U.S. Department of Education—Readiness and Emergency Management for Schools (REMS) Technical Assistance Center

LESSONS LEARNED
From School Crises and Emergencies

Vol. 5, Issue 1, 2010

PREPARING FOR A CYBER SECURITY BREACH BEFORE ONE OCCURS: University of Southern Mississippi National Center for Spectator Sport Safety and Security's Cyber Security Tabletop Exercise (TTX) (2010)

In March 2010, a cadre of "hacktivists" leveraged their collective capabilities to mount a nationwide, coordinated cyber attack. A sophisticated network of relationships enabled the adversary to degrade Internet connectivity, disrupt industrial functions, and ultimately erode confidence in everyday communications. Due to their critical nature and perceived vulnerabilities, the adversary specifically targeted several critical infrastructure sectors, along with state and federal agencies, the media, and universities. The adversary was acutely aware that attacks on IT and communications interests would not only impact those sectors but would also result in cascading conditions suffered by other targets.

University of Southern Mississippi (USM) school officials became aware of the attack when reports began circulating that certain online service support systems (including financial aid) were down or behaving erratically due to what appeared to be a massive computer virus. A counterfeit Malware CD, containing the malicious code, had been distributed to unsuspecting USM students as "free swag" in the campus commons. Using a virus that generated counterfeit digital certificates, the adversary directed unknowing USM web users to "spoofed" websites where funds were extorted and personal information was mined. Coordinated attacks on domain name servers and telecommunications router infrastructure resulted in a distributed denial of service and unreliable telephony. Users were intermittently unable to access websites, send e-mail, and make phone calls. The USM chief information security officer (CISO) received e-mail threats and false Amber Alerts were broadcast. Upon consulting with the Multi-State Information Sharing and Analysis Center (MS-ISAC), it was revealed that six other universities in the region were having similar problems. The series of suspicious events compelled the USM CISO to request activation of the state's Emergency Operations Center.

While the above scenario did not actually occur, it represents a real potential threat for any institution of higher education. James A. McGee, program coordinator and outreach specialist of the University of Southern Mississippi's National Center for Spectator Sport Safety and Security, not only recognized the vulnerability of his institution to such an attack but also decided to address this vulnerability before it was too late. To do so, he developed the above scenario as part of a Tabletop Exercise (TTX) specifically designed to help improve his school's ability to respond to such an event in the future.

> The exercise simulates a sophisticated cyber attack campaign through a series of modules directed against critical infrastructures. The intent of these modules is to highlight the interconnectedness of cyber systems with the physical infrastructure and to exercise coordination and communication between the public and private sectors. —*Description of Tabletop Exercise scenario from USM Cyber Security TTX*

This Lessons Learned document describes USM's development and implementation of this Tabletop Exercise, and the lessons learned from a cyber security breach—before one actually occurs.

Development of the TTX. The University of Southern Mississippi, located in Hattiesburg, Miss., is a 2008 Emergency Management for Higher Education (EMHE) grant recipient. One grant activity was to conduct three tabletop exercises (TTXs) to test the institution's emergency management plans, and McGee seized this opportunity to address what he saw as an important emerging topic. "I think just about any current intelligence you look at will show significant vulnerabilities exist related to cyber systems, and universities are really dependent upon that capability," said McGee.

To garner support for this idea, and bring on board parties necessary for its implementation, McGee talked at length with the IT personnel at USM and their campus EMHE grant advisory group about the potential threats posed to the school and university system by cyber security breaches. Soon after, all agreed this was a topic the university and its partners could benefit from examining, and McGee crafted the exercise.

McGee understood the need to create a TTX on cyber threats that was specific to the university environment. However, because no other existing cyber security TTX's for universities were found, he created one himself. By piecing together materials from cyber exercises done at the national level, and adapting them to fit the setting, McGee created a TTX specific to the unique needs and concerns of an institution of higher education. In the end, McGee created a three-part package, including a facilitator's guide, participant's guide, and training PowerPoint presentation for "The University of Southern Mississippi National Center for Sport Safety and Security Cyber Security Tabletop

Cyber Security Tabletop Exercise Objectives

The University of Southern Mississippi (USM), in collaboration with its state and local emergency response partners, conducts a Cyber Security TTX using the four phases of emergency management (prevention-mitigation, preparedness, response, and recovery) as a foundation to:

- Examine the capabilities of USM to prepare for, protect from, and respond to the effects of cyber attacks.
- Exercise senior leadership decision-making and interagency coordination of incident responses in accordance with the USM Cyber Response Plan or applicable plan.
- Validate information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information.
- Exercise intra-governmental (federal-state) coordination and incident response.
- Identify policies or issues that hinder or support cyber security requirements.
- Identify public and private interface communications and thresholds of coordination to improve cyber incident response and recovery, as well as identify critical information sharing paths and mechanisms.
- Identify, improve, and promote public and private sector interaction in processes and procedures for communicating appropriate information to key stakeholders and the public.
- Identify cyber physical interdependence of infrastructure of real world economic and political impact.
- Raise awareness of the economic and national security impacts associated with a significant cyber incident.
- Highlight available tools and technology with analytical cyber incident response and recovery capability.

Exercise." The exercise was inaugurated March 9, 2010, on the USM campus, with McGee directing.

Implementation of the TTX. For the exercise to be a success, said McGee, and have real consequences for preparedness efforts, it was crucial to recruit the key players on campus and in emergency management for participation. "It is important to get the word out a few months in advance," advised McGee, "so that people can put the date on their calendars….With a cyber exercise, you want to have as much attendance and participation as you can get, as this problem really affects everyone."

McGee first went to the university president's office, and then to all the various entities that have an interest in this topic or emergency management, in general, to recruit participants. "Whatever the exercise is going to be testing does customize, a bit, who will be participating," McGee explained. Generally, the campus crisis team and police department representatives participate, but for this exercise, the audience was heavily comprised of members of the IT department. In addition, university personnel, the state Emergency Operations Center coordinator, and community representatives were involved, totaling around 12 – 15 active participants with at least 40 – 50 people observing. "The entire IT department showed up en masse," said McGee, "I think because they were so interested in the scenario, and we were doing an exercise that was bringing attention to this issue."

Lessons Learned from Conducting the TTX. "If I could point to one takeaway [lesson] overall," McGee observed, "it was the fact that despite what we all know about the dependency that the entire university has on the cyber system, if there was an outage, [we] would really be in dire straits, and would really have to scramble to correct that situation. This is something that hasn't really been discussed big-picture-wise."

Following the conclusion of the exercise, participants contributed to an after-action report, identifying vulnerabilities and areas for improvement. Many of these can and should be considered by institutions everywhere as ways to begin improving cyber security on campus. They should:

- Identify the critical window of time, after which continued data loss and malfunction of specific systems would be catastrophic, and develop a contingency plan that addresses continuing university academics and business operations in the event of a long-term cyber outage.
- Determine whether there is a formal emergency communication plan with other nearby universities, or even regionally or statewide among institutions of education, for cyber security threats and outages; if a communication plan is not found, work to develop one.
- Conduct an informational campaign so students and staff know where to go to get information during an emergency, and establish emergency communication procedures and back-ups in the event of an outage, including:
    - An off-campus website that is updated by a third party
    - A phone line that can be called for up-to-date information
- Conduct training across campus for students, faculty, and staff on:
    - The dangers of a cyber outage, considering the extent of campus dependency on computers and networks, and the widespread effects one would cause.
    - How cyber breaches can be prevented (e.g. antivirus software) and awareness that any machine can be compromised, not just servers, to create a systemwide attack.

- Conduct a vulnerability assessment for the existence and location of classified research data on campus.
- Develop standard policies and procedures for servers across campus, especially those outside the IT department's control.
- Consider developing a university working group to address cyber outage issues.

Participants in the USM cyber security TTX on March 9 at USM gave positive feedback. McGee said that members of the IT department found that the scenario accurately and realistically addressed potential cyber security issues. "[IT staff] was satisfied with the scenario, and what it tried to extract, in terms of vulnerabilities and weaknesses," said McGee. At the same time, university and other emergency personnel who participated did not indicate the scenario was too technical for them to follow.

Working together to brainstorm a response to this scenario improved dialogue and connectedness between university administrators, emergency personnel, and IT staff. Perhaps most important, university personnel recognized that they need to come up with both a short-term and a long-term strategic plan for this type of scenario, having not previously recognized that a cyber breach would create such far-reaching problems. "This is a topic people don't want to think about," said McGee, "but the reality is that this is one of the greatest vulnerabilities on campus, while also being an avenue that can lend itself to causing the most damage."

To access USM's Cyber Security Tabletop Exercise materials, visit:
http://rems.ed.gov/index.php?page=resources_Repository_Browse

This *Lessons Learned* publication was written during the summer of 2010 with the assistance of James McGee of the University of Southern Mississippi's National Center for Spectator Sport Safety and Security.

The REMS TA Center was established in October 2007 by the U.S. Department of Education's Office of Safe and Drug-Free Schools (OSDFS). The center supports schools and school districts in developing and implementing comprehensive emergency management plans by providing technical assistance via trainings, publications and individualized responses to requests. For additional information about school emergency management topics, visit the REMS TA Center at http://rems.ed.gov or call 1-866-540-REMS (7367). For information about the REMS grant program, contact Tara Hill (tara.hill@ed.gov) or Sara Strizzi (sara.strizzi@ed.gov).

This publication was funded by OSDFS under contract number ED-04-CO-0091/0002 with EMT Associates, Inc. The contracting officer's representative was Tara Hill. The content of this publication does not necessarily reflect the views or policies of the Department, nor does the mention of trade names, commercial products, or organizations imply endorsement by the U.S. government. This publication may also contain hyperlinks and URLs for information created and maintained by private organizations. This information is provided for the reader's convenience. The Department is not responsible for controlling or guaranteeing the accuracy, relevance, timeliness, or completeness of this outside information. The inclusion of information or a hyperlink or URL does not reflect the importance of the organization, nor is it intended to endorse any views expressed or services offered. All hyperlinks and URLs were accessed September 2010.