CGRC Meeting Minutes 4/5/2019

CGRC 4/5/19

Time: 10:00 AM

Location: 8A EWFM, rm 625

Attendees: Eric Zematis, James Monek, Walt Conway, Steve Oblas, Rich Bauer, Alex Radus, Kim Nimmo, Madalyn Eadline, Yenny Anderson, Dan Lopresti, Donna Cressman

Welcome to the committee:

Start up meeting since this committee hasn't met in several years. Walt Conway, Steve Oblas, Madalyn Eadline & Dan Lopresti were past members of this group

Scary Stories:

- 1.3 million identities stolen at Georgia Tech (Banner school)
- WPI student gains access to admissions portal and can edit his file - no hacking required through Salesforce - student reported to Wpi to tell them to fix it
- Students can download pictures of every student on campus and have their picture and university ID number - AT LEHIGH - Eric working with Adirondack to see what can be done. LIN was accessed as well. Only current students were affected. Need to address our practice and how we handle this - published to the Adirondack service. Don't have resources to test everything.

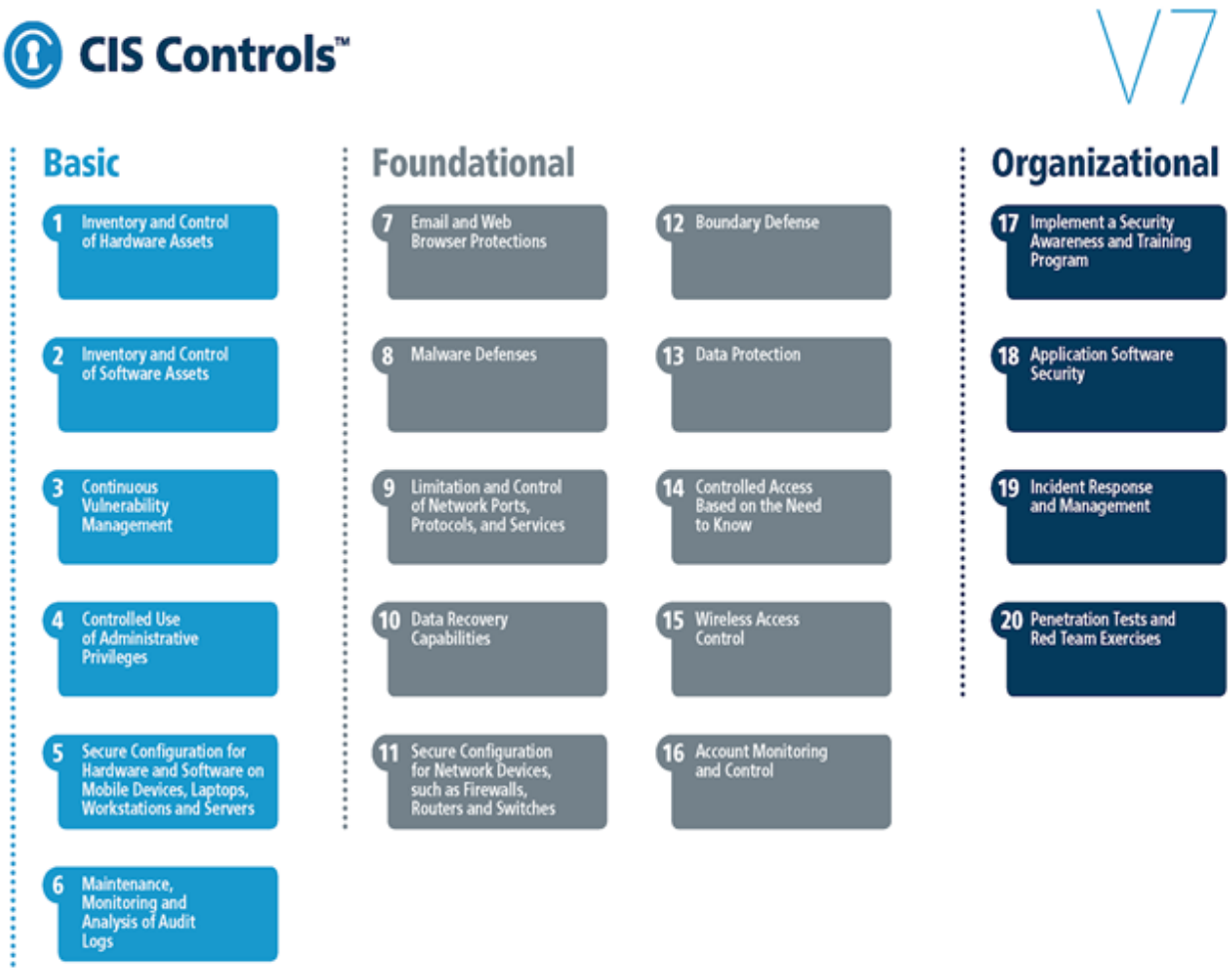
We need to:

- Help secure infrastructure - prevent
- Help educate people - when a security incident does happen it should not be a surprise to senior leaders and we need to respond effectively

What is our current reality?

CIS controls -

A common set of security controls ranked by which ones are most effective against known attacks. As a higher education institution we have weaknesses with these controls. For example, we allow many people to access our network which creates issues with knowing every device on the network (CIS Control #1)



Risk assessment vs other universities - We participated in a risk assessment workshop and scored 3.3 out of 5 (is good) - Lehigh

1.9 out of 5 - other universities.

Overall, Lehigh does a lot of good security activities compared to other universities. Unfortunately it is a race against attackers and not other universities.

Who are we?

Currently defined as: (This is from the previous iteration of the CGRC. Do we need to rewrite this?)

The Cyber Governance, Risk Management and Compliance Oversight Committee provides guidance and oversight to the information security policies, strategies, and initiatives at Lehigh University. The Committee is led by the Chief Information Security Officer and is comprised of representatives from the Faculty, Legal Counsel, Risk Management, Internal Audit, University Communications and Public Affairs, Student Affairs and Library and Technology Services.

What is our relationship to the other committees:

- Data Governance
- Risk Management
- LTS Committees
    - ACIS (Advisory Council for Information Services)
    - ISSC (Information Systems Steering Committee)

CGRC Charter

- We will need a formal document defining purpose, authority, membership, roles and responsibilities.
- We will need to review the charter template
- Looking for volunteers for charter group

    - Dan Lopresti (remote), James Monek, Alex Radus, Walt Conway
    - Students want things private
    - FERPA regulations
- Collecting data - security devices - include privacy
- What is the relationship of privacy. When do we disclose data/ information?
- Stream data into cloud or server on campus
- HVAC - if it's too hot in building it can affect data on servers

History of the CGRC committee:

Steve Oblas, Walt Conway were in the committee. The committee dropped off after Keith Hartranft started. Keith was active in the community but relied on smaller groups and committees.

The committee discussed privacy policies that were outdated

Walt suggested that we bring in Baker Tilly - **Eric reached out and they will represent going forward**

Risk Management needs to be involved

Dan Lopresti said that the Cloud is the big question.

Security of using the Cloud.

How can we carve out the network for security?

Steve Oblas - His group does a lot with the media.

- Widespread phishing scam.
- Potential exposure of student pictures and LINs. **As of April 5, 2019 at 5:30 pm, Eric announced this was patched this and there was no evidence that anyone maliciously exploited the vulnerability**
- Public perception.

Eric - The CGRC committee needs to sit in the middle and connect to the other committees

- Example, When a question came up a month ago about using a 3 or 4 catergory Data Classification systems it is best handled by the existing Data Stewards group.

Policy creation

Security strategy

Opinions from outside LTS - opinions, heard on the street, etc

Committee to community

- The LTS ACIS committee takes its policies to the Lehigh community for approval. Can we have this committees policies go through that process rather than create our own.

Other business:

What are we about and make this a policy

1. Information security policy - need to establish working group after Charter Committee
2. Privacy & Acceptable Use Policy review - Legal is creating a working group for this and we can coordinate with them
    a. Rapidly changing privacy landscape (GDPR, CCP)
        i. GDPR - subset
    b. Web site privacy policy

General Discussion

Cloud security - big things will go to cloud - need privacy

Banner will go to Cloud

Social media for class - such as Facebook live accounts

Some faculty will use social media in their classroom. What happens if a student doesn't have a media account. These students will miss out on information. Having a media account is not mandatory. We should have an alternative for these students. We can not force students to use social media.

Do we have a policy to prevent students from going with a 3rd party.

Professor communication outside of Lehigh.

Team Drive to CGRC - all information is in here. Material is sensitive.

- All monthly reports
- Audit report
- Agendas
- Minutes

Meeting cycle: End of May; end of Sept; end of November