



EAB

Tabletop Exercise: Emergency Response

Responding to the COVID-19 Crisis: Part C

This situation belongs to [EAB's "Tabletop Exercise" Resource Center](#). There, you will find an explanation of the value of these exercises, guides for facilitators and observers, and an after-action report template.

We recommend this situation as the first of a multi-part tabletop exercise featuring Situations Part A and B, which can also be found in the resource center.

Responding to COVID-19 Crisis: Part C

In a week, staff and faculty awake to find several computer systems not working, including the e-mail and phone system, and social media is abuzz with students saying they cannot get into their classes.

Soon, IT staff discern that a cyberattack has occurred. They are saddened, but not surprised: with university community members logging in from so many networks, putting unfamiliar flash drives into borrowed laptops at home, clicking links and attachments in e-mails from many non-university individuals they are coordinating with, etc., they knew they were unusually exposed and vulnerable.

This could not come at a worse time:

- Online classes taking place over the Learning Management System (LMS) were about to result in final exams.
- Admissions, enrollment, and marketing staff are engaging in intensive yield efforts as the deposit deadline approaches, with prospects whose data is now stored in an inaccessible Customer Relationship Management (CRM) product.
- Academic advisors and financial aid officers now cannot access curricular or financial data in the Student Information System (SIS) or Enterprise Resource Planning (ERP) system.
- The development office was also running a “week of giving” campaign, asking alumni to give to a crowdfunding campaign to support student financial assistance, the webpage for which is now not functioning.

All suddenly grind to a halt. Your e-mail and phone system also rely in part on broader IT systems, and are also down.

Your institution’s typical cybersecurity incident response begins. But your IT team is exhausted, having been working around-the-clock to enable remote instruction, and some staff are not available, having taken sick leave. As a result, they are moving slower than usual to respond, not detecting the breach right away, delayed in understanding the nature of the vulnerability, and systems downtime stretches on as they must triage the restoration of certain services and systems before others.

However, they can conclude the hackers’ motive may have been to intercept the millions of dollars about to flow out of university payment systems in refunds. Luckily, they were not successful. However, the hackers did access some students’ personal and financial data.

Because this breach is bigger than any the university has encountered recently and is highly-visible because of the widespread nature of the outage at a time when campus is fully reliant on online systems, the incident response team needs input from university leaders on how to respond to certain aspects of it.

Moreover, university leaders must preserve to the extent possible the continuity of institutional operations during this time.

Discussion Questions

After reading the situation above together, participants should endeavor to work through the following questions below in the time they have permitted. **We recommend 30 to 60 minutes.**

NOTE: In this scenario, consider if the facilitator should divide the group in half for focused conversation on different questions for a short time, before then coming together to work through all the questions together.

- How should the university respond to this cybersecurity breach? Be specific: who should do what, and in what order? What departments, academic or administrative units, or teams should be involved?
 - What is our institution's typical incident response system for a breach like this, and what is the role of IT versus other university leaders and divisions?
 - How/does the COVID-19 crisis change the way we would otherwise to a cybersecurity breach? For example, breaches of this sort would typically trigger legal review and both internal communication and external/public communication to notify of a potential breach and to reduce reputational risk.
 - What external resources or vendors do we rely on for cybersecurity matters (e.g., forensic or technical specialists), and are they available during this time? Do we engage law enforcement, knowing they could offer much help, but are prioritizing the many hospitals under similar threat from hackers right now and will likely be slow to respond?
- The scenario cites several systems and important ongoing processes right now that would be affected.
 - What other systems and ongoing important efforts/initiatives would likely be affected by the above systems going down?
 - The CIO asks university leadership to advise on what systems are most important and should be restored first. The first system can be available within 12 hours, while the last ones may not be available for 48 to 72 hours. What is the recommendation?
- Revisiting the systems mentioned and the aspects of our work that they support, what actions could the university take to support each of its efforts if the relevant system remains unavailable for several days?
 - Teaching and learning
 - Communication with admitted students and applicants
 - Advising and student services for current students
 - Fundraising
 - Others represented by participants during this scenario

Post-Discussion Debrief

After working through the above exercise, the facilitator should lead the group through a shorter discussion exploring the below questions in the time they have permitted. **We recommend 15 to 30 minutes.**

Note: We recommend conducting a fuller debrief after the conclusion of a multi-part tabletop exercise, to aid in completion of an after-action report. These questions are designed to prepare the group to contribute more fully at that final stage.

- This case makes us realize the many technology systems we rely on to do our jobs, every day, but especially remotely.
 - What communication and collaboration systems would be down during this, making it difficult for us to even discuss and resolve the situation? Without university phone and email systems, how would staff get in touch with one another?
- How does COVID-19 and its resulting impacts make us more vulnerable to cyberattacks?
 - What proactive measures can we take now to protect against this possibility – hardening systems, creating backups, reducing staff and faculty likelihood to succumb to social engineering schemes, etc.?
 - What systems are most important to protect?
- In this scenario, IT staff is slow to respond because they have been working overtime for weeks on end. What are the consequences of an emergency that continues to strain a team that is already “at capacity”? How can we augment or cross-train, bring in more resources now, fight burnout and fatigue, etc.?