CHECKLIST \ BY AMY MCINTOSH

How to Create Your University's Incident Response Playbook

FOLLOW THESE STEPS TO ENSURE YOUR PLAN IS READY FOR ACTION.

Make sure you have a clearly defined incident response policy. This defines key terms, establishes time frames and priorities for responding to incidents, and explains all roles and responsibilities. The incident response policy will help inform your incident response plan.

Develop incident response processes. In addition to security-related processes, be sure to define processes for communication, reporting, sharing information and coordinating with law enforcement. Set aside adequate funding for development and maintenance of these procedures.

Regularly review and update your incident response playbook. Plans should be reviewed at least once a year and revisited when the university's incident response policy changes.

Cover relevant technologies in your incident response budget planning. Technologies might include continuous monitoring, centralized logging and log analysis, network security controls, vulnerability management systems, anti-malware and anti-phishing tools, and ticketing systems.

Provide training for everyone involved in the incident response plan. Internal and outsourced incident responders are important players, but don't overlook security operations center personnel, IT support staff and end users when developing your playbook. Training for all parties on software, incident identification and reporting is critical.

Conduct regular training and tabletop exercises. Exercises and tests ensure all appropriate parties know their roles in carrying out the incident response plan. They also can be valuable for identifying shortcomings in the plan itself.