Senior leadership and administrators

Govern resilience, make crisis decisions, and fund the controls that keep the campus running.

Before — prepare

- Set risk appetite in writing. Cybersecurity is enterprise risk, not an IT cost center.
- Approve a written incident-response plan and authorize the IR team to act under defined thresholds.
- Fund phishing-resistant MFA, immutable backups, EDR, segmentation, and security staffing as a baseline.
- Sponsor an annual tabletop exercise with cabinet, communications, and legal participation.
- Set policy on third-party software risk; require security review for systems holding student, research, or financial data.
- Define decision authorities now: Who can take systems offline? Who can authorize ransom-related discussions with insurer/counsel? Who notifies the board?

During — respond

- Convene the crisis team; defer to the Incident Commander on technical sequencing.
- Make business decisions IT cannot: which services to suspend, which to maintain, what to communicate to whom and when.
- Engage outside counsel and your cyber-insurance carrier early. Understand the insurance's required steps before you take them.
- Treat the ransom decision as a strategic, legal, and ethical question — not a technical one. Coordinate with counsel and law enforcement; many demands can be addressed without payment.
- Communicate calmly and frequently to the campus and trustees. Acknowledge what you don't yet know.

After — recover & learn

- Receive the AAR and approve a remediation plan with timelines and budget.
- Report to the board, regulators, and accreditors as required.
- Re-baseline cybersecurity investment based on observed gaps; do not let the moment pass without funding decisions.
- Recognize the responders. Burn-out after a major incident is real and costly.

Self-audit checklist

- Cybersecurity risk appetite and policy are documented and current.
- An IR plan exists with named roles and pre-approved authorities.
- MFA, EDR, immutable backups, and segmentation are funded baseline controls.
- An annual tabletop exercise has been run with cabinet participation.
- Third-party risk review is required for systems holding regulated data.
- Decision authorities for crisis steps (take offline, ransom posture, board comms) are documented.
- Cyber-insurance, outside counsel, and IR retainer are in place and known to the IR team.

Created by Joshua Gerstenfeld and Scott Jacques with support from the CrimRxiv Consortium. Code MIT-licensed; content licensed CC BY 4.0. Sources: NIST SP 800-61r3, NIST IR 8374, CISA #StopRansomware, EDUCAUSE. See: https://github.com/crimconsortium/campus-ransomware-playbook