14 February 2017 LMIS

In attendance:
James Berhanrd
Lisa Woods
Jeremy Cucco
Hilary Robbeloth
Mike Benveniste
Kate Cohn
Andrew McPherran
Patrick O'Neil
Ann Gleason
Linda Williams

The meeting was called to order at 8:16 a.m.
Jeremy Cucco opened with the last main item of business to discuss after the Cloud: Security
Cloud storage will still be discussed in the context of security later today.

Security
Health Insurance Portability and Accountability Act (HIPAA) and Federal Educational Rights and Privacy Act (FERPA) are the primary area with mandatory compliance.
Our network storage and email systems are not HIPAA certified. Personal health information should not be floating around.
To set the stage for security threats, Jeremy noted an experiment of last summer in which a Palo Alto network traffic analyzer was temporarily implemented to monitor attempted cyber-attacks. In one week we had 2.5 million attempted attacks on the network.

He noted that insider threat is largely *not* here because of the respectful nature of our students. Some of the threats are brute force attack – hacking a password most common. Several types of threats involve code injection looking for weaknesses. Some are denial of service attacks – these are particularly problematic as students need to be able to access dining accounts and moodle.

Brute Force threats from outside are not seen as a MAJOR problem. Generally the biggest threat on campus is insider access security threat; that is, someone gets a password and access.
SOCIAL ENGINEERING is the biggest threat. People seeking access guess or engineer information. OR they access it from improperly stored or disposed confidential information, like a class roster that is not disposed of properly
Different categories of outside entities seeking inside access:
Phishing emails. Common
Whale phishing – a large group particularly with access to money or financial information
Spear phishing. Highly targeted
SPAM filters get most of these. The university's SPAM filters are largely rule-based and target specific words in emails. For example, one filter deletes all emails that say "click here to log in" as it's a common wording in Phishing messages. On the other hand, some of the spam filters inadvertently keep out real emails in the intent of blocking malicious email, for example Amazon

web services used for a class where the term “Click here to login” was used in an email that was a legitimate message.
A Rainbow Table is a list of words that a person is known to use. A hacker would use a hashing algorithm to come up with the permutations and they get the hash across the system. A long password made up of multiple words is better and is less likely to be able to be cracked by a rainbow table.

A few tell-tale signs of SPAM or Phishing messages. We do not send out emails from the Help Desk – service desk, yes. But Help Desk is too common. Also, don’t give out your username and password over the telephone and it’s never requested in an email.

Students often have their mail routed to regular email which makes it harder for them to sort through and spam lowers defenses. Some spam is crafty spam, though most is just annoying. Username and password is the holy grail for hackers and you need to have a defense strategy. You make different separate domains but if someone is able to escalate permissions then it becomes dangerous. Then the hacker finds operating systems that are out of date and patches need to be done regularly.
Hacks are commonly available as downloads on the Internet. Script Kiddies download hacks as executable hacks and can run them indiscriminately. Only purpose is to destroy things.

Lisa W.: Are our laptops automatically updated? Windows machine and mac need to be updated automatically.
Jeremy: To be on the university network, all endpoint computers must have auto-updating turned on as a rule (validated by SafeConnect). Therefore, all systems connected to campus should technically be regularly updated.

All of these issues relate to security of information on campus. We ought to have more security associated with sensitive information and security awareness training so sensitive forms are not sent over email.
Lisa: we ought to recognize the type of information we are handling. Security is not just a computer issue but how paper documents are also used. Difficult to keep track of sensitive information.
Someone noted that we need to be more conscientious about SHREDDING. Cross cut shredders. Disallow cell phones in a paper records space.

Is the Cloud safe?
Patrick: a cell phone can be used to photograph records and then send them out. This makes the images public.
Jeremy: We can try to protect information through policy control and technical control. University would intercede in the second case.

Regarding Privacy concerns: the university does not monitor internet traffic. Demographic information is reported in aggregate, so not individual information – not religion or cultural information.

Back to paper documents: Frequency of pickup should increase so shredding can happen much more frequently. If bins are full, take documents to TS for shredding {Update: Contact Linda Green in finance to have additional bins brought by if needed}.

James: Where are we as a campus security wise?
Jeremy: we are in a good situation now. How much is exposed is the question. What will we accept and how much is covered by insurance. Reputation of university is compromised. As are people. We patch as frequently as possible with firewalls. However, accidentally someone's password may become public.
We are all responsible for information on the university computers.
Meeting was adjourned at 9:13 a.m.