The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

LOCATION:
Northridge, CA, US

YEAR:
2011

STATUS:
Laureate

CATEGORY:
Safety & Security

ORGANIZATION:
California State University Northridge

ORGANIZATION URL:
http://www.csun.edu/

PROJECT NAME:
Virtual Information Security Center

PROJECT OVERVIEW
The Virtual Information Security Center (VISC) is a transformation approach to providing a set of information security services for participating campuses that were historically provided by the campus' Information Security Officer and staff, including information security risk management, incident management, standard/procedure development, monitoring, and information security product evaluation. The VISC focuses primarily on security services (incident management, operational activities, and security projects) that can be highly standardized across campuses, delivered remotely and which lend themselves to economies of scale and which mitigate the greatest risk to the CSU campuses. Once fully operational, the Virtual Information Security Center (VISC) will be an integral part of participating campus' information security programs. The VISC will operate virtually; its staffing will remain resident on multiple campuses and VISC services will be delivered remotely using applications and tools to perform campus scanning and identify vulnerabilities using remote forensics tools. In addition, an online learning system is being used to deliver security awareness training. During the four month pilot, service offerings were limited and no full-time staffing was deployed to the Center. Once fully operational, the VISC will be led by a full-time ISO familiar with information security policies and practices. The Director will be responsible for day-to-day operations for the Center, including the supervision of information security analysts. The VISC Director will be hired by the Center Governance Committee. Security analysts will be initially contributed to the Center by member campuses. The VISC will provide three general types of services: • Incident management - The Center will offer incident management services that assist campuses to establish standard procedures for responding to a significant information security breach. Should a breach occur, the Center will aid campuses by gathering information, conducting forensic investigation, and other activities needed to understand the extent of the breach, its causes and the steps required to remediate vulnerabilities. • Operational activities – The bulk of the Center's routine services will focus on monitoring the usage of participating campus networks and systems to detect unauthorized access and potential vulnerabilities.

Tasks will include the review and assessment of security logs and system generated alerts. • Information Security Projects – Center staff will also undertake research and development projects such as reviewing security tools or products such as encryption and technology, developing security standards, analyzing the operational implications of a policy change, assisting with audit responses and remediation activities, and coordinating campuses' participation in system-wide projects that impact security. Campus responsibilities will include delivering in-person training and communications (leveraging where possible materials developed at the VISC), advising units on maintaining physical security of information assets and managing the deployment of new security technologies that cannot be deployed remotely. Guidance for these activities will be provided by the VISC. Many of the challenges associate with the VISC are because it is a new model of service delivery. Challenges included working in disperse geographical locations, agreeing upon a consistent set of information security services, managing governance, and developing a funding model.

SOCIETAL BENEFITS

The benefit of VISC is the design of the service model, which can be replicated and utilized by other constituents, outside businesses, and other business partners. It is an innovative approach to offering information security services, which can be applied to other shared services.

PROJECT BENEFIT EXAMPLE

"Today, the security center offers a full range of services, including risk assessment, policy implementation, incident management and vulnerability scanning. It has been so successful that we eliminated an IT management position at California State University, Northridge, and allocated those dollars to other projects." – Hilary J. Baker Baker, Hilary J. "Working It Out Together." EDTECH Magazine. Feb. 2011. http://www.edtechmag.com/higher/updates/working-it-out-together.html

IS THIS PROJECT AN INNOVATION, BEST PRACTICE? Yes