After-Action Report

FEMA/EMI Virtual Table Top Exercise
Cyber – Cyber event that disrupts A-State’s cyber security operations
December 09, 2021

Executive Summary

On Thursday, December 09, 2021, A-State executives and key leaders from campus and community response departments engaged in a tabletop exercise to test the campus’ Business Continuity Plan (BCP) and Emergency Operations Plan (EOP). The scenario presented to participants was based on lessons learned from the Cybersecurity & Infrastructure Security Agency (CISA), Federal Emergency Management Agency (FEMA), and Emergency Management Institute (EMI). The content and specific situation selected for the A-State exercise simulated a cyber-attack on A-State’s online infrastructure. The exercise pushed our Cybersecurity and Information Technology Services (ITS) team to their limit and demonstrated where university executives will report during a major campus cybersecurity incident.

The results of this test include recommended improvements in five general areas; including updating the BCP, improving emergency communications protocols between different departments, training employees about cyber threats annually, administering simulated cyber security threats on employees of the campus biennially, and updating information.

The following report includes details for areas of improvement identified during the exercise and its follow-up activities.

Updating the BCP

Department of Safety/Emergency Management (DSEM) & ITS will work together to complete the following:

- Update the backup for The System Vice President for IT.
- Share the plan with leadership each time updates are made.
- Update the executive leadership team members and contact information in the plan.
- Update phone numbers and the call tree in the plan.

Emergency Communications

- During the exercise it was discovered that many of the participants were unaware of who had taken the place of those who no longer work for the Department of ITS at A-State. To correct this, once the call tree is updated on the BCP, DSEM and ITS will work together to brief all leadership on campus on the corrections and updates.
- All staff will also be reminded of who they are to report to if they are exposed to a cybersecurity threat or phishing email, by ITS.

Cybersecurity Trainings

- A-State leadership will orchestrate informational trainings annually, to staff and faculty, on cybersecurity knowledge and how to report phishing emails and cyber threats to the campus cyberinfrastructure.

Simulating Cybersecurity Threats

- The A-State Cybersecurity team will lead in efforts to test faculty and staff's cybersecurity knowledge by sending out fake phishing emails biennially to selected departments with leadership buy-in and notification to leadership. These simulated cybersecurity threats will determine which departments are most at risk and will also determine which departments and employees need to be retrained on procedures. DSEM, HR, Marketing, and ITS will work together to ensure that the rollout is effective.

Updating Information

- Faculty and staff need to know who to contact for every situation. This is why all contact information will be updated in the EOP, BCP, and Emergency Procedures Handbook (EPH) annually by the leadership that attends to each plan. The EPH is given to all new employees and will remain up to date. The DSEM will ensure that all information on the BCP, EOP, and EPH is accurate and does not contradict one another.
- Biannually the Crisis Assessment Team as defined in the Data Center Incident Recovery Plan (DCIRP) and Team Leaders from the Business Unit Recovery Team (BURT) will meet to formally review and confirm any revisions to the plan. Plan changes will be documented in the Plan Revision section, and ITS will be responsible for distributing updated plan documents. The Chief Information Officer (CIO) will provide an annual status report on continuity planning to the Executive Steering Committee. The BCP will be regularly reviewed and revised to reflect ongoing changes to resources, business functions, etc. In addition, any updates must be tested and personnel trained accordingly.
- The following departments have a role in the BCP and will assist with updates: Enrollment Management, Registration, Financial Aid, Admissions, Payroll, Treasury, Sponsored Programs Accounting, Procurement, Travel/Disbursement/Controller, and Banner/Technical Support.