Notes from the Information Security Advisory Council

Thursday, October 9, 2014
9:00-10:00 a.m. (Room 102, Watauga River Room, PSU)

In Attendance:

Lisa Burwell, Toney Carey, Amy Carson, Justin Cervero, Laramie Combs, Laura Crandall, Ron Dubberly, Matt Dull, Jay Fenwick, Oscar Knight, Karen Main, Angie Miller, Beth Pouder, Jonathan Reeder, Kathy Roark, Norma Riddle, Amy Sanders, John Secreast, Trent Spalding, Julie Taubman, Jim Webb (chair), Wyatt Wells, Kevin Wilcox

National Cyber Security Awareness Month - Jim Webb

Jim Webb informed the group that October is National Cyber Security Awareness Month and made them aware of the presentation the security group in ITS are giving. The topics are: "Managing Your Digital Footprint", "Your Online Reputation" and "Anatomy of a Hack". He also informed the group of the security video contest for employees for security awareness.

Recent Security Events – Jim Webb

Jim mentioned two recent vulnerabilities that have affected many campuses, Heartbleed and Shellshock. Appalachian was not exploited by these recent events due to the quick response by the system administrators in departments and in ITS.

Presentation on PCI Compliance (Payment Card Industry) – Oscar Knight

Oscar Knight gave a brief presentation about the importance of PCI compliance for Appalachian and explained the how the compliance process is very complex and specific. The three largest users on campus are Athletics, the Bookstore, and Food Services.

Information Security Policy for Appalachian State University – Jim Webb

Jim showed the group the draft of the Information Security Policy, developed by the sub-committee of JJ Brown, Toney Carey, Gunther Doerr, Barbara Krause, Trent Spaulding, and Wyatt Wells.

He asked the group to look at the policy in depth and to send him any comments. After the council has approved the draft of the security policy, it will then go to various groups on campus for approval, including the faculty and staff senates, the council of chairs, the dean's council, the IT executive council for governance, and the chancellor's cabinet.

Additional Working Groups from the Security Advisory Council – Jim Webb

There are other security subjects that additional working groups need to be established for, two of these are

1. Developing a Security Awareness program for the campus.
2. Security Tool Review Team - (to be used [primarily by the other IT Governance committees as they make decisions about services and applications on campus)

Support for this Council and the other Technology Portfolio Committees – Julie Taubman

Julie Taubman informed the group of current work to help support the committees in the governance process. This includes plans for:

- A manual, or orientation guidebook, for the Technology Portfolio committees to outline roles and responsibilities, and common processes including reviewing portfolios, and making recommendations for new applications/services.
- To ensure that security and infrastructure concerns are considered when any TPC considers a new application or service, we are considering a process where committees review a list of criteria – such as:
    - Type of data utilized by the application/service -- Data classification (e.g., confidential information, etc.)
    - Mission critical: Whether the application has a considerable impact if the application/service is down for 24 hours or the data integrity/high availability is mission critical
    - Reputation impact: if a disruption of the application/service would impact the reputation
    - Storage needs, where application will reside, etc.

  These criteria could be placed in a checklist that is reviewed by a TPC when considering new services/applications, or potentially modifications to existing services/applications, to ensure that Security and Infrastructure needs are considered, and vetted.

  In September at the quarterly Chairs meeting, the Chairs of the TPCs requested that the applications/services in the Tech App + Service Catalog be placed in a database with some additional information, including type of application/service, to facilitate their reviews of their portfolios.

Data Protection Toolkit – Secure File Transfer – Jim Webb

The campus has been requesting a way to transfer files with sensitive information in a secure manner. Jim showed a demo of a program called File Locker that may be a solution. There is a small pilot group currently using this program and Jim asked for more areas to use it and give feedback.

Security Awareness Training – Jim Webb

There are online training videos covering wide topics on security called "SANS-Securing the Human". Jim will send out the credentials to the council members to review these videos and to give feedback on how these may be used to help make the campus more aware of security.

Next Meeting

The next meeting will be held on Thursday, November 20th at 9:00 am.