Communications, public affairs, and legal

Honest, timely, well-coordinated communication keeps trust intact and meets legal duties.

Before — prepare

- Pre-draft holding statements, FAQ skeletons, and stakeholder lists for a ransomware-style incident.
- Map regulatory and contractual notification obligations: FERPA, HIPAA (if applicable), GLBA, state breach laws, GDPR (for EU-resident data), grant requirements, and insurer terms.
- Establish out-of-band communication channels (mass notification, SMS, fallback web page hosted off your main domain) and test them.
- Identify and brief spokespeople; coordinate roles between communications, legal, IT, and senior leadership.
- Build trust ahead of time with student media, local press, and the campus community — an established voice helps in a crisis.

During — respond

- Use the IR plan’s communication cadence: frequent, factual, and consistent. Don’t speculate on attribution or scope.
- Coordinate every external statement with legal, IT, leadership, and (where relevant) law enforcement and insurer counsel.
- Be transparent about what you know, what you don’t, and what you are doing. Vague statements erode trust faster than honest uncertainty.
- Have a single source of truth (a status page or pinned campus channel) and direct everyone to it.
- Track all communications in the incident timeline; they are part of the regulatory record.

After — recover & learn

- Issue closing communications: what happened (at the appropriate level of detail), what was affected, what changed, and what people should do.
- File required regulatory notifications within statutory deadlines; document the analysis behind notification decisions.
- Conduct a communications-specific AAR: what messaging worked, what didn’t, where channels failed.
- Update playbooks, contact lists, and templates with what you learned.

Self-audit checklist

- ■ Pre-drafted holding statements and FAQ skeletons exist for cyber incidents.
- ■ Regulatory and contractual notification obligations are mapped and current.
- ■ Out-of-band communications channels (mass notification, off-domain status page) are tested.
- ■ Spokesperson assignments and approval workflow are documented.
- ■ Relationships with student media and local press exist before a crisis.
- ■ Legal, IT, comms, and leadership have a joint review cadence at least quarterly.

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