Disaster Resilient Universities® Network Cybersecurity Facilitators Guide

When a cyberattack strikes an institution of higher education (IHE), rapid coordination and total alignment are critical. However, many institutions only discover their structural blind spots through the painful clarity of hindsight. This guide can help IHEs shift from reactive to proactive by prompting teams to uncover conflicting assumptions, clarify roles, and address vulnerabilities before a cyberattack occurs.

This question set was developed by a team of seasoned senior-level leaders serving in enterprise risk management, emergency management, IT, and information security at IHEs across the country. These top-tier professionals infused this guide with their real-world experience navigating actual crises. Because of their expertise, this tool is specifically adapted to the unique realities of college environments, such as:

- Open research ecosystems and academic freedom
- Shared governance and decentralized IT systems
- Federal funding obligations and public accountability
- Overlapping campus and external law enforcement jurisdictions

How to use this tool

This tool is a facilitator-ready set of questions designed for enterprise risk managers, emergency managers, CISOs, CIOs, and law enforcement leaders to conduct proactive alignment sessions.

- **The Goal:** Use these lists of questions to prompt discussions that get your CISO, CIO, ERM, EM and legal teams on the same page before a cyberattack occurs.
- **The Structure:** The guide is broken into six logical domains. Each section contains a specific objective, followed by a two-tiered list of questions.
- **Prioritization:**
  - Focus first on “the most important questions to ask” sections. They address the highest-priority strategic and operational vulnerabilities.
  - If there’s time and bandwidth, move on to the “If you can, also ask” sections to deepen the discussions and uncover additional risks.

This project was supported by a generous gift from Deloitte & Touche LLP (Deloitte). Points of view or opinions in this document are those of the authors.

Domains

1. Shared Understanding in a University Environment

Why ask these questions: The objective is to expose differing mental models, given academia's dual mission of openness and security.

The most important questions to ask:

- What constitutes a cybersecurity incident?
- What triggers do you look for to activate your team for a cyberattack?
- What characteristics move an incident from routine, day-to-day operations to needing higher-level coordination?
- How do we know what data has been exposed?

If you can, also ask:

- What is the potential impact of a cyberattack on you, your department, or your team?
- What kind of data do you have? Which projects/grants may have/produce data that is critical to secure funding?
- What is the role of the IHE's cybersecurity team during and after a cyberattack?
- Do we have the right people on the response team? Do they have the skills to address the issues?
- What are the implications of personal compromise when traveling abroad?
- What keeps you up at night regarding cyberattacks at our IHE?

2. Communication

Why ask these questions: The objective is to uncover and address fragmented information flows across colleges, labs, and administrative units.

The most important questions to ask:

- Who are the key stakeholders? Do we know everyone who needs to be informed?
- Who will be the point person to deliver updates to:
  - Students
  - Employees (staff)
  - Media
  - Faculty
- What are some triggers that would prompt your specific involvement?
- How will we balance attorney-client information with the need to update our community?
- Who "sounds the alarm" that a cyberattack has occurred?

If you can, also ask:

- What channels are available for communicating with students, faculty, and staff?
- What is the best way to ensure everyone reads and understands messaging?
- How often should we communicate with our community during an incident?
- What do you specifically need to know about a cyberattack that is occurring or has occurred at the IHE?
- When do we include the general counsel's office to preserve attorney-client privilege?

3. Coordination Across Academic, Research, and Public Safety Domains

Why ask these questions: The objective is to clarify roles ahead of time across overlapping but culturally distinct functions.

The most important questions to ask:

- Which specific departments should be informed first if there's a suspected cyberattack?
- Do we believe everyone knows what to do in a cyberattack? (Who do we think does not know what to do?)
- During and after a cyberattack, how often should coordinators meet to ensure things are aligned?
- What coordination mechanisms should we use to align key stakeholders during a cyberattack?
- Who leads the coordination meetings?
- Do you know who to alert first if you receive information about a potential cyberattack?

If you can, also ask:

- Does the emergency management/enterprise risk team have a different response model than the IT department for cyberattacks? Should there be one model?
- What should emergency management's role be in a cyberattack?
- What should IT's role be in a cyberattack?
- Do you know what your specific role is during a cyberattack?
- When should we activate the EOC?
- Which is a bigger concern: too many individuals in the room, or not enough/not the right people in the room?
- What platforms should we use to coordinate during an incident?
    - Voice calls?
    - Chats/DM/Slack?
    - Texts?
    - Incident management platform?
- What is the easiest way for your department to communicate information to others about a cyberattack?
- Should we do a tabletop exercise ahead of time? Do we think we would learn from it?

4. Trust Among Administration, Faculty, and External Partners

Why ask these questions: The objective is to surface trust barriers that inhibit rapid action and honest disclosure.

The most important questions to ask:

- Would you be hesitant to share or be concerned about sharing certain information during or after a cyberattack? If yes, what information, when, and why?
- What are your greatest concerns about trusting other people, departments, or teams during a cybersecurity event?
- How would we frame discussions about cybersecurity and its response around our institution's mission?
- How might a cyberattack affect your:
  - Research
  - Transparency efforts
  - Labor

If you can, also ask:

- If something goes wrong, will everyone point fingers? Or will they have each other's back?
- Are there instances where security policies have inhibited your work?
- Do you meet regularly with anyone on the IHE's cybersecurity team(s)?
- What connections can you make with stakeholders now that would improve trust when a cyberattack happens?
- Can you identify individuals who have influence and can speak for you?
- What is the potential loss of research grants related to this incident?
- What are the challenges around central vs. specialized research requirements during a cyberattack?
- What critical deadlines would be affected by a cyberattack?
- Who do we consider an external partner?
  - Parents?
  - Donors?
  - Visitors?
- Who in this group needs to be aware of information about a cyberattack?
- Do you focus on the "what" or the "who" when reviewing after-action reports?

5. Law Enforcement & Investigative Considerations

Why ask these questions: The objective is to align investigative needs with institutional mission and risk.

The most important questions to ask:

- What incidents should campus police bring to the attention of the cybersecurity team?
- What incidents should the IHE bring to the attention of law enforcement agencies?
- Who should be the primary point of contact with the FBI during an incident?
- Who should be the primary point of contact with law enforcement? Does it depend on the agency?

If you can, also ask:

- Should we keep the investigation and forensics separate from our operational impacts and response?
- What changes do we need to make to our information-sharing practices if we are dealing with a criminal investigation?
- Are there protocols and relationships we can develop now with law enforcement agencies?
- Should we do exercises now with law enforcement to test our cyberattack plans?
- Do we have a model for how to work alongside law enforcement?

6. Risk, Compliance, and Sponsor Obligations

Why ask these questions: The objective is to make implicit constraints explicit, especially those tied to federal research funding.

The most important questions to ask:

- How are we going to ensure we meet compliance (FERPA, GDPR, and other) requirements and deadlines during a cyberattack so that we avoid fines and penalties?
- What should we do if enterprise risk management's priorities are different from IT's priorities?
- What laws do we have to consider during cyberattacks? And how can new administrators get up to speed on those laws during an incident?
- How do public records laws apply to your work and to the IHE's information during and after a cyberattack?

If you can, also ask:

- In the event of a cyberattack, what is the immediate risk to the safety and security of our students, faculty, and staff?
- Who needs to know about the cyberattack, and when?
- What specific regulations apply to compromised data at the university? And to your work?
- How will our IHE's insurance coverage work for a cyberattack? What is covered and not covered? What are our obligations to the insurer?
- Do our international travel policies consider cyberattacks?
- How can we safeguard confidentiality of research data before a cyberattack occurs, especially with regard to nondisclosure agreements and other legal agreements?

- Will we still be able to meet our training requirements under accreditation and Clery Act if we experience a cyberattack?
- Should we report cyber risks to the board and the implications related to incidents and controls?