Information Security Workgroup
April 8, 2021
Zoom Session

Present:	Rick Salomon, Student Affairs	Lynne Harrington, EMIS
	Kelly Sebastian, Office of the President	Bill Leddy, A&F
	Kristy Cutter, OCOB	Joe Emenaker, OCOB
	Bill Hendricks, CAFES	Jarrod Plevel, CAFES
	Arthur Heubner, CSM	James Mwangi, CAED
	Josh Machamer, CLA	David S. Bains, CPC
	Craig Nelson, UD	Trish Brock, R-EDGE
	Joan Pedersen	Doug Lomsdalen, ITS
	Brandon Goddard, CENG	Kyle Gustafson, ITS
	Jon Vazquez, ITS	Gary McCrillis, ITS
Absent:	Derek Gragson, CSM	Robert Crockett, CENG
	Troy Weipert, A&F	

I. 2021 Annual Risk Self-Assessment (ARSA)

Per CSU Policy (8020) we are required to conduct an annual risk assessment; we accomplish this task via the Annual Risk Self-Assessment. This year, we're significantly reducing the requirements from each College and Division; focusing on just the completion of the questionnaire.

The goal of the annual assessment is to improve asset inventory, correlate use of security tools and improve the ARSA process.

The "kick-off" letter with instructions will be sent the week of April 4th; responses are due May 28th.

II. Update: Multi-factor Authentication (MFA)

We enabled MFA, on web-based applications, on December 9, 2020. We currently have 38.2K users enrolled in Duo. It was asked of us to extend MFA Remember Me to 30 days; since the change, we have reduced authentications by 50%. We also enabled Bring your Own Security key and TouchID; providing users more options for authenticating (and reducing the need for a mobile device).

a. Up Next:
   i. Emeritus (Summer/Early Fall 2021)
   ii. Department Accounts (TBD)
   iii. Admin Accounts (TBD)

III. CSU CO InfoSec Audit Update

The information security audit is still ongoing; the CSU requested more evidence this week. The Information Security team is working with the appropriate office to collect the data.

We recently increased the amount of data we can ingest into Splunk security tool, we're working with departments to get high-risk workstations added. Adding the high-risk workstations will remediate one of our audit findings.

IV. CSU Cyber Hygiene Project

A CSU campus suffered a disruptive breach, significantly disrupting operations by impacting their Domain Controllers/Active Directory. The end game of the malicious actors was to obtain sensitive data to hold for ransom.

The CSU Chancellor's Office directed each campus to assess and enhance five primary areas:

a. Active Directory
b. Securing Network and Remote Access
c. Domain Controller and System Hardening
d. System Logging and Monitoring Tools
e. User Account Security

The ITS Information Security Office worked with a variety of campus entities to remediate many of the issues identified. We've developed projects for the remaining work and seeking ITS leadership approval on recommended architecture configuration.

V. **Segment Tech Park Network**

For years, the tenants of the Tech Park have been on the Cal Poly network; this project will segment them in their own area of the network and unable to affect any of our Cal Poly network resources. Work by ITS is slated to be complete by mid-April.

VI. Action Items

ISO: Send Annual Risk Self-Assessment Kick-Off letter to ISCs.

VII. Next Meeting

a. July 8, 2021, 1:10 pm – 2:00 pm, via Zoom