Case Study
Organization Security Program for Higher Education

Client

Nationally Recognized Private University

This nationally recognized private university (the University) offers undergraduate, graduate, and doctoral programs. It has an undergraduate enrollment of about 4,500 students and graduate enrollment of more than 2,000.

Challenge	CBTS solution	Results
• The University has a diverse network that supports multiple devices used by students, faculty, staff and guests • The University needs to meet federal compliance to protect financial and personal information • The University requires a secure network with various tiers of wireless access that allows access to internal applications, services and data storage	• CBTS conducted a wide-ranging security assessment • CBTS created a security road map with a prioritized list of recommended initiatives • CBTS was engaged in constant reviewing and consulting on the University's security posture • CBTS made continual recommendations to improve the University's overall security strategy	• The University has grown their security capabilities • The University has a security strategy in place • Students, faculty, staff, their computing assets, and data are much better protected • Peace of mind for their leadership team

Business Challenges

The University is the home and center of learning for thousands of undergraduate and postgraduate students, and the employer for hundreds of faculty and staff. The IT organization operates the internal network, which serves students, faculty, and staff. The team is trusted by students, faculty, and staff to protect their personal and financial information, and to ensure their assets are safe – and not targeted by attackers - while connected to the University network.

The University's network is quite diverse. An Internet-facing presence serves visitors, students, faculty, and staff with applications and services. Students, faculty, and guests also access the Internet through the University network via various tiers of wireless access, as well as computer labs and office/classroom connectivity. Finally, a protected network segment for faculty and staff allows access to internal applications, services, and data storage.

Risk priorities are designated by leadership, concerned about loss of financial and personal information, research, and public confidence due to a breach. Mitigation of these risks is ultimately the responsibility of the security program. Compliance with federal regulations such as FERPA is also covered by this team.

The University needed to ensure their security program was capable of meeting these requirements. What policies need to be in place to govern the behavior of all users of the network? What processes make up the operational rhythm of the security team? What technical controls and defenses provide protection and visibility? What metrics should be used to measure the effectiveness of the program?

CBTS and the University had worked together on several other IT projects, including deployment of network and server technologies, and due to the success of these projects, the University selected the CBTS Security Services team of consultants to help understand and improve their security posture.

CBTS solution

CBTS worked with the University to plan a wide-ranging security assessment. Using widely accepted security standards such as ISO27000 and the Center for Internet Security's Critical Security Controls, CBTS evaluated the program in place at the University. A more tactical view of security risk present in the network was provided by a vulnerability assessment, focused on the University's server and network infrastructure population.

This set of assessments produced a roadmap, with a prioritized list of recommended initiatives for the coming years that would improve the organization's security posture. The University committed to enacting as many of these recommendations as possible in three years. Within the first year, an information security officer (ISO) was hired to oversee execution of the initiatives recommended by CBTS.

Three years later, the University had progressed significantly. The network looked much different, with the presence of new security controls protecting critical data stores and applications. Policies that addressed a number of areas have been established, providing guidance to users around data handling, elevated privileges, and internet use. Wishing to continue growth, CBTS was engaged once again to review the state of the security program.

CBTS solution (continued)

As a security expert, CBTS invests heavily in keeping up with the threat landscape that is changing constantly and substantially every day. Our team understands new vulnerabilities, malware families, and attack vectors, as well as security technologies that have entered the market to combat these threats. The CBTS Security Services team supports the University's security program year-round with current knowledge and expertise to help them mitigate their organizational risk.

CBTS assessed the security program and architecture at the University, discovered gaps, and provided new recommendations on the next phase of growth. CBTS was also asked to evolve its tactical assessment of vulnerabilities, this time with a penetration test. First, CBTS crafted a simulated phishing attack against the University's staff in an attempt to gain access to the protected internal network. Using this access, CBTS simulated a network-based attack against internal assets, with the goal of locating and stealing sensitive data.

A new set of findings reports and a new roadmap were presented to the University's security team. CBTS continues to strengthen the University's security posture in this long-term strategic partnership.

Products and Standards Used

- Tenable's Nessus
- Rapid7's Metasploit Pro
- Center for Internet Security's Critical Security Controls
- International Standards Organization's ISO27000 Series

CBTS Engineers and Consultants Deployed on the Project

- An Account Manager
- A Senior Security Architect
- A Security Engineer
- A Service Delivery Manager

Results

The University has grown in its capabilities and has a strategy for continued growth. Students, faculty, staff, their computing assets, and their data are better protected. Risk is more effectively managed. The University's CIO along with their leadership and trustees are able to rest easier knowing the security program is mature and functioning well.