Information Security Workgroup
July 8, 2020
Zoom Session

Present:	Doug Lomsdalen, ITS	Lynne Harrington, Academic Affairs
	Troy Weipert, A&F	Arthur Heubner, CSM
	Robert Crockett, CENG	Joe Emenaker, OCOB
	Kristy Cutter, OCOB	Jarrod Plevel, CAFES
	Craig Nelson, UD	James Mwangi, CAED
	Rick Salomon, Student Affairs	Jarrod Plevel, CAFES
	Jeff Nadel, CENG	Andrea Burns, CPC
	Debra Valencia-Laver, CLA	David S. Bains, CPC
	Kyle Gustafson, ITS	Brian Gautry, CPC
	Jon Vazquez, ITS	Sarah Jones, ITS
	Craig Schultz, ITS	
Absent:	Richard Cavaletto, CAFES	Derek Gragson, CSM
	Kelly Sebastian, Office of the President	Gary McCrillis, ITS

I. 2020 Annual Risk Self-Assessment (ARSA)

The 2020 ARSA officially closed June 26th; thank you to those who have submitted their ARSA Questionnaire and Server worksheets. For those areas who haven't submitted, don't fret, we're still accepting them. We also are looking forward to the improved security posture of the campus as our security tools are deployed enterprise-wide.

a. Doug Lomsdalen reported workstation survey submissions were lower than expected, he will provide a report by College/Division.
b. This summer Gary McCrillis will be reviewing submissions and compiling data and reports.
c. Final report will be issued by 9/25/2020 and we'll present roll-up info at our October ISC meeting.

II. Multi-factor Authentication (MFA)

ITS kicked off an MFA project July 1st; ITS will be enabling MFA at the person level for most person-types. When individuals log in via SSO, they will be prompted to authenticate through Duo. We'll be adding this extra layer of security to protect critical Cal Poly data and resources.

a. Person types impacted:
    i. Faculty / Staff / Students (admitted, current, recent) / Affiliates
    ii. Phase II: Emeritus
b. ITS ISO/MARCOM will draft communication for Divisions/Colleges to ask users to sign up early.
c. ITS ISO will work with Cal Poly Human Resources and Academic Personnel to ensure communication trickles down to respective unions.

III. ICT Dashboard / Status Check

To fill a need and meet a CSU Accessible Technology Initiative, Craig Schultz put together the ICT Dashboards. The ICT Dashboards are one-stop shop to review the status of an ICT submission, identify what ICTs are coming due (based on trigger info), and general search capability for products in use. If an ICT (formerly E&IT) has been accomplished since 2015; it can be found in these dashboards.

a. Craig provided a demo of the dashboards; showing how users can navigate to check on the status of "in-progress" ICTs; Renewal lists (month/annual views); and completed reviews.
b. Cal Poly is working with Survey Gizmo to seek a feature update to address the password issue we experience.
c. Previewed the new "short form" ICT Review.

IV. Security Tidbits

Remote work has proven to be a challenge on many fronts, and has definitely garnered the attention of the Information Security Office. We've been diligently watching logs to identify anomalies and indicators of compromised. We're proud of our user-base; June had our lowest number of compromised accounts in 15 months!

a. Remote Work Environment
    i. In partnership with Splunk, they upped our ingest rate and configured "out-of-the box" dashboards to track remote work stats (e.g., Cal Poly Global Protect VPN and Zoom).
    ii. Our goal is to improve logging to allow us more detailed reporting for security response.

b. Splunk
    i. We're enabling more and more features of Splunk's Enterprise Security; currently implemented are phished accounts and malware alerts.
    ii. The team is currently working on developing automated response to a variety of alerts identified; the ISO team will work with stakeholders on the appropriate business process to work through a variety of alerts (e.g., ticketing, emails, …).

c. WAF Reverse Proxy
    i. WAF: Web Application Firewall.
    ii. We currently use Signal Sciences' agents on our Drupal environment. To simplify the implementation of WAF features (without the agent) the security team is working on creating a Reverse Proxy.
    iii. Our goal is to start implementing the WAF Reverse Proxy starting in the Fall Quarter. It will be a slow and methodical approach, starting with test cases and roll out.

V. Action Items

Doug: Provide a workstation survey summary by Division/College
Doug: Work with ITS MARCOM to draft initial language around MFA for Division/Colleges
Doug: Ensure MFA (Duo Security) communication goes out to Cal Poly HR/Academic Personnel for unions
Kyle G: Reach out to Student Affairs regarding enabling WAF on sensitive servers/apps.

VI. Next Meeting

a. October 7, 2020, 1:10 pm – 2:00 pm, Bldg 02 / Room 024 or via Zoom