Appalachian
STATE UNIVERSITY

Information Security Advisory Council

February 16, 2017

1.0 WELCOME

Jim Webb welcomed everyone to the 10:00am meeting held in the Walker College of Business Board Room, Peacock Hall #2013

Members in Attendance:

- Crystal Brooks, Tim Burwell, Clayton Christian, Laura Crandall, Matt Dull, Regina Hartley, Oscar Knight, Barbara Krause, Angie Miller, Terry Rawls, Jim Webb, Kevin Wilcox

Members Absent:

- David Jamison, Amy Sanders, Rachel Serrano, Robin Tyndall

2.0 REPORTS & STATUS UPDATES

SECURITY OPERATIONS REPORT – KEVIN WILCOX:

Recent Security Incidents:

- A puzzling incident occurred that the security team is trying to figure out. A faculty member clicked on a legitimate mailing list that they planned to join. Within 5 minutes of joining, the faculty member received 2,500 or more emails saying “Thank you for subscribing to our mailing list.” Not only were there more than 2,500 emails, they were in a multitude of languages (Russian, Arabic, Italian, etc.)
- Nothing high risk has come up lately
- Recent investigations have shown that there are a large number of departments that have a lot of data available.
- There was a recent incident that involved a student using a computer that was out in the open after hours. There was no malicious intent, but it shows that there is a greater need for physical security.
- A way to better secure the University’s physical assets is to work with University Police to work towards getting more physical security throughout campus (video cameras, making sure doors are locked, etc.)
- There was also a discussion of an incident that took place that needs to remain confidential. The incident has been resolved.

POLICY & COMPLIANCE REPORT – OSCAR KNIGHT:

PCI-DSS Updates:

- ITS partners with the Foundation to help with their compliance. The Foundation uses Authorize.net. Authorize.net decided to take down their firewall. The Foundation is now looking for a new solution. Oscar Knight & Laura Crandall have been in discussion with the Foundation’s bank. This leaves the Foundation with 2 vendors, which is challenging. It appears that even the banks don’t always know how to be compliant with PCI.
- The University is not completely PCI Compliant, but we are working on it. We are looking for encryption solutions to become compliant. We are not alone – there are a lot of UNC institutions that are also not yet compliant.
- Some of the work to become compliant is technical, but most of it has to do with relationships, dealing with vendors, etc. There are many conference calls and meetings that take place.

- SAQ, which is conducted yearly is completed.
- The Holmes Center is going to start doing Point-to-Point encryption
- Point-to-Point encryption was installed in Student Programs and they loved using it. They said it was really easy to use.

SECURITY AWARENESS REPORT – CRYSTAL BROOKS:

Campus Training Engagements:

- Over the past few months, Jim and the Security Team have given Security Presentations to Staff Senate, the Athletics Department, and are scheduled to speak to the Student Development Directors and Student Development Employees.
- We have reached out to Amy Roberts' DRA group & Faculty Senate and hope to speak with them soon.
- Our next group to reach out to would be the High Security Area Groups – this will be more focused on keeping data safe and private, especially when dealing with names, addresses, social security numbers and grades.
- Jim and the Security Team is always open to come speak with any department that would like to have them come speak. Contact Crystal Brooks to schedule a Security Presentation.

Monthly Newsletter:

- We've had some good feedback on the January newsletter. The February newsletter is almost ready to go out. February's newsletter focuses on FERPA. There is vital information for faculty and staff in this newsletter.

Suggestions:

- We need to find a way to broaden the awareness of security threats throughout our campus. Any suggestions would be welcome.
- Angie Miller has seen some incidents of people signing up for the Affordable Care Act subsidy and are able to get this money by stealing information from other people. We need to add this to our topics to inform the University.
- We need to work on training employees not to send their personal information in an email (this happens frequently with people emailing HR and the University Counsel's Office). We need to stress the fact that email is not secure and personal information should not be shared via email. We need to work on File Locker.

3.0 OLD BUSINESS

SECURITY STANDARDS (Approved):

- **Encryption Standard**:
  - ISAC Approved
  - CIO is currently reviewing the standard

SECURITY STANDARDS – ONGOING FEEDBACK:

- **Remote Access Standard** (Soliciting Feedback) –
  - Personal equipment being used to open University data – there needs to be more training on this
  - We are looking to identify high security areas to see who should/should not be using their personal equipment to open University data
- **Secure Data Handling Standard** (Approval Review) -
  - Saving sensitive data needs to be consistent within a department
  - Guidelines need to be turned into requirements
  - Data disposal needs to be included in this standard
  - There needs to be a definition of confidential & sensitive that everyone adheres to.

  - We don’t want departments or people within a department to elevate a record if it’s not really sensitive just because they want to keep the data close to them.
  - The simplicity of breach data elements helps with knowing what data tiers each piece of information falls into.
  - The Office of General Counsel gets a lot of confidential/sensitive data via email and need to know how to put a stop to this. This might be something that Jim speaks to the departments about.
  - There are external services that can encrypt emails for people sending and receiving confidential/sensitive data
  - Clayton Christian looked over this standard and has some concerns about how some areas have sensitive data
  - Will look at Secure Data Handling Standard at March’s meeting.
- **Acceptable Usage Policy** (On Hold):
  - In the coming months, the plan is to put this online.
  - They decided to go forward with this with David Hayler, interim CIO.
  - There will be a security presentation with Faculty Senate discussing using personal equipment to access work data. Personal equipment can be considered a public record.
  - Electronic Discovery can be conducted on email. Even if you use your personal email, the court can make you show all of that email if a person has their AppState email forwarded to their personal account. This is not a good idea to do.
  - Keep work email on work email and personal email on personal email.
  - Every communication with a student is likely an education document.

4.0 NEW BUSINESS

- University Data Asset Inventory + Data Governance: What are all the systems out there that have data?
  - Clayton Christian: they compiled data inventories that ITS had put together. The internal audit project was the completion of that project. Did this data inventory properly identify the systems that were out there? It did.
  - There is a lot of work still to be done, but there should be another governance group created to work on this.
- Penetration Testing of Banner ERP Systems:
  - Third party security Assessment went really well. The report that we got back had small findings, but it spoke highly of our work.
  - The medium issue was in development for old form for direct deposit. This will not exist when we make the migration to Banner XE.
  - They couldn’t make an attack work. They spent 2 weeks trying to do that & couldn’t get into the system at all.
- Email Spoofing + ITS Mail Validation - Feedback:
  - Chancellor Spoof Messages: There are applications that can dramatically stop the spoof messages that are sent from places other than Appalachian State. The Chancellor is very concerned about this – it is a big reputation issue. This is not something that we can do quickly. If we flip the switch today – it would appear that IT broke something that someone is working on.
  - We need a central location for sending out emails. UNCG uses Google Groups and then there’s a record of what has been sent out.
  - iModules is a legitimate service for Alumni, but it might look like spam to recipients.
  - Could we validate emails green if it has been validated by ITS and red if it has not been validated? It’s a good idea, but then we are trusting everything that comes through and become complacent.
  - We have a lot less control over our email due to the fact that we use Google
  - Leadership wants us to improve in this area and this is something that we are looking at.
- Multi-Factor Authentication Update (Duo):

	o Good news – we did get the funding for this. The contract has been sent out. ISAC can be early testers in this. One of the initial places to start this is VPN. We didn't go through a governance process to approve Duo, but we use it because of our involvement in certain groups that has caused it to have very attractive pricing and our sister institutions are already using it.
6.0	**MEETING ADJOURNED**
	Jim Webb thanked the group and adjourned the meeting at 11:20am.