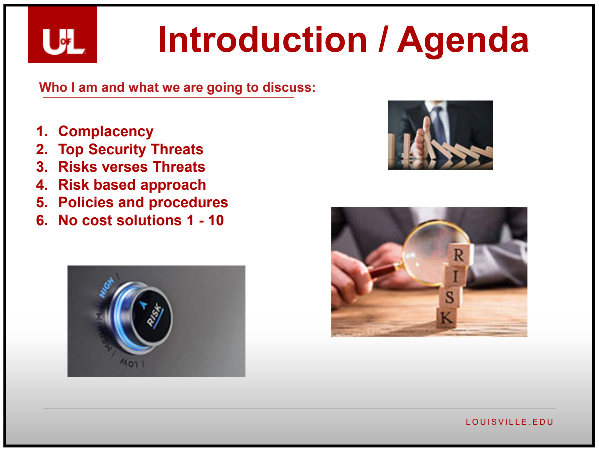
UNIVERSITY OF LOUISVILLE

Fall KASFAA Conference
Presented by: UofL Information Security Office
Speaker: Lisa Cooper

October 10, 2019



Introduction / Agenda

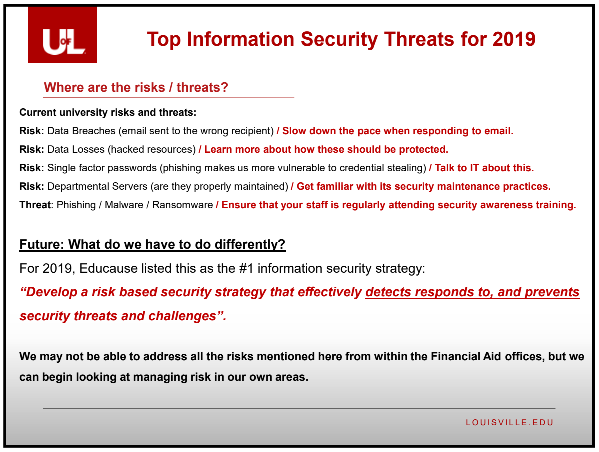
Who I am and what we are going to discuss:

1. Complacency
2. Top Security Threats
3. Risks verses Threats
4. Risk based approach
5. Policies and procedures
6. No cost solutions 1 - 10

LOUISVILLE.EDU

Complacency is not the way to go….

LOUISVILLE.EDU



Top Information Security Threats for 2019

Where are the risks / threats?

Current university risks and threats:

Risk: Data Breaches (email sent to the wrong recipient) **/ Slow down the pace when responding to email.**

Risk: Data Losses (hacked resources) **/ Learn more about how these should be protected.**

Risk: Single factor passwords (phishing makes us more vulnerable to credential stealing) **/ Talk to IT about this.**

Risk: Departmental Servers (are they properly maintained) **/ Get familiar with its security maintenance practices.**

Threat: Phishing / Malware / Ransomware **/ Ensure that your staff is regularly attending security awareness training.**

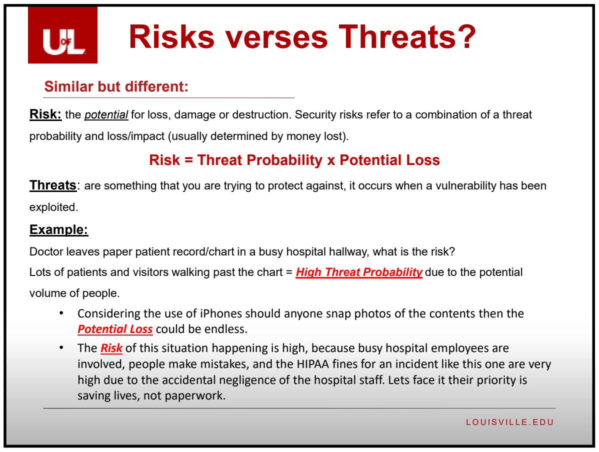
Future: What do we have to do differently?

For 2019, Educause listed this as the #1 information security strategy:

"Develop a risk based security strategy that effectively detects responds to, and prevents security threats and challenges".

We may not be able to address all the risks mentioned here from within the Financial Aid offices, but we can begin looking at managing risk in our own areas.

LOUISVILLE.EDU



Risks verses Threats?

Similar but different:

Risk: the *potential* for loss, damage or destruction. Security risks refer to a combination of a threat probability and loss/impact (usually determined by money lost).

Risk = Threat Probability x Potential Loss

Threats: are something that you are trying to protect against, it occurs when a vulnerability has been exploited.

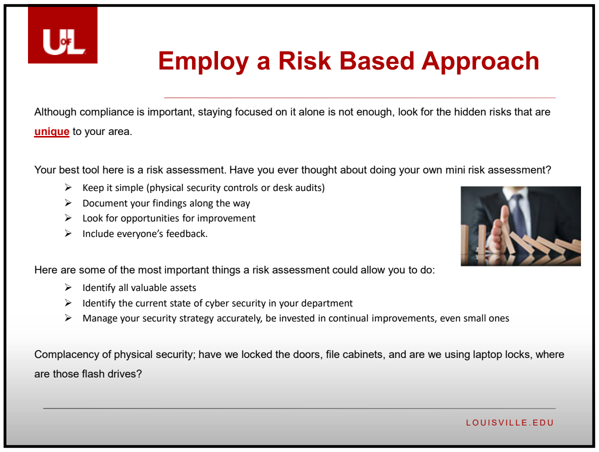
Example:

Doctor leaves paper patient record/chart in a busy hospital hallway, what is the risk?

Lots of patients and visitors walking past the chart = ***High Threat Probability*** due to the potential volume of people.

- Considering the use of iPhones should anyone snap photos of the contents then the ***Potential Loss*** could be endless.
- The ***Risk*** of this situation happening is high, because busy hospital employees are involved, people make mistakes, and the HIPAA fines for an incident like this one are very high due to the accidental negligence of the hospital staff. Lets face it their priority is saving lives, not paperwork.

LOUISVILLE.EDU



Employ a Risk Based Approach

Although compliance is important, staying focused on it alone is not enough, look for the hidden risks that are **unique** to your area.

Your best tool here is a risk assessment. Have you ever thought about doing your own mini risk assessment?

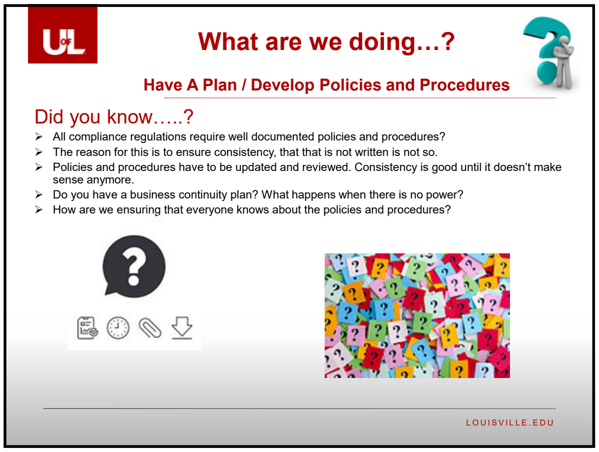
- Keep it simple (physical security controls or desk audits)
- Document your findings along the way
- Look for opportunities for improvement
- Include everyone's feedback.

Here are some of the most important things a risk assessment could allow you to do:

- Identify all valuable assets
- Identify the current state of cyber security in your department
- Manage your security strategy accurately, be invested in continual improvements, even small ones

Complacency of physical security; have we locked the doors, file cabinets, and are we using laptop locks, where are those flash drives?

LOUISVILLE.EDU



What are we doing…?

Have A Plan / Develop Policies and Procedures

Did you know…..?

- All compliance regulations require well documented policies and procedures?
- The reason for this is to ensure consistency, that that is not written is not so.
- Policies and procedures have to be updated and reviewed. Consistency is good until it doesn't make sense anymore.
- Do you have a business continuity plan? What happens when there is no power?
- How are we ensuring that everyone knows about the policies and procedures?

LOUISVILLE.EDU

No Cost Solution #1

Security Awareness Training

When is the last time your staff attended information security awareness training?

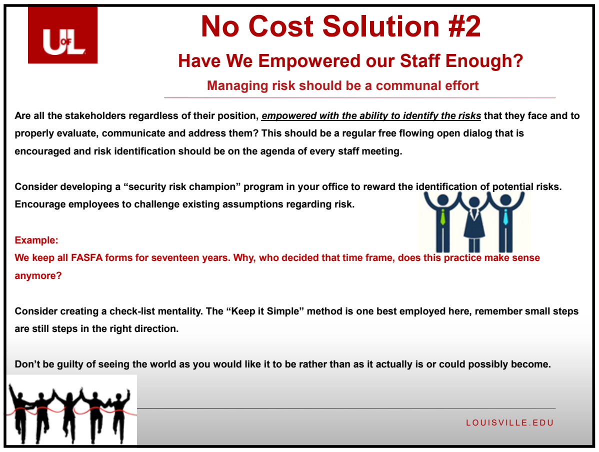
- Some regulatory compliance standards state that this is required.
- Do this at least annually.
- Keep records on who attended.

Questions to ask yourself:

- Does your staff know how to spot a phishing scam?
- How many new employees do you have?
- Does your CISO offer this service?

This process cost nothing but it helps kick off the conversation.

LOUISVILLE.EDU



No Cost Solution #2

Have We Empowered our Staff Enough?

Managing risk should be a communal effort

Are all the stakeholders regardless of their position, ***empowered with the ability to identify the risks*** that they face and to properly evaluate, communicate and address them? This should be a regular free flowing open dialog that is encouraged and risk identification should be on the agenda of every staff meeting.

Consider developing a "security risk champion" program in your office to reward the identification of potential risks. Encourage employees to challenge existing assumptions regarding risk.

Example:
We keep all FASFA forms for seventeen years. Why, who decided that time frame, does this practice make sense anymore?

Consider creating a check-list mentality. The "Keep it Simple" method is one best employed here, remember small steps are still steps in the right direction.

Don't be guilty of seeing the world as you would like it to be rather than as it actually is or could possibly become.

LOUISVILLE.EDU

No Cost Solution #3

Data Inventory

Do you know where your sensitive data is?

- Who is handling it and why?
- Are we just doing what we have always done?
- How much sensitive paper is in our offices, why?
- How can we protect what we didn't know we had?

- Know what you have
- Know where it is
- Know who owns it and who maintains it
- Know how important it is to the institution

This process cost nothing but the payoff is huge!

LOUISVILLE.EDU

No Cost Solution #4

Data Purging

Are we keeping things that we no longer need?

Do you have paper hoarders in your office / desk audits?

Do you have a sensitive data retention policy that is *consistently* followed?

- **Remember to consider state laws on data retention**
- **And ensure that it includes electronic data/systems**
- **Use secure data sanitization methods**

Communication: are we telling our students how long we will be keeping the data that they entrust us with?

What if we gave them a promise that their data would be removed from our systems by a specific date?

- **Our policy says to retain data for 5 years after graduation and then destroy**.

LOUISVILLE.EDU

No Cost Solution #5

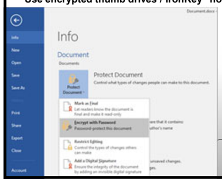
Using Encryption Methods

Add a password to any Office product and the file is automatically encrypted with 256 bit encryption

- **Using the same password for this method is fine, share it with the office**
- **If you forget the password then you have lost the file**
- **Never email the password**

Use 7-Zip to encrypt a group of files

Use encrypted thumb drives / IronKey "not free"



Info

Document

Protect Document

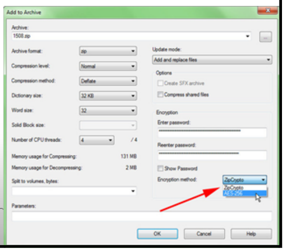
Control what types of changes people can make to this document.

Mark as Final: Let readers know the document is final and make it read-only

Encrypt with Password: Password-protect this document

Restrict Editing: Control the types of changes others can make

Add a Digital Signature: Ensure the integrity of the document by adding an invisible digital signature



Add to Archive

Archive: 1508.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 4 / 4

Memory usage for Compressing: 131 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options: □ Create SFX archive □ Compress shared files

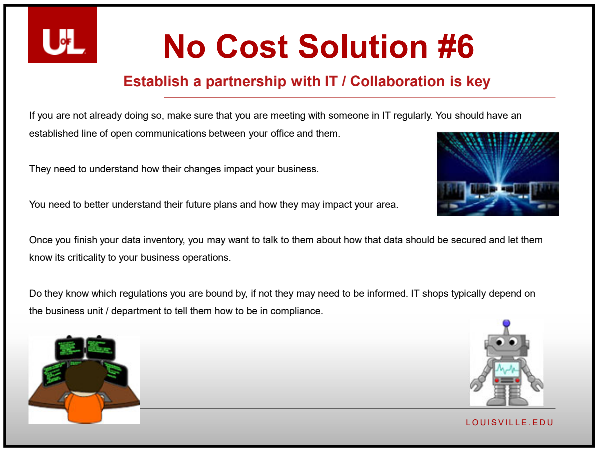
Encryption

Enter password:

Reenter password:

□ Show Password

Encryption method: ZipCrypto (ZipCrypto, AES-256)



No Cost Solution #6

Establish a partnership with IT / Collaboration is key

If you are not already doing so, make sure that you are meeting with someone in IT regularly. You should have an established line of open communications between your office and them.

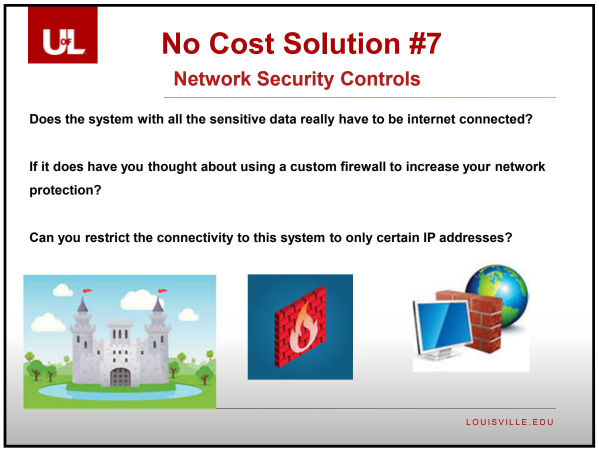
They need to understand how their changes impact your business.

You need to better understand their future plans and how they may impact your area.

Once you finish your data inventory, you may want to talk to them about how that data should be secured and let them know its criticality to your business operations.

Do they know which regulations you are bound by, if not they may need to be informed. IT shops typically depend on the business unit / department to tell them how to be in compliance.

LOUISVILLE.EDU



No Cost Solution #7

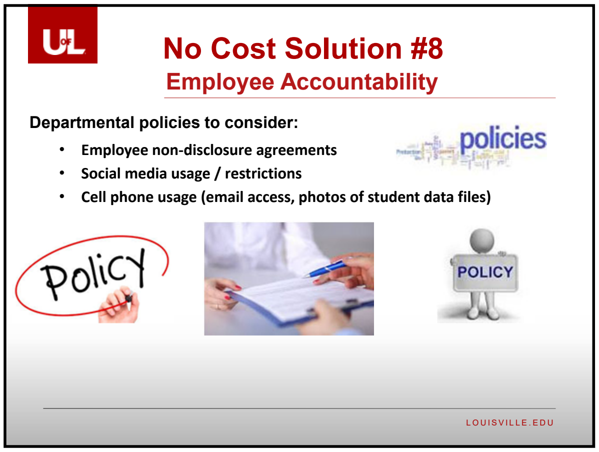
Network Security Controls

Does the system with all the sensitive data really have to be internet connected?

If it does have you thought about using a custom firewall to increase your network protection?

Can you restrict the connectivity to this system to only certain IP addresses?

LOUISVILLE.EDU



No Cost Solution #8

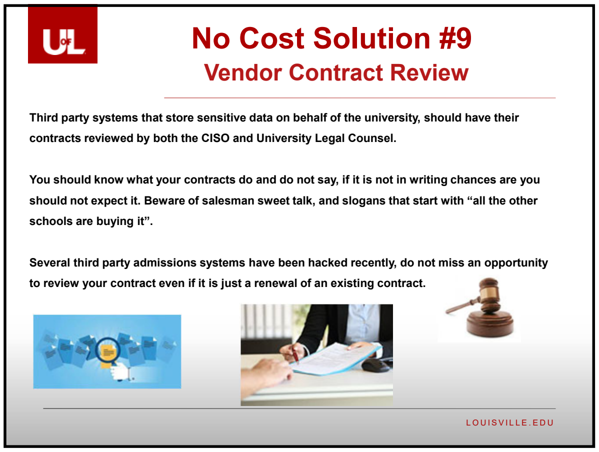
Employee Accountability

Departmental policies to consider:

- **Employee non-disclosure agreements**
- **Social media usage / restrictions**
- **Cell phone usage (email access, photos of student data files)**

policies
Policy
POLICY

LOUISVILLE.EDU



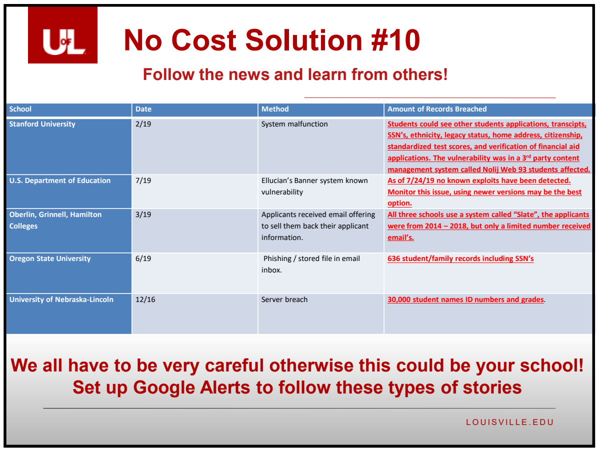
No Cost Solution #9

Vendor Contract Review

Third party systems that store sensitive data on behalf of the university, should have their contracts reviewed by both the CISO and University Legal Counsel.

You should know what your contracts do and do not say, if it is not in writing chances are you should not expect it. Beware of salesman sweet talk, and slogans that start with "all the other schools are buying it".

Several third party admissions systems have been hacked recently, do not miss an opportunity to review your contract even if it is just a renewal of an existing contract.

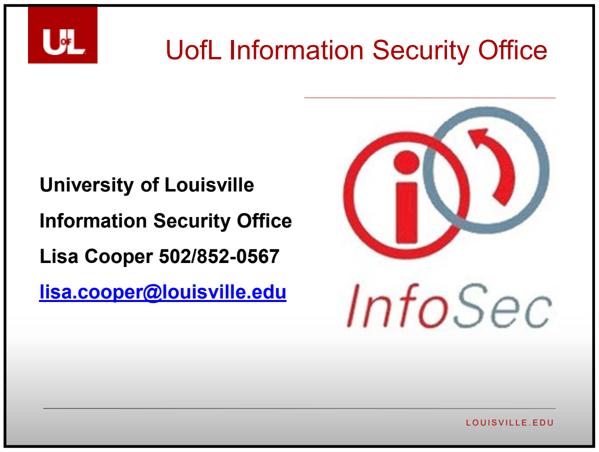


No Cost Solution #10

Follow the news and learn from others!

School	Date	Method	Amount of Records Breached
Stanford University	2/19	System malfunction	Students could see other students applications, transcipts, SSN's, ethnicity, legacy status, home address, citizenship, standardized test scores, and verification of financial aid applications. The vulnerability was in a 3rd party content management system called Nolij Web 93 students affected.
U.S. Department of Education	7/19	Ellucian's Banner system known vulnerability	As of 7/24/19 no known exploits have been detected. Monitor this issue, using newer versions may be the best option.
Oberlin, Grinnell, Hamilton Colleges	3/19	Applicants received email offering to sell them back their applicant information.	All three schools use a system called "Slate", the applicants were from 2014 – 2018, but only a limited number received email's.
Oregon State University	6/19	Phishing / stored file in email inbox.	636 student/family records including SSN's
University of Nebraska-Lincoln	12/16	Server breach	30,000 student names ID numbers and grades.

We all have to be very careful otherwise this could be your school!
Set up Google Alerts to follow these types of stories



UofL Information Security Office

University of Louisville
Information Security Office
Lisa Cooper 502/852-0567
lisa.cooper@louisville.edu