PROGRESS REPORT

Working Group Name: Cybersecurity

Working Group #: 37

Chair: Ed Pierson

Date: April 20, 2022

Update on Actions Taken Since Last Report:

The Working Group continues to meet as a collective team. We have divided up into 4 sub teams.

- Sub Team 1 – Identify the key Identity and Access tools and policies. The Identity and Access sub team was tasked to provide recommendations to ensure that Cybersecurity remains a top priority as it relates to Identity and Access. Sub team members recognized that significant effort and progress has recently been made toward improving Identity and Access Management (IAM) by IAM experts in TAMU Security with partnerships from across campus via working groups, and nationally recognized consultants that assessed and evaluated our current state in depth, conducted many interviews, and ultimately mapped out the exact steps needed.
- Sub Team 2 – Identify the device policies that are needed to better secure them.
    - Implementation of a centralized endpoint services request process for both physical and virtual servers and related services whether located on campus or in the cloud.
    - Standardize on a modern and centralized IT asset management system.
    - Standardized on a set of effective and centrally managed tools.
- Sub Team 3 – Identify the security services needed by Research customers.
    - Creation of a small team of Cybersecurity/IT Risk Management professionals dedicated to ensuring Texas A&M University retains and increases its grant competitiveness.
    - Research Information Security Working Group or Task Force placed under the current IT Governance structure, aimed at continuously gathering feedback from researchers, keeping a finger on the pulse of research and researcher security needs, and pipelining that information towards the creation of new useful and improved tools, processes, and resources for researchers.
- Sub Team 4 – Identify the security services needed by our applications. Create a Secure SDLC program consisting of the following elements:
    - Identify and procure Secure-SDLC enterprise level tools. Without these tools it is not possible to ensure Secure development or assess the state of security of applications and software, at scale. Such tools are not cost prohibitive but are vital to this program.
    - Employ Product Security or Application Security experts who will not only run the program but also work collaboratively with university Application Developers to ensure the program is successful.
    - Create and maintain a comprehensive secure-development training program. This training program will be co-developed by Application Security experts and Senior

Application Developers to ensure it adequately addresses all aspects of the secure-SDLC.
    - This program will **include a well-defined process and pipeline** for enterprise application and software assessment and secure-development.

Next Major Issue to be Addressed:

Each of the sub teams are meeting 1-2 times per week and doing a report out to the main working group. We expect most of the sub team reports to be ready for review by the main group by the end of April. Once the sub team reports are completed, we will write up an executive summary report and submit all 5 documents for review by the SIC.

Problems or Barriers Encountered and Solutions Identified:

Shortages of staffing within the IT teams will limit the availability of staff to build the new infrastructure needed to consolidate services.

Deliverables Completed:

In process but not completed.

Timeline for Completion of Remaining Deliverables:

- Identify the identity and access programs that will better support the organization: April 29th
- Identify the best practices and policies needed to support the incredible range of devices in use at TAMU: April 29th
- Identify the security services needed to better support our research efforts: April 29th
- Identify the security systems needed to ensure proper Application security in both internally developed software and purchased products: April 29th