Information Security Workgroup
January 8, 2019
Education, Building 02, Room 024

Present:	Doug Lomsdalen, ITS	Lynne Harrington, Academic Affairs
	Troy Weipert, A&F	Rick Salomon, Student Affairs
	Craig Nelson, UD	Eumi Sprague, CPC
	Bob Crockett, CENG	Jarrod Plevel, CAFES
	Debra Valencia-Laver, CLA	Arthur Huebner, CSM
	Jon Vazquez, ITS	Gary McCrillis, ITS
	Jeff Nadel, CENG	
Absent:	James Mwangi, CAED	Derek Gragson, CSM
	Kelley Sebastian, Office of the President	Kristy Cutter, OCOB
	Richard Cavaletto, CAFES	

I. OS/Security End-of-Life Updates

January 14, 2020: Win7/Windows Server 2008/R2
January 2020: Major browser support for TSL 1.0 & 1.1
November 20, 2020: RedHat/CentOS 6.X

Significant work has been accomplished. For remaining devices, fill out exception request to request permission for system to remain on the Cal Poly network. Doug Lomsdalen provided details of the information requested for the exception request process.

II. KeyServer Update

KeyServer is a comprehensive tool helping with asset and software inventory. Doug Lomsdalen provided an overview and a detailed handout of its capabilities in terms of reporting. Craig Schultz will establish user accounts for ISCs (or delegate).

III. 2020 Annual Risk Self-Assessment (ARSA) Focus

Gary McCrillis highlighted focus areas for the 2020 ARSA. This year's focus is centered around Center for Internet Security (CIS) Controls:

a. Inventory of Hardware Assets
b. Inventory of Software Assets
c. Continuous Vulnerability Management
d. Maintenance, Monitoring and Analysis of Audit Logs
e. Malware Defenses

During 2019 ARSA, we saw a disconnect between the number of devices reported by the divisions and colleges and the numbers the ISO team sees in Qualys, Sophos and KeyServer.

IV. 2019 Information Communication and Technology (ICT) Stats

Doug and Gary provided an overview of ICT stats from 2019; it was a busy year with the review of 324 ICT submissions. The majority of the submissions were for software and web-based products. Approximately 10% of the submissions processed/stored Level 1 data.

V. Security Projects

a. Cloud Access Security Broker (CASB)
Doug provided an overview of the work being done with CASB, highlighting when the service is fully operational, we will be able to open OneDrive up for external sharing.

b. Splunk
Jon Vazquez spoke briefly on our recent acquisition of Splunk and how the ISO team is moving from the Logging project of last quarter to ingesting the data in order to more proactively monitor activity on the network.

c. Email Security
Doug identified a variety of security controls the ISO team is advocating for implementation to improve the security posture of our email system.

VI. Action Items

Doug Lomsdalen: Provide SHI info for Extended Server Support.
Doug Lomsdalen: Follow-up with potential for patching through SCCM/JAMF.
Craig Schultz: Can updates be made within KeyServer (e.g., drop devices)?
Doug Lomsdalen: Hold a meeting to discuss strategies to "stop" use of links in emails.
Jon Vazquez: Research other email application options when legacy protocols are disabled.

VII. Next Meeting

a. April 8, 2020, 1:00 pm – 2:00 pm, Bldg 02 / Room 024