand as the team prepares to respond in case of an emergency.

Institutions should consider having this discussion with the local police department and other first responders. In the middle of a violent event, such as a hostage situation or mass shooting, there are certain pieces of information that responders would find useful to know beforehand. Learning this information and coming to an agreement on providing it on a regular basis helps both organizations learn more about each other's security requirements and makes it easier to work together when planning for a significant security event.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; and Intelligence and Information Sharing capabilities.

Areas of Improvement

Areas of Improvement are defined as opportunities for stakeholders to possibly enhance their security posture.

1.) Exercising and Validating Plans

- Establishing and practicing a consistent exercise program, especially before planned events, validates plans and refamiliarizes employees with the processes necessary to execute the emergency plans set out by leadership.
- Performing a consistent review of information sharing agreements should be included as part of these exercise programs.

While almost every participant of each individual workshop generally knew of the existence of incident response plans within their organization, there was less uniformity in terms of knowing how often and how thoroughly those procedures were exercised. Some institutions had a schedule of exercises planned throughout the year while other institutions executed training in a less consistent manner. These exercises were often at the team or departmental level, rather than involving the university as a whole. Some participants' IT departments had formal or informal procedures in place to trigger an exercise after a major crisis. Overall, while some exercising and training occurs in participants' schools, it is not at the consistent level of an effective program.

Regularly exercising and validating emergency procedures and plans allows institutions to ensure that those plans reflect the current realities that inform them. This can include details such as the risk assumptions the plan is based on, changes in technology (including software and hardware), or a lack of critical supplies. While crafting the plan initially is a vital step, deliberate preparedness including scheduled plans reviews, training and exercises are critical parts of an effective preparedness cycle and help ensure viable plans and procedures are up to date with evolving threats, and institutional structure and staff changes. In addition to validating plans, exercises provide an opportunity for staff to practice procedures and improve their ability to respond to incidents. A best practice is to consider the development of a multi-year training and exercise program that allows time and resources to be scheduled to ensure all desired areas are addressed over an acceptable period of time.

There are resources to help universities start up a structured exercise program. DHS Protective Security Advisors and FEMA Regional NIMS Coordinators are federal representatives serving as subject matter experts capable of advising or assisting American institutions with improving their physical and cyber security posture. At the state level, both fusion centers and National Guard units are available to help lead or assist with various types of exercises. For universities that don't have connections with these organizations, REN-ISAC can serve as an advocate to build that relationship and as a clearinghouse of information on additional resources to build exercise programs and other emergency preparedness activities.

Another critical observation that came up during one workshop was the importance of giving staff the time to refamiliarize themselves with relevant procedures and agreements when preparing to execute an event with a more significant scope. Almost all schools have a written procedure for how an event is executed, from the first submission of interest to the day of the event itself. There are often methods of escalating the attention administrators should give an event and the committees, such as emergency management or student events, that can become involved. Often, this is the point where staff from

departments not directly responsible for events become involved and can provide information or feedback, as necessary. Reviewing these procedures keeps personnel aware of the ways they can participate in this process.

Some institutions also have information sharing agreements with other universities, government agencies, or third party organizations such as REN-ISAC. Just like incident response plans, these agreements need to be reviewed and updated to validate their effectiveness. Reviewing these agreements also allows personnel to refamiliarize themselves with how to properly participate in that information sharing process. Organizations that engage in information sharing define what information or data should be shared, the method of sharing it, and the level of access other entities will have to the information, along with many other components. Unlike emergency procedures, information sharing is a constant process that requires consistent engagement by staff, so an organization should check both how it should be sharing information and whether it is currently sharing information appropriately. Furthermore, as discussed with attendees during the workshop, organizations may be unaware of the level of protection that an information sharing agreement provides. Getting comfortable with these details can allow an institution to more confidently become involved in the information sharing environment.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; and Intelligence and Information Sharing capabilities.

2.) Conducting Institution-Wide After-Action Reviews in the Aftermath of Major Incidents

- Commitment by leadership is necessary to ensure proper after action reviews are conducted in the wake of a large event.

One workshop was the first time many stakeholders involved in a recent major event at a participating institution's campus were brought back together. The group observed the difficulty of finding and scheduling the time to conduct post-event/post-incident after-action reviews. Bringing together stakeholders from multiple divisions of the university allowed participants to get a better picture of the full operation and what issues and concerns other sections had to face, resulting in improvements to better manage future events. However, differing schedules and other concerns create obstacles to reconvening experts, conducting a full post-incident analysis, and implementing lessons learned.

Administrations should consider putting policies and procedures in place to ensure time is set aside after declared emergencies and other significant events to ensure institution-wide after-action reviews are conducted in a timely manner. After an incident, attention can become unfocused as those who responded return to their steady-state routine and face potential backlogs of work due to concentrating on incident response. It is up to leadership to provide the space for staff to discuss the emergency as a learning experience and to extract lessons to help future efforts.

Core Capabilities: This observation speaks to the Planning and Intelligence and Information Sharing capabilities.

3.) Determining Thresholds for Cutting Off Critical Network Resources

- Institutions should decide ahead of an emergency their thresholds for removing important IT components from the network, including up to the point of cutting the organization off from the internet itself.

When discussing approaches to mitigating denial of service attacks, participants at one workshop discussed their institutions' thresholds – if any - for cutting off critical network resources. It was agreed that taking any vital network resource offline during an incident had to be done through a deliberate process that had been approved by all involved stakeholders before any emergency occurred. One participating institution described how, even after correctly executing its playbook during a real-life incident, there were some issues that came up due to having not tested the written process beforehand and not having the relationships with other departments to course-correct in the middle of the incident. The university emphasized that this deliberate process is important because the consequences of taking such drastic measures for the first time during an emergency could become more harmful than the emergency itself.

There are three components to this process: uncovering implications, deciding thresholds, and assigning authority. First, all stakeholders within an organization should be brought together to gain a full understanding of what departments would be impacted by losing a critical network resource and how significant those impacts would be. This can be achieved via planning and coordination meetings, existing security forums, or planning workshops. Second, IT staff should know what thresholds should be passed before it is acceptable to implement the discussed action. These requirements should be discussed and agreed upon among all stakeholders, so there is a level of comfort when rapid action has to occur. Finally, once the thresholds are known, the authority to order that action should be assigned to the most appropriate position in the organization.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; and Cybersecurity capabilities.

4.) Identification and Protection of Critical Facilities

- Protecting critical campus infrastructure from protestors requires inventorying critical facilities, identifying the most vital buildings, and strengthening access controls to best secure them during an emergency.

Participants at multiple workshops brought up concerns and solutions regarding physical access to important components of cyber and physical infrastructure on campus. Due to differences in culture between facilities professionals and IT professionals, it can be difficult to cooperate in order to mitigate these issues. Some of the participating institutions combined infrastructure security into long-term processes, such as business continuity requirements containing checklists that help identify high-value or high-risk assets that may need extra protection during a major event. Other schools included preparedness efforts during event planning processes, such as establishing that law enforcement would conduct security assessments at nearby venues. However, the majority of schools present at the workshops did not have methods to identify critical assets and even fewer schools had the ability to quickly identify them in case of a rapidly developing emergency like expanded protests.

At one workshop, a participating institution's IT department discussed how it had gone through the process of locating and recording every piece of IT infrastructure on campus. This inventory became a useful resource for cyber security professionals, but other participants, specifically facilities and physical security professionals, suggested that tracking additional metrics for each piece of infrastructure—such as the criticality value of the asset to daily operations and a priority list of the most vulnerable assets to physical access—would make the inventory more valuable. This type of information can help emergency management departments better understand what to secure using its limited resources; however, as

some participants noted, not all of the university's departments present at that workshop were aware of this inventory despite the potential to use this resource to improve campus-wide response efforts.

Identifying facilities critical to the school's operations and hardening them against illegal access reduces the risk of sabotage from protestors, activists, or other actors who might threaten an institution. Since it takes a significant investment of time to prioritize assets and apply corrective measures to improve their security, this is a project that institutions should execute on a continuous basis, rather than during the run-up to a major event. There are always new pieces of data that could be gathered to refine an institution's emergency response plans and strengthen the administration's security posture. A representative selection of stakeholders is necessary to achieve insight into both the critical facilities that exist and what types of data could best inform the university's plans to protect these facilities.

Core Capabilities: This observation speaks to the Planning; Intelligence and Information Sharing; Access Control and Identity Verification; Physical Protective Measures; and Infrastructure Systems capabilities.

5.) Increasing IT Security's Involvement in the Response to Physical Incidents

- The integration of physical and cybersecurity professionals within an organization creates an environment for more robust preparation efforts and a more cohesive response during emergencies.
- The response to physical security incidents, such as protests or violent crime, can be enhanced by the permanent inclusion of IT personnel in the response team.

At several workshops, IT and computer security professionals asked law enforcement and emergency management professionals a significant question: "How can we support your mission better?" Many of these professionals felt that, if they had a better understanding of the physical security personnel and officer's capabilities and needs, there were ways their technical expertise could be applied to the problems that these departments faced. Their counterparts were receptive to this question and there were many discussions on the value of having universities bring the two disciplines together for more deliberate discussions addressing potential IT support capabilities.

One institution spoke to how, until recently, its incident response team did not have the proper level of cyber-specific participation at the table. This resulted in a process that was not well-informed by the technical considerations, limiting response options. Including the Chief Information Security Officer on the team brought new benefits: enhanced information and the potential to build additional capabilities. Being involved in the incident response process from the beginning gives analysts space to search for network changes that could be occurring due to an upcoming physical event, such as the hacktivist reconnaissance after the controversial speaker announcement seen in one of the variants of Module Three of the workshop scenario. Once the IT department is experienced with the physical security response process, it is also in a strong position to provide new and unique capabilities to its physical-security partners.

Breakout sessions were scheduled at some of the workshops for participants to discuss the benefits and capabilities that IT departments could offer to physical emergency responders if they were included in a more holistic manner. Suggestions included creating methods to track suspects and victims involved in the on-campus bombing introduced in a variant of Module Five, such as tracking media access control addresses or enhanced logging of targeted university websites for campus and local police, streamlining crisis team communications through apps for tracking crowd density based on network activity, and

listing commercial software options previously unknown to physical security professionals. The results from the discussion demonstrated there is abundant opportunity for physical and cybersecurity professional to improve each other's operations through enhanced integration, collaboration, and education.

Core Capabilities: This observation speaks to the Planning; Operational Coordination; Intelligence and Information Sharing; Cybersecurity; Long-Term Vulnerability Reduction; Threats and Hazards Identification; Operational Communication; and Situational Assessment capabilities.

6.) Streamlining Emergency Responders' Access to Internal Campus Resources

- IT departments find it difficult to quickly credential outside responders without advance preparation.

Determining how to swiftly give first responders arriving on campus access to on-campus resources was a theme at multiple workshops. One participating IT department discussed the difficulty of integrating off-campus emergency responders with internal university resources. They explained the recent challenges their university's IT department encountered when attempting to grant a local fire department access to an internal hazardous materials storage tracking website maintained by campus staff. As it was an internal website, they had to determine how to assign campus accounts to firefighters for that single purpose. In addition, unlike university administrators, firefighters needed to access the website on mobile phones for which the site was not configured. At another workshop, a participating institution noted prior difficulties in adding local, state, and federal responders to the emergency management resources it uses for large events. During a past major event, the university discovered that the process to give responders access to wireless networks, software, and analytic tools was overly time consuming and tied up IT personnel that could have been better used elsewhere. This was partly due to the sudden nature of the event and subsequent protests. Not all law enforcement officers present on campus were able to get access before being deployed.

Many universities maintain internal resources that would be valuable for emergency responders to have access to when they report to incidents occurring on that institution's campus. These resources can provide critical information or enhance existing capabilities during especially dangerous events, allowing responders to do their jobs more effectively. However, these services are typically created with the assumption that only on-campus personnel will want permission to use them and are often managed in a decentralized manner, making it difficult to maintain full awareness of what exists. Departments in charge of administrating such resources should explore ways to quickly provide these network resources to first responders in case of an emergency. In addition, university staff should consider proactively reaching out to local police, fire, and emergency services agencies to discover what sorts of resources they might find most useful. Doing this groundwork before a major incident can save significant amounts of time during the incident response process and allows responders to do their jobs better.

In order to reduce inefficiencies in the runup to major events, universities should consider creating the capability to easily add local partners to their emergency management platforms on an as-needed basis. This is can be done through federating network systems with the organizations the university will draw upon during crises. Emergency management, campus law enforcement, and the IT departments can help prioritize the most likely partners the campus will need. This is key, as the federation process can be intensive as organizations work together to become interoperable at the IT level. However, the

payoff comes with the capability to quickly give credentials to outside personnel in the leadup to large events, saving time and effort for everyone involved.

Core Capabilities: This observation speaks to the Operational Coordination; Intelligence and Information Sharing; Access Control and Identify Verification; Operational Communication; and Situational Assessment capabilities.

7.) Providing Cyber Defenders with a Broader Threat Context

- Cyber defenders often do not have access to the information sources or the training to understand both the broader issues and the broader threat environment that gives context to IT security priorities.

During a discussion on the hacktivist network reconnaissance in a variant of Module 3, participants of one session noted the challenge that cyber defenders have in understanding and reacting to the changing global cyber threat context that might increase the risk of such an attack against their school. They observed that, while cybersecurity professionals are highly experienced in their areas of responsibility, other areas of the organization and the local environment impact how they do their work. Non-cyber events increase threats to the campus network, whether it is a campus professor publicly signing a controversial letter or an activist group announcing a boycott that includes the university. A mature cybersecurity team understands and responds to this larger threat environment, particularly in the increasingly complex and blended threat environment in which higher education is operating.

The benefits of this maturation are a faster and more thorough response to threats. Potential threats come to the attention of a well-developed security department sooner and with more detail. It is this detail that allows for a more deliberate and robust set of mitigations to be put in place. When the department better understands the nature of the threat and threat group targeting an institution's network, a more informed assessment of actual risk can be made, and appropriate mitigations can be put into place that are tailored to the known tactics, techniques, and protocols used by the threat.

Core Capabilities: This observation speaks to the Intelligence and Information Sharing; Screening, Search, and Detection; Cybersecurity; and Situational Assessment capabilities.

8.) Using Social Media and Email Monitoring to Improve Awareness, Planning, and Response

- Social media and email can be a useful source of intelligence both when making response plans and when responding to an incident.

A trend in the discussion at one of the workshops revolved around how to best monitor social media and student email to help inform preparedness efforts. While there was interest in the topic, no participant felt they had a cohesive approach. Many schools have the capability to monitor the most popular social media sites, especially Twitter, along with emails sent from campus affiliated addresses. However, the availability of and access to this software varies on the departmental level, rather than being available across the entire administration. Information silos are a common occurrence. One participant described how their IT department was using social media monitoring to track campus robberies without realizing their police department had feeds that could be combined with theirs to reduce redundancies.

Properly integrating and utilizing monitoring capabilities has the potential to give institutions the information necessary to best become aware of, plan for, and respond to all the threats a campus faces.

Social media can serve as an excellent source of intelligence on what is occurring on and around campus, whether it is planned gatherings, common crimes, or situations of concern. Once analyzed, it can inform plans, policies, or procedures that an administration is developing, as well as being immediately available to first responders focused on protecting life and promoting safety. In comparison, email monitoring can be a powerful tool, but one that requires being deployed in a more limited fashion. Most participants' experience involved technology that searched for keywords in student email only after they were alerted of a threat through other means, such as public social media.

Core Capabilities: This observation speaks to the Planning; Intelligence and Information Sharing; Threats and Hazards Identification; and Situational Assessment capabilities.

9.) REN-ISAC Providing Social Media Awareness Resources

- REN-ISAC could provide assistance or even open-source code to help stand up a social media monitoring capability to institutions with limited resources.

An idea discussed during one workshop was that, for university IT teams with limited resources or bandwidth, REN-ISAC could serve as a potential clearinghouse of social media awareness resources, such as white papers or ready-made code that provides a minimum level of social media monitoring capability. For many smaller security teams, building out a social media awareness capability is not a high-level priority in the face of the numerous responsibilities they have and the large amount of network activity they have to respond to. Acquiring an off-the-shelf social media awareness capability can reduce a team's time investment but at a significant cost to their budget, while building the capability in-house skews the tradeoffs in the opposite direction. REN-ISAC could serve as a compromise between these two options by assisting these teams and providing resources to reduce the amount of bandwidth a small IT team needs to begin observing social media for potential threats.

Also noted during the workshop was how the state fusion center provided various useful resources to college campuses. REN-ISAC's pre-existing partnerships with similar organizations, in addition to law enforcement agencies and DHS, create another useful avenue for the wider higher education community. These connections allow REN-ISAC to have a broad conversation with all relevant stakeholders about who is doing what in the area of social media monitoring and how their capabilities can be best shared and integrated to the benefit of the higher education community. The ensuing collaboration between stakeholders can create a network that universities can easily tap into as they begin to build out a social media awareness capability.

Core Capabilities: This observation speaks to the Intelligence and Information Sharing; Screening, Search, and Detection; Community Resilience; and Long-Term Vulnerability Reduction capabilities.

10.) Connecting to Broader Security and Emergency Management Organizations

- Many campus security focused organizations have resources to help schools determine an approach to a wide selection of emergency management topics.

A strong theme observed during one of the workshops was participants' clear desire to reach out to larger security and emergency management organizations in order to improve their institution's security posture. Representatives from both the state's Department of Justice and fusion center were present to educate attendees about the information sharing environment locally, while REN-ISAC spoke to the environment on a national level. Despite participants' interest, many universities, especially IT

departments, only build these sorts of connections on an ad hoc basis. REN-ISAC discussed how it could contribute to schools' efforts in this niche, serving as a clearinghouse of information and assistance to help higher education more easily connect with these larger, more focused organizations.

As emphasized by the first principle in the DHS slogan Connect, Plan, Train, Report, connecting to security organizations specialized in understanding the threat environment of a sector, region, or state gives colleges access to a wealth of information—information that allows them to create better security plans in the short term and make smarter security investments in the long term. Local, state, and federal organizations are available to provide free assistance to universities confronting complex security events. These organizations can provide analysts capable of contextualizing threat information and help share knowledge between fellow stakeholders, such as best practices or lessons learned from prior experiences.

Core Capabilities: This observation speaks to the Intelligence and Information Sharing; Public Information and Warning; Threats and Hazards Identification; and Situational Assessment capabilities.

11.) Requesting Threat Assessments from Local Law Enforcement

- Local and state police departments typically offer threat assessments for organizations on request at no cost, which provides a good foundation for campuses with limited resources to begin managing their security posture.

When discussing how schools with limited resources and bandwidth can still improve their security posture, law enforcement attendees at one workshop promoted the idea of universities reaching out to local and state law enforcement agencies to request a no-cost threat assessment of their campus. These programs typically bring a trained officer or analyst out to the facility who will work with staff on identifying and mitigating any vulnerabilities. In addition, this person can serve both as a liaison who can connect the school with other agencies and resources available in its region and as a subject matter expert capable of providing an up-to-date view on the threats and vulnerabilities that an institution should prioritize as it strengthens its security program. Over time, one threat assessment can turn into a continuous program that helps strengthen ties between the campus and local law enforcement.

Core Capabilities: This observation speaks to the Physical Protective Measures; Community Resilience; Long-Term Vulnerability Reduction; Risk and Disaster Resilience Assessment; and Threats and Hazards Assessment capabilities.

12.) Improving the Process to Provide Law Enforcement with Pertinent Evidence after Violent Events

- Discussions with local law enforcement before an event can ensure potential evidence from campus data sources will be appropriately processed after a major incident.

When answering questions about how to properly wrap-up after a violent protest, one important topic at one workshop was determining how to ensure that law enforcement receives any relevant evidence produced or collected by the university, with a specific focus on video and audio retrieved from security cameras. While participating law enforcement explained how some police body camera providers offer "citizens portals" for third parties to upload potential evidence in a legal and secure manner, there are not many solutions that exist to help universities effectively address this challenge. Participating IT departments felt that it is possible to build an IT solution to this issue, but all attendees emphasized that

proper coordination with legal stakeholders would be key to ensuring any system is useful for local, state, and national law enforcement.

Security cameras create large volumes of data for security experts to analyze after events involving the movement of large groups of people, especially once arrests are made. When law enforcement is involved in this procedure, determining how to properly transmit this data into their custody becomes an important subject. Universities should consider taking the time to have this discussion between facility management, IT, legal stakeholders, and local police so that a process can be in place before a significant incident occurs. Having this capability gives law enforcement the ability to determine misconduct and secure evidence more quickly and gives institutions the ability to cooperate with authorities more efficiently.

Core Capabilities: This observation speaks to the Planning and Forensics and Attribution capabilities.

13.) Involving Students in the Emergency Response Process

- Student feedback and insight can be incorporated into the administration's response process at multiple points in order to create plans that better meet the needs of the campus population.

Participants at one workshop felt that there were places where students could help improve their school's overall emergency response process, especially when it comes to a controversial speaker like the one presented in the scenario. Universities have differing levels of involvement with their student population, but every participant had an institutionalized connection that they could leverage for various tasks. However, this connection is not always well-integrated into the emergency management process. With regards to the scenario, some institutions expected students to reach out to the administration in an informal manner with any concerns or intelligence on the planned demonstrations during the day of the speech, while others expect certain departments, typically student affairs, to conduct that sort of investigation. There is often no proper process in place, or most personnel are unaware of the details of the process.

A strong connection with the student body opens up new options for emergency preparedness and response personnel. At the most basic level, utilizing that connection to educate students on various preparedness topics, from natural disasters to campus power or internet outages, increases the overall population's resilience when such events occur. One participant discussed how their institution provides tours of the campus data center in order to demonstrate the importance of such infrastructure. Other participants focused on how they have used these connections as both a moderating influence and a source of intelligence on student protests and other disturbances. The administration can learn about potential events earlier and prepare for them, while maintaining a dialogue about what lines students should not cross. One participant recounted how this approach works for cyber events as well after discovering the cause behind a DDoS attack on the campus network was due to an escalated feud between gamers, one of which was living in the dorms.

Core Capabilities: This observation speaks to the Planning; Public Information and Warning; Intelligence and Information Sharing; Community Resilience; Threats and Hazards Identification; and Situational Assessment capabilities.

14.) Identifying and Communicating Organizational Information Requirements

- A clearly identified method to discover, update, and communicate information requirements to all participants is necessary to keep the security stakeholders at all divisions of the university aware of what each other needs to make critical decisions.

A critical observation at one workshop was that participants were sometimes not aware of the types of information that other stakeholders in their organization needed to make critical security decisions. Furthermore, once learning this, those formerly unaware attendees were often willing to gather and provide that information to their security partners. Institutions confronting complex security events should consider discussing, defining, and sharing mission critical information requirements and deadlines for each of the departments and with appropriate partners and suppliers involved in the process in order to strengthen their security posture. Engaging in this process before major events allows every department and partner involved to fill in previously undiscovered gaps and increase dialog between the most relevant stakeholders.

Beyond the identification of information requirements, workshop participants noted the desire for a method to identify these security information requirements across the whole organization on a continuous basis and distribute them to the rest of the organization. This is an area of opportunity where schools can create a set of procedures to maintain and communicate a unified understanding. A planning workshop is one way organizations can begin the process to discuss and capture such requirements. Leaders at institutions might consider the benefits of consistently thinking about both the information they need to make the security decisions they are responsible for and the personnel they would like to be in communication with to receive that information.

Capabilities: This observation speaks to the Planning; Operational Coordination; and Intelligence and Information Sharing capabilities.

15.) Reducing Alert Fatigue

- Properly managing the flood of information shared among organizations allows cyber and physical security professionals to focus on the most critical items.

When discussing the thresholds necessary for an institution to focus on responding to a specific security threat, participants at one workshop noted the constant risk of falling into alert fatigue. Both physical security focused and cybersecurity focused practitioners warned how constantly receiving warnings and alerts can lead to decreased awareness of true threats, though cyber-focused participants observed that alert fatigue is the default state of their profession due to how complex IT has become. Alert fatigue can occur for procedural reasons, such as not having the right policies and capabilities to sort large volumes of data from an information sharing agreement, or technical reasons, such as managing automated alerts while defending a large and complex IT infrastructure. Security professionals can be overwhelmed by data, and important alerts can be lost in the noise.

For organizations receiving information, managing alert fatigue requires setting institutional information requirements and the proper curation of information. Knowing what threats are prioritized by leadership is a valuable sorting tool for analysts. Similarly, building the capability to properly label, sort, and study data saves analysts time and allows them to provide better results. For organizations disseminating information, proper context needs to be given along with the data so that those receiving it have actionable steps they can take in response. Context also allows the receiver to better rank how

applicable the threat is to their circumstances. In addition, knowing the recipient's information priorities can cut down on gathering and sending information that won't be utilized at the end point.

Core Capabilities: This observation speaks to the Public Information and Warning; Intelligence and Information Sharing; Situational Assessment; and Cybersecurity capabilities.

16.) Cost of Security

- Events featuring controversial speakers tend to have significantly increased security and, therefore, significantly increased security costs.
- There are many financial, organizational, and legal uncertainties regarding what parties are responsible for paying those costs.

A persistent concern brought up throughout one workshop was how to approximate cost and appropriately fund the security required to host a controversial speaker on campus while keeping the student population safe and secure. Institutions have experienced legally imposed restraints on cost-saving measures, such as cancelling events due to excessive costs or shifting the financial burden onto the organization requesting the space. The workshop discussion did not delve into the reasons for this and instead focused on the effects of this uncertain environment. Schools do not currently have a metric by which to consistently set prices for events based off of the security requirements they will entail.

In order to better understand this issue, it was suggested that many schools would like to learn what the common considerations are that other schools face when appropriating funds for these events and if those schools have had any leeway in variable charges based on the risk profile of different groups. This is an area where bringing together data and experience from institutions that have gone through these types of security events could bring large benefits. Having these targeted institutions go through a facilitated process can result in thoughtful discussion and, eventually, guidance for the higher education community as a whole.

Capabilities: This observation speaks to the Planning; Risk and Disaster Resilience Assessment; and Threats and Hazards Identification capabilities.

17.) Reducing Duplication of Effort

- Departments within both the university and community security partners duplicate certain actions when preparing for the same security event.
- Discovering duplications and streamlining actions should create an improved planning process.

When discussing gathering threat information before the controversial speaking event in the scenario, one workshop discovered that institutions often duplicate actions across departments that could be streamlined and enhanced through cooperation, especially in instances of analyzing the threat environment. With events staff, local police, campus police, and government agencies all conducting separate threat assessments of the speaker's prior events, this process could be streamlined and enhanced through cooperation. In addition, some departments utilized robust tools that the wider community did not know about. These departments noted they were willing to share with other stakeholders in order to improve those stakeholders' outcomes.

Addressing duplication of effort has potential benefits, both within an institution and within the broader security community surrounding the campus. Within the school, departments should consider hosting frank, open, and consistent dialogue about what actions they are undertaking to respond to a significant

security event. Together, units can eliminate redundancies and integrate preexisting efforts or tools. Approaching the problem this way has the added benefit of clearly defining responsibilities and capabilities, so an institution can utilize them again for future events. Within the broader security community, efforts to reduce duplication builds ties with the partners that are necessary to maintain the physical and cyber security of the campus. A common operating picture of the security environment these organizations are operating within can be developed, allowing everyone involved to better understand their duties and roles when a significant security event or challenge occurs.

Capabilities: This observation speaks to the Planning and Operational Coordination capabilities.

18.) Reluctance to Share Information about Cyber-Attacks

- Many institutions have an unwillingness to share information on attacks targeting themselves with the broader education sector.

When discussing how an institution's response to a widespread cyber campaign might change whether or not it was the first organization to be targeted, participants at one workshop highlighted the general reluctance most organizations have with regards to sharing any information pertaining to a significant cyber-attack against their network. If such information is released, it is usually significantly delayed and, therefore, out of date, making it impractical for network defenders to use. It was acknowledged that in some cases, there are important legal considerations that may restrict or prohibit the ability to share 100% of the details surrounding an attack with external organizations; however, participants felt there were targeted approaches where the most critical facts could be distributed to boost the education community's resilience without major drawbacks.

Participants also felt that, while the education community as a whole is slowly getting better about sharing, there are still significant gaps of trust between stakeholders. Reputational damage is a major concern and steps must be taken to alleviate any risk of it occurring when an institution decides to share actionable information about any attacks itself suffered. Third-party information sharing organizations, such as REN-ISAC, can be a useful place to get data anonymized before sending it to a wider community. The effectiveness of this method depends on the trust and reputation surrounding the third-party organization, which is built over time.

Core Capabilities: This observation speaks to the Intelligence and Information Sharing and Cybersecurity capabilities.

Challenges

Challenges are defined as inherent issues that, in today's threat environment, are unable to be truly eliminated, just mitigated.

1.) Protests May Occur Regardless of Controversial Event Approval

- If an event is controversial enough, similar, or worse, levels of protest may occur whether a university approves or denies the original event.

When discussing the event approval processes used by institutions, workshop participants noted that both higher education institutions are often caught in a "Catch-22" when confronted by a controversial speaker wanting to use their facilities. Whether or not the school actually moves forward with the event, there is a risk of blowback from those both supporting and opposing the activity. This is especially the case with groups who deliberately court such a reaction and are prepared to respond whether or not the speech occurs. Therefore, many schools risk a protest simply from having a controversial speaker approach them in the first place.

Core Capabilities: This observation speaks to the Public Information and Warning; Intelligence and Information Sharing; and Situational Assessment core capabilities.

2.) Deciding on Appropriate Law Enforcement Presence at High Risk Events

- Determining the right level of law enforcement presence at a potentially volatile event is difficult.

When discussing the processes of becoming aware of potential protests on campus, workshop participants brought up the challenge of judging the appropriate amount of campus and local police to assign to an event. A small police presence may be overwhelmed and unable to effectively respond to escalating violence and property damage. A larger police presence allows a quicker response to an escalating threat but could be viewed as an overreaction which agitates protesters, or as seen as an impediment to free speech. In either case, a negative incident could damage a school's reputation. Universities have to make this determination for each event, and there is no easy choice on the spectrum available between these two responses.

Core Capabilities: This observation speaks to the On-scene Security Protection, and Law Enforcement; Threats and Hazards Identification; and Situational Assessment capabilities.

3.) Managing Insider Threat

- Insider threat is a persistent concern due to the inherent trust institutions must give their employees.

A perpetual risk brought up during one workshop was how damaging a disgruntled insider can be to an institution's network. Employees and other staff may have a comprehensive understanding of operations and are knowledgeable enough to cause technical difficulties if they become malicious. This a challenge that cannot be eliminated but may be mitigated through closer integration among all stakeholders involved with handling potential troublemakers, especially recently terminated employees. IT, human resources, facilities, and other departments need to be proactive in their efforts to identify persons of concern and reduce the issues they can cause.

A similar challenge brought up during that discussion was how seniority at a university, access control, and critical backups intertwine. It was observed that, generally, the longer a staff member had been present at an institution, the more accounts they have access to and, therefore, the harder it is to manage those accounts and recover them if that person were to leave. The practice of accruing credentials is a common one and is exacerbated by the typical length of a university career, making it difficult for IT administrators to properly manage and curtail one person becoming a critical point of failure for multiple niche resources.

Core Capabilities: This observation speaks to the Cybersecurity; Access Control and Identity Verification; and Threats and Hazards Identification capabilities.

4.) The Rapid Pace of Media, Social Media, and "The Story"

- Both social media and reporters can get ahead of an event, spreading inaccurate information.

When discussing how to organize and manage media presence on campus at one workshop, a local police department brought up prior violent events where it had been a challenge to manage media and communications during a rapidly changing situation. Examples were cited of media contacting the department to ask about details that were not true or the department discovering tweets posted online with inflated casualty amounts, which in turn caused various state and federal level agencies to prepare for a response to a situation that did not exist. While many universities have a robust ability to respond quickly through social media, the workshop's participants recognized that this is a persistent and complex challenge that is extremely hard to solve in an environment where social media is often changing and is used so ubiquitously.

Capabilities: This observation speaks to the Public Information and Warning capability.

5.) Media Sensitivity to Cyberattacks

- Despite the actual scope of any cyberattack targeting a university, there is always a high risk of the media exaggerating its impact.

At one workshop, during a discussion of the various website defacements that participants have seen over their careers, the risk of the media turning relatively simple actions by unskilled criminals into a much larger story was brought up. Even if the impact is low, such as a compromised website not related to the school's main page or a temporarily seized social medial account, it was observed that the headline in the news the next day could still likely be that the institution was "hacked" with all the consequences that are implied. This creates a perception-management issue for IT or public relations departments that will not quickly go away.

Core Capabilities: This observation speaks to the Public Information and Warning capability.

6.) Protest Organization Moving to Private Channels

- The amount of insight public social media applications can provide into potential protest planning is diminishing.

Student affairs representatives participating in one workshop signaled a trend they are finding to be a challenge when tracking student protests: the movement of online student protest organization from public to private forums. In the past, it was easier to locate potential student protests as they were often formed around a public social media page that both advertised and organized the event. Searching for these pages helped college administrations keep track of campus activity, even if they were not

informed of the activity officially. That is not always the case anymore and these conversations have been moving to more private, often encrypted, social media applications, making it difficult to know of a protest's existence ahead of the fact.

Core Capabilities: This observation speaks to the Planning and Threats and Hazards Identification capabilities.

7.) Split Attention During Crises

- The attention given to a planned or unplanned incident takes away from attention given to basic network defense duties.

When discussing the scenario at one workshop, participants noted how useful it was that the scenario provided advanced warning of an attack. Much of the time in IT, there is no warning. Once an attack occurs and the network is known to be compromised, IT departments will take an "all hands on deck" approach to fixing the damage, especially if it is a smaller team with less resources. The risk of focusing the IT team's attention on the immediate threat and away from its regular day-to-day operations is a threat in and of itself. Those duties build the foundation of network defense and, if neglected due to lack of organizational bandwidth, can create further vulnerabilities to be exploited by attackers.

Core Capabilities: This observation speaks to the Operational Coordination and Cybersecurity capabilities.

Section 3: Conclusion

Throughout the 2018 REN-ISAC Blended Threat Resilience Workshop Series, the series had success in supporting the stated exercise objectives and included valuable dialogue among the participants, both in higher education and among critical security partners. The exercise highlighted Best Practices, Areas of Improvement, and Challenges that can be further explored and developed to bolster higher education security preparedness, response, and coordination, both at individual institutions and across the research and higher education environment.

With the changing threat landscape and the risk implications technology is experiencing across higher education, REN-ISAC has successfully facilitated meaningful discussion regarding security preparedness broadly across organizations and beyond single organizations—informing and enhancing the individual and collective security and preparedness of the research and education community across the United States and throughout the broader REN-ISAC membership. From the first workshop in Indiana to the series' conclusion in Florida, participants were able to identify real experiences, challenges, and successes from recent years and events that can serve as valuable examples for others within the higher education community.

Among the outcomes, this series was intended to identify best practices, preparedness gaps, and opportunities for improvement that the community could learn from and further consider for their individual and community security and resilience. Productively, workshop discussions provided new ideas, organizational and community successes and challenges, and enhanced REN-ISAC's and participating organizations' understanding of the higher education security environment. As this initial exercise series concludes, there has been clear value in the national conversation and the collective findings presented in this final report.

This report strives to share valuable ideas and considerations for higher education and partner organizations to further consider and develop to further their individual and collective security and preparedness in this evolving complex and blended threat environment.

REN-ISAC thanks all of the participating organizations in Indiana, Arizona, North Carolina, Oregon, Massachusetts and Florida that have candidly shared their ideas and experiences for the betterment of our community's collective security and preparedness.

Appendix A: Acronyms

- DDoS – Distributed Denial of Service
- DHS – U.S. Department of Homeland Security
- EOC – Emergency Operations Center
- FEMA – Federal Emergency Management Agency
- HSEEP – Homeland Security Exercise and Evaluation Program
- IT – Information Technology
- MOU – Memorandum of Understanding
- REN-ISAC – Research and Education Networks Information Sharing and Analysis Center

Appendix B: Complete 2018 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].

Module One: Twist & Shout

Scenario

Today is **[T Minus Three Months]**. Last week you received an application for a controversial, off-campus, speaker to rent space at your campus to host a speech on **[T]**. The request that you have received outlines that the main event will be a two-hour long speech starting at 7:00 p.m. that includes a question and answer session with the audience. In addition, there will be a more private, invite-only reception for the speaker occurring later in the evening that is being sponsored by a campus student organization.

Today, after the university announced the event, it appears to be gaining traction both locally and on the national news. Similarly, on social media, national and local groups on both sides of the political spectrum have issued statements supporting or opposing the speech, and there are suggestions of gatherings in support and opposition to coincide with the two events.

Questions

1. What offices within your organizations would be notified of the application and who would approve or disapprove of the request?
2. If approved, who is notified of the event? What does that process look like?
3. As gatherings are announced and the level of attention and media awareness increases, what actions would you take at your campus and impacted facilities?
    a) Would you reach out to other schools or facilities that have hosted this, or similar, speakers? What other means would you use to assess the threats and risks of this event?
    b) What coordination would you conduct with local organizations?
    c) What coordination would occur with local law enforcement?
    d) Would there be any communication or coordination with faculty and/or the student population?
4. Would your organization identify if the speaker was invited by a student organization or other campus member? Does that matter?
5. Would you seek the assistance of student government or other student groups to help with planning the event and addressing security concerns?

Module Two: Power to the People

Scenario

Today is **[T Minus One Month]**, and the controversial speech was approved and is now one month away. During this period, you have gradually become aware of multiple threats to your university's facilities in response to this event. There have been multiple Facebook events created that describe themselves as protests either intended to counter or support the speech, respectively. Some are being planned by student organizations, others by local community groups. There are a significant percentage being organized by outside actors, and it is likely there will be many people from out of state arriving on campus. In addition, a cyber activist group has tweeted statements that may be interpreted as threatening to attack campus networks for perceived failures in the university's approach to the event. Both the events and the statement have utilized a set of Twitter hashtags that have become commonly associated with the controversial speech.

Questions

1. How would your institution become aware of these threats? How would you continue to monitor such threats (i.e., online, security networks, law enforcement, etc.)?
2. What is the threshold for when a planned protest becomes a risk concern that requires increased security measures?
    a) What type of routine protest/demonstration procedures do you have in place?
    b) What triggers changes and how are those coordinated?
3. How does your security plan change depending on the specific venue (stadium, auditorium, field house, classroom, etc.) where the speech will be held?
4. What other sources of information and intelligence would you be likely to use that have not already been discussed?
5. What types of communications would be occurring as threats increase and escalate?
    a) Internally among security teams?
    b) With school leadership?
    c) With school population?
    d) With parents and/or alumni?
    e) With local law enforcement and responders?
    f) With local organizations (businesses and others in potential protest or spillover areas)?
    g) With media?
6. In this or a like situation, is there any other information you would want to know or have access to, from your organization or other partners?
7. Are there any actions you could take at this time to help proactively manage potential/emerging security concerns?

Module Three: Revolution – Vignette One

Scenario

Today is **[T Minus Two Weeks]** and you have been made aware of a "target list" available on Pastebin that is being distributed on certain activist websites and forums. This list contains names, email addresses, and, in some cases, the physical addresses of professors, students, and other campus personnel that have been linked to planned campus protests that promote messages opposing the values of the online community propagating the file. While the list itself does not advocate for any specific action, conversation around the list has included posts saying that "something should be done with them." You are told the information was likely scraped from a combination of public sources and the directory that any student, staff member, or alumni can access.

Questions

1. Under routine conditions, would you notify non-IT security personnel about such threats? Would you notify physical security personnel? Does this change given the upcoming speech?
2. What actions would IT security personnel take upon such notifications?
    a. Notifications?
    b. Security measures?
3. What actions would physical security personnel take upon such notifications? How does this change given the upcoming speech?
4. Would you contact local law enforcement? Who is responsible for such notifications?
5. Would you attempt to identify who may be responsible for such posts?
6. Does the apparent age of the Pastebin data have any relevance, e.g. does your process vary by age of data?

Module Three: Revolution – Vignette Two

Scenario

Today is **[T Minus Two Weeks]** and you have been alerted to potentially concerning hacktivist chatter on social media by a cybersecurity vendor. Their analysts have uncovered conversations and a Pastebin containing details on your university's technical infrastructure to such a degree that the vendor suspects basic network reconnaissance has been conducted against the university's police department and emergency communication system. Separately, university staff have reported network activity targeting your student portal that could potentially have been a trial DDoS.

Questions

1. Under routine conditions, would you notify non-IT personnel about such threats? Would you notify physical security personnel? Does this change given the upcoming speech?
2. What actions would you take upon such notifications?
    a. Notifications?
    b. Security measures?
3. What webpages are the most essential for the university to recover from a potential DDoS outage, if any?
4. Have you experienced a DDoS attack at your institution? Were there any notable successes, challenges, or lessons learned you can share?
5. Are there any resources or capabilities you'd want to have or have access to that you don't presently have?

Module Four: Come Together

Scenario

Today is **[T]**. The speech will be occurring as scheduled. The campus is largely crowded with speech attendees, protestors, and media. Although it was not required, many professors cancelled their classes. Protester turnout is higher than estimated. Though the vast majority of demonstrators on campus were peacefully protesting during the period before the speech, you are being told that violence has broken out between opposing groups. This has occurred both at the facility where the speech is being held and at other locations on campus, resulting in dozens of minor injuries.

Questions

1. What physical and cybersecurity measures have been put in place ahead of such an event?
    a) Are there increased security procedures that are taken? Increased staffing?
2. How would you plan to handle groups of protesters wandering outside of designated areas?
3. How will you handle media being on campus?
    a) Are there any different considerations for “national” media different than local media?
4. As physical altercations begin, what actions would you anticipate by school personnel and local law enforcement?
5. As security concerns increase, how do you prioritize the protection of people and assets (facilities, infrastructure)?
    a) Do you have an established priority list?
    b) Is there an established decision-making protocol?
    c) Is this a campus decision or is it coordinated with local law enforcement?
6. Have you documented and practiced crowd control and evacuation procedures?
7. Would you anticipate any social media use to maintain awareness of protest activities?
    a) Do you have social media awareness built into plans and procedures and who is responsible for it?
    b) Would IT work in coordination with your institution’s social media personnel?

Module Five: Something – Vignette One

Scenario

The speech recently ended, and you expect many protestors to begin leaving campus. However, you soon learn that a car has rammed into a large crowd crossing a road on campus, resulting in a dozen estimated wounded, many of whom are in a critical state. The driver of the car escaped from the scene on foot, but police have apprehended a suspect on campus that is believed to be the driver. Media coverage is still in the preliminary stages and reporters are asking for comments. There are multiple rumors or falsehoods out there about this incident, including:

- **Incorrect Report**: Two of the wounded have died.
- **Incorrect Report**: The ramming was deliberate attack by one faction of protestors against an opposed group of protestors.
- **Incorrect Report**: The driver of the car has a gun in their possession and is still at large.

Questions

1. How long after a major event do you maintain enhanced security?
2. Who would be responsible for security response and coordination? Who would be involved in the response?
    1. What would you be doing to secure the areas around the incident and protect personnel?
    2. What would you expect the medical response to look like at this time and what potential issues could you anticipate?
3. Who would be responsible for communications and what would you be communicating:
    1. Internally to organizational leadership?
    2. To the student population and others on campus?
    3. To parents and alumni?
    4. To the media and via social media?
4. With the likelihood of increased visits to university websites, what impact/disruption could that have on the organization and are there ways to mitigate those issues?
5. **Small Group Discussion:** Are there any additional actions IT security could take to assist with physical security activities at this time?
    a) Can IT security help in locating individuals?
    b) Can IT security help in communications?

Module Five: Something – Vignette Two

Scenario

The speech recently ended, and you expect many protestors to begin leaving campus. However, you soon receive multiple reports of a detonation on campus. On a well-traveled pathway between the building hosting the controversial speaker and the parking lot, what is currently suspected to be an improvised explosive device hidden in a trashcan has detonated. The explosion has injured a group of protestors and resulted in a dozen estimated wounded, many of whom are in a critical state. Media coverage is still in the preliminary stages and reporters are asking for comments. There are multiple rumors or falsehoods out there about this incident, including:

- **Incorrect Report**: Two of the wounded have died.
- **Incorrect Report**: Multiple detonations occurred.

- **Incorrect Report**: Campus security officers have found a suspicious package near the president's office.

Questions

1. How long after a major event do you maintain enhanced security?
2. Who would be responsible for security response and coordination? Who would be involved in the response?
    a) What would you be doing to secure the areas around the incident and protect personnel?
    b) What would you expect the medical response to look like at this time and what potential issues could you anticipate?
3. Who would be responsible for communications and what would you be communicating:
    a) Internally to organizational leadership?
    b) To the student population and others on campus?
    c) To parents and alumni?
    d) To the media and via social media?
4. With increased visits to university websites, what impact/disruption could that have on the organization and are there ways to mitigate those issues?
5. At the completion of notable events or incidents, how do you review actions taken, key decisions, capture lessons learned, etc.?
6. **Small Group Discussion:** Are there any additional actions IT could take to assist with physical security activities at this time?
    a) Can IT help in locating individuals?
    b) Can IT help in communications?

Appendix C: Combined Observations

Note: Venue indicates the host school where the discussion occurred, not the institution that brought up the observation.

Observation	Observation Type	Venue
A Comprehensive Campus Speaker Approval Process	Best Practice	Northwestern Academic Computing Consortium; Harvard University
Multi-Year, Multi-Stakeholder Meetings	Best Practice	Purdue University – Fort Wayne; Duke University
Proactive Management of Protest Groups On-Campus	Best Practice	Purdue University – Fort Wayne; University of Florida
Memorandums of Understanding to Defer Cyber Risk	Best Practice	Arizona State University; Duke University
Third Parties to Enhance Communications Capacity During and After Critical Incidents	Best Practice	Arizona State University; Harvard University
Exercising and Validating Plans	Area of Improvement	Purdue University – Fort Wayne; Arizona State University; Duke University; Northwestern Academic Computing Consortium
Identification and Protection of Critical Facilities	Area of Improvement	Northwestern Academic Computing Consortium; Harvard University; University of Florida
Increasing IT Security's Involvement in the Response to Physical Incidents	Area of Improvement	Duke University; Northwestern Academic Computing Consortium; Harvard University
Streamlining Emergency Responders' Access to Internal Campus Resources	Area of Improvement	Arizona State University; University of Florida
Protest May Occur Regardless of Controversial Event Approval	Challenge	Duke University; Harvard University
Deciding on Appropriate Law Enforcement Presence at High Risk Events	Challenge	Northwestern Academic Computing Consortium; University of Florida