2018 Blended Threat Resilience Workshop Series
Final Findings Report Brief

TLP: WHITE

About the Workshop Series

Inspired by a desire to strengthen the higher education community's response to blended, or complex, threats, REN-ISAC planned and executed six Blended Threat Resilience Workshops in diverse locations across the U.S. The workshops were interactive events where security professionals from a multitude of disciplines participated in creating strategic, policy oriented response to a hypothetical blended threat, which REN-ISAC defines as a physical or cyber danger that has the potential for crossing over to the other side and that may harm life, information, operations, the environment, and/or property.

REN-ISAC's inaugural 2018 program utilized a threat-informed and peer-approved scenario based on a hypothetical, controversial speaking event and surrounding hacktivist activity. By using this topic to focus the discussion, participating professionals could confront a topical concern that many campuses are facing while also gaining proficiency in responding to the broader topic of blended threats. Walking through this scenario allowed participants to experience a major incident from different points of view and learn how to more effectively cooperate with other security-related fields.

About this Document

To encourage security improvement within the larger higher education community, REN-ISAC documented the session conversations and extrapolated high-level observations in the 2018 REN-ISAC Blended Threat Resilience Workshop Series Final Report (read the full report). For the Final Findings Report Brief, we have sorted through the Final Report to provide the top five best practices revealed during the workshop series.

This document is TLP:WHITE, so we encourage you to share these findings with colleagues, supervisors, and administration at your institution.

Suggested Best Practices

1) Provide Full IT Support to the Emergency Operations Center

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

2) Create Memorandums of Understanding to Defer Cyber Risk

When IT security departments encounter denial of service attacks or data exfiltration attempts, they may need to call upon additional security operations personnel, network bandwidth, or other necessary cybersecurity capabilities. Creating memorandums of understanding that unites groups of institutions can rapidly allow incident responders to bring in additional resources from other institutions quickly and easily.

3) Create a Comprehensive Campus Speaker Approval Process

Institutions can gain better intelligence on the event's inherent risk by integrating emergency management into the speaker approval process. Using a single, online form for all proposed on-campus events automates the process of notifying the correct stakeholders involved in event-application approval, including local law enforcement when necessary. Centralizing the speaker approval process raises awareness of campus-hosted activities while greatly reducing the chance of not recognizing a potentially controversial application. While implementing this kind of approval process requires a large investment of time and resources, it can be a powerful tool to manage the varied activites that occur on a college campus.

4) Set Up Preauthorized Procurement Procedures Before an Incident Occurs

During incident response, institutions may need to make emergency purchases to better handle a rapidly changing situation. Preauthorizing funds gives incident responders more freedom and speed to procure what is needed to quickly solve the problem. 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.

5) Manage On-Campus Protest Groups Proactively

In order difuse the possibility of violence, an institution should create and follow a deliberate process for messaging protest groups before and during a planned event. Administration-supported teams of university staff can act as liaisons to protest organizers, providing a conduit between protestors and the administration and law enforcement. The liasons are responsible for ensuring the protest group's safety, as well as the safety of other attendees, university staff, and innocent bystanders. Law enforcement may be standing by for support, but only when the potential for violence appears, are they called in to take control of the scene.

Want More Information?

For a full list of best practices, as well as areas of improvement and challenges noted by workshop participants, consult the 2018 REN-ISAC Blended Threat Resilience Workshop Series Final Report.

Interested in hosting or participating in one of our future Blended Threat Resiliency Workshops? Contact Sarah Bigham at sarah@ren-isac.net.