

## What to Do When Your Problem Hits the 6:00 News

Donna Liss  
The University of Kansas

---

---

---


---

---

---

---

---



## Case Review

- What was it like when the incident happened?
- What are the controls (i.e., policies and procedures) needed when dealing with a security incident?
- Who should respond when there are security incidents?
- What are the things that people don't think of?

---

---

---


---

---

---

---

---



## The Incident: Facts and Climate Surrounding the Incident

- File contained data from Student Information System extract matching on:
  - Country of permanent address
  - Presence of visa information
- Included some U.S. students due to mismatches
- 1,450 records with the following information:
  - Name
  - Student ID #
  - SSN #
  - Passport #
  - Country of origin
  - Visa status

*This incident occurred as part of the new international student tracking program required by Homeland Security*

---

---

---

---

---

---

---

---

## What are the Controls Needed?

The main controls include the following:

- Crisis communication plan
- Technical security incident response procedures (including forensic handling procedures, chain of custody, etc.)
- Policy on whether and how to notify the affected individuals
- Protocol for working with Public Relations, the Media, and Legal Counsel
- Policy and procedures for dealing with notification of law enforcement

*.... there are more controls, but these are the basics policies and procedures needed.*

---

---

---

---

---

---

---

---

## Who Should Respond When There Are Security Incidents?

First, gather the right individuals:

- CIO and Other Relevant Technical Staff
- Policy Staff
- Legal Counsel
- University Administration
- Public/Media Relations
- Affected University Office(s)
- Public Safety Office (if relevant)
- IT Security Office

Next, define what your successful outcomes are:

1. Protect and inform the students
2. University acts, and is viewed as, a responsible organization

---

---

---

---

---

---

---

---

## Who Should Respond When There Are Security Incidents?

■ And define what you want to communicate:

- We know the facts, including which data were involved
- We acted quickly
- We are doing what we can to address the problem
- We are respectful of other people
- We are cooperating with law enforcement
- We accept responsibility for making it better

■ Assign a single spokesperson

---

---

---

---

---

---

---

---

## Successful Outcome 1: Protect and inform the students

### Actions:

- Partnered with Student Body President, Student Senate, International Students Office, and Legal Services for Students
- Created informed team focused on incoming and outgoing communications with affected students
- They heard it directly from us
- We provided information plus assistance
- Communication via email & U.S. mail
- Open, frequent communication diffused student frustrations relatively quickly

---

---

---

---

---

---

---

---

## Successful Outcome 1: Protect and inform the students

### Successes:

- Students were involved and felt cared for
- No protests, No lawsuits
- Students had resources to get the information they needed
- They trust us more when we're honest, even if they are frustrated
- They knew we were prepared and eager to help
- Should another incident occur, they have the expectation that we will communicate openly
- When dealing with potential fears, it's better to communicate more rather than less

---

---

---

---

---

---

---

---

## Successful Outcome 2: University as a responsible organization

### Actions:

- Immediately contacted the INS, FBI, and the KU Public Safety Office
- Contacted the vendor and selected other IT professionals
- Gathered roundtable of administrators to address problem
- Communication with the Media -
  - Wrote a brief to ensure all participants received exactly the same version of events
  - Went public within 24 hours
  - Called press conference and started it with a strong statement from the university
  - Brought informed student spokespeople to the press conference, so they were prepared to comment based on the facts

---

---

---

---

---

---

---

---

## Successful Outcome 2: University as a responsible organization

### Successes:

- Assessed level of partner knowledge and know-how, and helped them look good
- Collaborative war-room model with all major players
- Did not shoot the messenger
- Kept the vendor name out of the press, and worked as partners
- TV reporters are less likely to hunt for unknown students to fill news spots
- Timeliness is key to keeping coverage proportional to the incident

---

---

---

---

---

---

---

---

## What Are the Things People Don't Think Of? ... or Lessons Learned

- Define the successful outcomes before any communication goes out
- Technical language – use precision
- Prepare communication materials (the technical response is relatively easy, it's the communication that's hard).
- After the fact – evaluate your response (we use the term "fail forward")
- Understand how other affected third parties will respond
- Your security office may know more than the FBI and Police
- Communication with internal staff is important too

---

---

---

---

---

---

---

---

## What Are the Things People Don't Think Of? ... or Lessons Learned

- This is the time to use media contacts; choose the reporter when possible
- Pre-educate media relations staff on the technical issues and language
- Law enforcement agents may not understand the technical issues, so be ready to educate them along the way
- The FBI has an equal interest in their own public image, and those interests may conflict with yours
- Don't shoot the messenger
- This will live on in the media!

---

---

---

---

---

---

---

---

## Case Review

In Summary:

- Have your control policies and procedures in place, and follow them.  
**If you don't have these in place, you will not be able to focus on your successful outcomes!**
- Define what your successful outcomes should be and what you want to communicate first, then evaluate all actions against these outcomes.
- Assign a single spokesperson
- As soon as feasible after the incident has passed, evaluate your response and adjust your controls as needed.

Questions?

---

---

---

---

---

---

---

---