CSU CCC UC

THE CALIFORNIA STATE UNIVERSITY

ALIGNING CYBER SECURITY ACROSS THE CSU

FOCUS ON EFFICIENCY

The Information Security team in the CSU Chancellor’s Office is leading a successful program across all 23 campuses to enhance cyber security by better assessing risk and evaluating program maturity.

California State University has been challenged for years in strategically aligning cyber security across its 23 geographically and programmatically diverse campuses.

Campus information security teams are largely responsive and tactical in countering threats and implementing solutions, but among the major challenges for these teams is inventorying sensitive data and determining a consistent method to assess risk and evaluate program maturity (a continuous measurement of the systems’ weaknesses and strengths).

Beginning in spring 2018, the CSU Chancellor’s Office Information Security team led a systemwide effort to inventory data and implement the EDUCAUSE Higher Education Information Security self-assessment tool across the CSU.

The initiative culminated in July 2019, and the CSU now has a means to quantify and prioritize risk aligned with the ISO 27001 framework (the standards set forth by the International Organization of Standards). These efforts increase efficiency and reduce cost and risk by enabling campuses to identify and focus on the most pressing cyber security concerns in a consistent manner across the CSU system.

MILESTONES

May 2018	• Project commences.
Dec 2018	• Initial status of inventory and initial Higher Education Information Security Council (HEISC) tool is completed.
Apr 2019	• Inventory status report, update of HEISC tool and identification of risks are completed.
July 2019	• Inventory, final updates to HEISC tool, risk mitigation and treatment plans are finalized.
Oct 2019	• Strategic risks based on findings are prioritized.
Nov 2019	• Campus chief information officers and International Standards Organization discuss prioritization of findings.
Dec 2019	• Cyber security State of the Union report is prepared for the CSU Chancellor from results of the systemwide strategic plan.

QUANTIFICATION AND RESULTS

Previously, approaches to inventorying sensitive data were not standardized and ad hoc. There is now a standardized approach to assessing the security program maturity at each campus and across the CSU collectively. A procedure is also in place to ensure systemwide adherence to the ISO 27001:2013 standard: Each university tracks via a Demming model score (a “plan, do, check, act” process improvement cycle) for its maturity of ISO 9 (access control standard) against the collective score for all CSU campuses: In May 2018 (the collective CSU score was 2.94; the mid-project score was 3.07; and the final score was 2.85). This is replicated for all 15 domains (the various cyber security spheres, such as security management, business continuity and compliance) for ISO 27001:2013 and may be used within each campus to assess against each college.

IMPACT AND BENEFITS

The project provided a systemwide analysis of security programs across all 23 campuses and the Chancellor’s Office with a numerical score in each of the 15 domains. Each campus now has an individual score and a collective system score to see where the campus stands in contrast to the overall system. The numerical score allows for assessment of areas of greatest risk and least maturity. As a result, campus security teams may focus on specific areas to reduce risk and cost, and increase program efficiency.

PROJECT TEAM

Michael Berman
Chief Information Officer,
CSU Chancellor’s Office

Ed Hudson
CSU Chief Information Security Officer

Leslie DeCato
CSU Application Security Manager

Kyle Westmoreland
Information Security Analyst,
CSU Chancellor’s Office

Mark Mason
Senior Security Analyst,
CSU Chancellor’s Office

Allen Le
Security Architect,
CSU Chancellor’s Office

Chief information officers and information security officers in each of the 23 CSU campuses

LESSONS LEARNED

1 Each campus interpreted the Demming model scores differently, so additional efforts were needed for consistent evaluation across the system.

2 Inventory efforts varied across each campus and across each platform (desktops, servers, applications, cloud storage, etc.); therefore, it was necessary to focus on continual improvement tailored to specific areas of the most risk.

The California State University
California Community Colleges
California Higher Education Collaborative
University of California
CSU

The Chancellor's Office Information Security team receives the Focus on Efficiency award.

FURTHER REFERENCES

EDUCAUSE Information Security Program Assessment Tool: https://library.educause.edu/resources/2015/11/information-security-program-assessment-tool

EDUCAUSE Higher Education Community Vendor Assessment Toolkit: https://library.educause.edu/resources/2016/10/higher-education-community-vendor-assessment-toolkit