IT and Security teams

Operationalize prevention, detection, containment, recovery, and after-action review at scale.

Before — prepare

- Enforce phishing-resistant MFA (FIDO2/WebAuthn) on privileged accounts; require MFA campus-wide.
- Maintain offline, immutable, and tested backups for tier-1 systems. Test restoration on a defined cadence.
- Segment networks: separate research, administrative, student, IoT/lab, and clinical environments.
- Disable or strictly gate Remote Desktop Protocol (RDP) and legacy VPNs; require MFA and conditional access.
- Inventory assets and software dependencies, including third-party SaaS. Track exposure to known CVEs.
- Run continuous endpoint detection and response (EDR) with tested response playbooks for common ransomware behaviors.
- Hunt regularly for indicators of compromise in identity providers (impossible travel, MFA fatigue, OAuth grants, mailbox rules).
- Practice a tabletop exercise at least annually with leadership and communications.
- Pre-arrange incident-response retainers, legal counsel, cyber-insurance contacts, and FBI/CISA points of contact.

During — respond

- Trigger the incident-response plan; appoint an Incident Commander and stand up a war room (in-person or out-of-band channel).
- Contain: isolate affected segments, disable compromised identities, revoke active sessions and refresh tokens.
- Preserve evidence: capture memory and disk images before reimaging where feasible.
- Stop further encryption: block known C2, disable risky outbound traffic, kill malicious processes via EDR.
- Engage law enforcement (FBI/CISA in the U.S.) and any cyber-insurance hotline early; do not pay a ransom without legal/exec coordination.
- Coordinate with communications and legal on internal and external messaging cadence.

- Track everything in an incident timeline — decisions, actors, timestamps. This is essential for after-action and notifications.
- Plan recovery in priority order using your business-impact analysis; do not restore unhardened systems back into a still-compromised environment.

After — recover & learn

- Validate eradication: hunt for persistence, scheduled tasks, rogue accounts, mailbox rules, and OAuth apps.
- Rebuild affected systems from known-good images; rotate secrets, certificates, and service-account credentials.
- Run a structured after-action review (AAR) with a blameless postmortem; produce a written report and tracked actions.
- Update detections, runbooks, and the playbook based on observed TTPs.
- Brief leadership and the board with what changed, what we still need to fix, and what we will measure next.

Self-audit checklist

- ■ Phishing-resistant MFA is enforced on all privileged accounts; MFA is required campus-wide.
- ■ Backups are immutable or offline and restoration is tested at least quarterly for tier-1 systems.
- ■ Network segmentation isolates research, admin, student, and IoT/lab environments.
- ■ RDP is disabled or behind MFA-gated, conditional-access VPN.
- ■ Asset and software inventory exists and is updated automatically.
- ■ EDR is deployed on all endpoints and tied to documented response playbooks.
- ■ Identity-provider hunting checks (impossible travel, OAuth, mailbox rules) run on a schedule.
- ■ Tabletop exercise has been run with leadership in the last 12 months.
- ■ IR retainer, cyber-insurance, legal, and FBI/CISA contacts are documented and current.

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