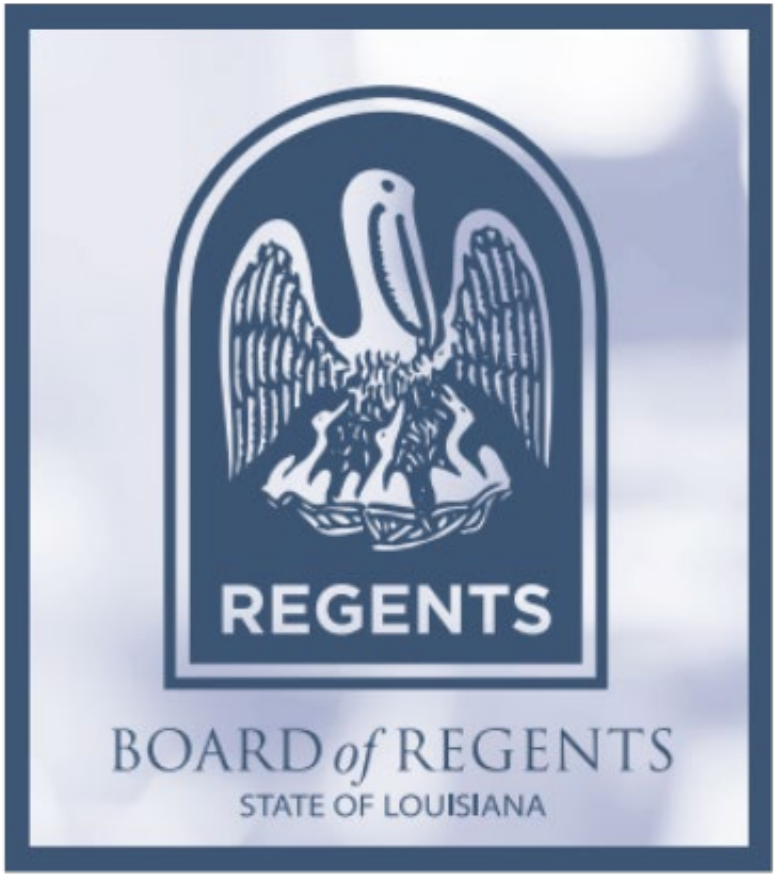
CASE STUDY EXERCISE

November 2022



RULES

- This exercise is NOT intended to ask the participants to find the exact source or motivations of the bad actors.
- This exercise is designed to create several scenarios and possibilities, highlighting the need for a Cyber Incident Response and Management Plan.
- No comment, question, or response from any participant is judged for accuracy.
- The scenarios contained in this exercise are purely fictional.
- No institution of higher education is targeted by the content in this exercise.
- It is ok to hypothesize any missing information. Indeed, much information is intentionally missing.
- This exercise is intended to engage technical experts and administrative personnel.
- Please think critically but be respectful of others.

GENERIC INFORMATION

- This is a case study a cyber incident that affects an unnamed University in Louisiana.
- This University does **not** have a cyber incident management and response plan.
- The University does have an I.T. staff that self-manages the network infrastructure.
- Classes for the Fall Semester Started on **Wednesday**, August 19, 2022.
- The University received large sums of tuition money right before school started.
- The University does not have a Continuity of Operations plan.

DAY 1: Wednesday

It is the first day of the new semester. In the morning hours, the University I.T. Department received four separate calls from the Bursar's Office. The calls were received by different members of the I.T. department.

Excepting only a few details, each of the calls from the Bursar's Office reported the same thing: while preparing monthly financial reports, several members of the Bursar's Office staff noticed that the accounting software is not reflecting accurate balances since the Bursar's Office received and input several thousands dollars towards different student fee bill payments yesterday from students, private lenders, and the U.S. Department of Education.

Three of the four I.T. Department personnel contacted by the Bursar's Office submitted helpdesk tickets with the name the accounting software provider, asking the vendor to inquire about the matter. The fourth I.T. Department personnel advised the Bursar's Office employee that she should log out of the software, reboot her computer, and then log back in. Without further instruction, the Bursar's Office tried to manually determine how the discrepancies occurred.

QUESTION SET 1

QUESTION: Is it effective for the I.T. Department to receive multiple calls from the same department about the same issue? Does this process delay or hurry necessary response activities?

QUESTION: Ideally, who would be notified about the event and by whom?

QUESTION: What kind of information should be recorded by whomever is tracking the issue?

QUESTION: Assuming the issue is classified as a cyber incident, what kind of questions should be asked and answered to help determine next steps?

QUESTION: What would it take to move this from a database miss-match to a software issue?

DAY 2: Thursday

Without the I.T. Department logging the calls or the Bursar's Office creating a central reporting mechanism for the calls, the I.T. Department did not realize that multiple users saw the accounting software discrepancies.

The Chief Operating Officer from the Bursar's Office, only learning of the issue on Thursday, checked the University's bank account, which reflects tuition payments, and finds the balance significantly below the anticipated balance. The Chief Operating Officer pulls the account activity for each account and sees several debit transactions to randomly named individuals over the last forty-eight hours.

The Chief Operating Officer alerts his immediate staff, which consists of his personal assistant, deputy Chief Operating Officer, and lead accountant, all of whom share the Chief Operating Officer's banking login, to ask if they knew anything about these transactions. Each of these staff personnel denied any knowledge of transactions.

The Chief Operating Officer immediately contacted the banking institution and had all the University's various accounts frozen.

QUESTION SET 2

QUESTION: Should the Chief Operating Officer unilaterally make the decision to freeze all the University's accounts?

QUESTION: With money missing from the accounts, is now the right time to contact some kind of law enforcement authority?

QUESTION: If the University had a Cyber Incident Response Manager, what actions should this individual be taking at this time?

QUESTION: Should the Bursar's Office alert other elements of the University's administration that there is a suspicious accounting error? Why/Why not?

QUESTION: Should any banking account access information be shared, much less the COO's account?

DAY 3: Friday

The Procurement Division of the University's Finance and Administration office received calls from two vendors stating that payments from the University were past due.

The Procurement Division checked its accounting software and saw that the disbursements were electronically sent two (2) days ago in response to the vendor's invoices. However, the vendors confirmed that it did not receive any recent electronic payments from the Procurement Division.

The Procurement Division contacts the University's Vice President to advise of the issue and then contacts its bank to learn that the funds were sent to accounts *not* belonging to the intended vendors.

QUESTION SET 3

QUESTION: Would a map of the University's network infrastructure be useful in matter? If so, how?

QUESTION: What does the University need to know in order to implement any short-term containment options?

QUESTION: If the University had not yet initiated ESF-17 assistance, should it? Was there an earlier time at which the University should have initiated ESF-17 assistance?

QUESTION: Is there anything the University can/should do to help protect other educational institutions?

QUESTION: How could Cyber Liability Insurance factor into this scenario?

QUESTIONS?

CONTACT INFORMATION

Dustin Glover
Chief Cyber Officer
225.773.6719
Dustin.Glover@la.gov

LTC Stephen Durel
Co-Lead of ESF-17
504.418.0957
Stephen.Durel@la.gov

Corey Bourgeois
OTS Cyber Incident Manager
225.279.4877
Corey.Bourgeois2@la.gov

CMSgt Don Hermann
Infosec Expert
504.237.7841
Don.Hermann@la.gov

Sarah Anderson
ESF-17 Counsel
225.615.0810
Sarah.Anderson@la.gov