Information Security Advisory Council

January 19, 2017

1.0	**WELCOME**
	Jim Webb welcomed everyone to the 10:00am meeting held in the Plemmons Student Union, Three Top Mountain Room #169 Members in Attendance: • Crystal Brooks, Clayton Christian, Oscar Knight, Barbara Krause, Angie Miller, Daniel Rawls, Rachel Serrano, Jim Webb, Kevin Wilcox Members Absent: • Tim Burwell, Laura Crandall, Matt Dull, Regina Hartley, David Jamison, Amy Sanders, Robin Tyndall
2.0	**REPORTS & STATUS UPDATES**
	SECURITY OPERATIONS REPORT – KEVIN WILCOX: • December 2016 was a busy month with several phishing attempts: 1) Spoofed Email from Chancellor Everts on Interpersonal Violence Training: ▪ Some folks gave their credentials, which caused their accounts to be compromised. ▪ There were some Direct Deposit changes that occurred due to this compromise. ▪ Direct Deposit was shut down for a period of time to safeguard other accounts that were compromised. ▪ No employees lost money. Everything was able to be reversed. ▪ There were about 12 more changes that have been made to employee Direct Deposit in the past couple of days. ▪ There have been conversations with other schools to discuss what has happened to see if there are any similarities 2) We have seen some multiple hacks/spoofs from the same people. They are trying multiple things using accounts they acquired in the first round of attacks. They have gathered this information and have sat on it until they are able to make other changes later on. 3) We know the IP address of the hackers, but haven't blocked them because we don't want to give away the fact that we know where they are. **What happens after there is a security incident?** ✓ After Action Review (AAR): This review function is written into the incident response plan. This is a requirement for incidents that pose a certain level of risk. ✓ ESRT Group gets together (General Council, Communications, Provost, CIO, CISO, OIS, and the affected business group). This group gets together to determine if there was a data breach. They brainstorm to come up with ideas that could have prevented this. They go through the brainstormed list to decide what is feasible and how they can approach it in the future. In the latest meeting, there were about 20-25 recommendations that were mentioned, with 2-3 high level review discussion items. Everyone at the table gets a chance to say what they think is a good recommendation ✓ An incident is not closed until these meetings occur **IMPORTANT INFORMATION ABOUT THE RECENT ATTACKS:** • These attacks are not unique to AppState. They are happening to other institutions of higher education. • The main motive of these attacks is to steal money. These are more sophisticated attacks & they are looking at all of our communications.

- The folks in the Service Desk found the most recent attacks.
- Oscar & Kevin are able to track the hackers' actions.
- Payroll is on alert to make sure that there are no changes in direct deposit
- There has been communication amongst University Police, the Chief Information Security Officer and the SBI
- The hackers are using Green Dot Cards because it is easier for them to set up and not give as much information as a bank.

NOTE: Some universities use Intranet for their forms, employee information, etc. We use the Internet, which would potentially allow hackers to download these forms and give fictitious information.
At the February 2017 meeting we will discuss using the Intranet instead of the Internet, as well as options for University communications.

UNIVERSITY COMMUNICATIONS INITIATIVE – OSCAR KNIGHT:

- Anything that comes from the Chancellor should be public
- There needs to be a webpage that validates all messages being sent out
- UNCG sends most of their university-wide messages through Google Groups to make sure that the communications are legitimate and there is a record of it

AFTER ACTION REVIEW IDEAS:

- We don't ask a lot of personal information of employees. Should we allow them to add cell phone and personal email to their profiles so that we can verify any changes made?
- If we have this type of personal information, should employees be able to opt in to this or should this be a requirement?
- Question: Would hackers be able to hack in and get the cell phone and email information? Possibly, but this will give us time to see what's going on.
- The reasons some employees may not want to share this personal information: 1) They don't want to share their personal information with their employer 2) They don't want to be charged for text messages 3) They don't want to receive multiple emails & texts.

POLICY & COMPLIANCE REPORT – OSCAR KNIGHT:

PCI-DSS Updates:

- Many schools struggle with deciding if this is a business aspect or an IT aspect. Most schools, including AppState, make this a joint venture.
- From a tech standpoint, processing credit cards with a desktop computer is problematic, so they changed it to Web POS. This has been employed with Conferences & Camps, and Parent & Family Services.
- Point-to-Point Encryption allows you to encrypt the data on the device – before it gets to your computer, it's encrypted
- PCI Validated: meets all of the PCI Council's regulations. Vendors seem to be compliant, but the gateway is not always compliant.
- The ASU Foundation is about to employ PPE.
- The Holmes Center will be using PPE as well
- Athletics will also be using PPE (currently using RFP)
- Oscar has been working on a way for the University to use the "new" technologies to keep our credit card data encrypted and the information safe. The new standards are costly upfront, but it lowers our compliance overhead.

3.0 OLD BUSINESS

SECURITY STANDARDS - APPROVAL REVIEW (Language + "Compliance Horizon":

- **Encryption Standard**:
  - Thank you to Barb Krause for looking over this standard
  - There is not a quorum today to be able to vote

- Working on a project to encrypt laptops
- The "musts" and "should" need to be clarified
- Need to be consistent within the document to make sure if it says "must" in one area, it has to say "must" in another area
- We need to get this passed so that we can have a solid accountability
- HR needs a solid measurement of accountability so employees know what is expected of them
- Some would like to see a training piece that goes with the new policies (like Securing the Human) and having a test that goes along with it to make sure the employees understand it and that there is a measurable outcome
- There is new supervisor training – it is voluntary, but it is really pushed for them to do it. This would be a good place to have this type of training.
- Some would like to see a monthly meeting across campus for supervisors where they hear about updates, new policies, etc. However, there are over 800 individuals on campus that are considered supervisors, so this would be a difficult thing to accomplish. This idea was implemented a few years ago and the meetings were hit or miss.
- Amy Roberts has the DRA Group monthly and they usually go over funds, but other groups are often brought in and asked to speak – this would be a good time for this type of training.
- David Hayler is the new Interim CIO and he is working closely with Jim Webb

SECURITY STANDARDS – ONGOING FEEDBACK:

- **Remote Access Standard** (Draft) – Feedback: Jim Webb is going to have a conversation with David Hayler on Friday, January 20, 2017 to discuss this.
- **Data Handling Standard** (Updated) – Discussion + Feedback:
  - Designation of secure data requirements
  - Each department needs to know how to handle their secure data
  - There is a list of areas that are known to handle secure data. The same set of tools needs to go to the units that have secure data.
  - The whole unit would be covered under this, rather than just certain individuals
  - Public data is web data
  - Approved storage of sensitive data is in this standard
  - Rachel Serrano has gone through to find secure information that should not be there
  - Process of Unsecured Confidential Data - Kevin Wilcox:
    - If someone has confidential data and they don't fix it in a timely manner, the Security Team then goes to the supervisor to get this done
    - The initial contact is via email. They give them a week and scan again in Identity Finder. If the confidential data is still there, the Security Team calls the employee to discuss what they might need to do to secure the data.
    - The plan for this is to go out and do direct engagement
    - A reminder that Identity Finder is being put on all computers throughout campus will be given to these individuals
    - During these conversations, the employee can talk about how data goes in and out in their department.
    - From a risk basis, the Security Team will work with one unit at a time and work throughout the year to get them all up to date on Identity Finder. This is a cleanup initiative.
  - This standard is still in the feedback stage, but this needs to get passed before the project phase can begin
  - File Locker is free, but ITS is looking at a longer term solution
  - According to Kevin Wilcox, when another institution got hit by hackers, everyone in their institution was put on Cloud Lock and they did away with other ways of sharing. As we see the way things are moving along, there is probably a possibility of seeing some ability to add more

	security to Gmail and to Drive, but at this time, that's not a possibility due to spend and human power. o Currently, Cloud Lock only covers certain seats, but can't cover the entire University. • **Acceptable Usage Policy** (On Hold): Jim Webb will be talking to David Hayler to try to reconnect to move this forward
4.0	**NEW BUSINESS**
	Email Spoofing + ITS Mail Validation - Feedback: Due to time constraints, this has been deferred to the next meeting. **OIS Monthly Newsletter – Feedback/Ideas:** • Keep it as compact as possible • Be able to click on links for more information • Don't be too repetitive, but don't be afraid to repeat things over time that are really important to us
6.0	**MEETING ADJOURNED**
	Jim Webb thanked the group and adjourned the meeting at 11:30am.