Ensuring compliance and cybersecurity resilience

Introduction

Founded several decades ago, a Midwest university had earned a worldwide reputation for offering excellence in academic leadership underscored by a rich heritage and challenging curriculum. Aided by contributions from a diverse faculty, staff, students, parents, and donors, the university had grown from a handful of original structures and a few hundred students to a thriving campus with two dozen buildings, several thousand students, and tens of thousands of alumni.

Ensuring that thousands of students, faculty, and alumni remain safe and secure to continue their educational and professional endeavors...

The university is responsible for protecting a vast amount of sensitive Personally Identifiable Information (PII) for all these individuals, such as social security numbers and financial details. They must also comply with several compliance mandates, including the Gramm-Leach-Bliley Act (GLBA) of 1999 that requires organizations acting as financial institutions to enlist adequate cybersecurity measures to properly safeguard PII. The university offers financial aid services, which requires frequent auditing for GLBA and other mandates by a professional compliance firm.

Challenges

The global pandemic has escalated security concerns for nearly all organizations. According to leading industry analysts such as Ponemon Institute and IDC, a cybersecurity attack now occurs every eleven seconds. Attackers are far more sophisticated and employ a variety of advanced techniques to penetrate a firm and cause damage.

CENETRIC

CASE STUDY

A cybersecurity attack now occurs every 11 seconds...

Increases in remote work and eLearning educational courses has expanded the use of Remote Desktop Protocol (RDP), and brute force RDP attacks are now the number one way ransomware is perpetrated. Higher education was hit with over 20,000 such attacks in 2020, and the average ransom now exceeds $250,000. Moreover, cybercriminals are no longer content with encrypting information and holding it hostage. They now threaten to expose PII and other sensitive data, which could cause serious reputational damage and violate GLBA and other compliance requirements.

The IT director at the university had installed several state-of-the-art security appliances and applications, but he had not yet fully updated the organization's security posture and Written Information Security Policies (WISP) to deal with escalating post-pandemic threats. Several of the university's departments were independently managing and maintaining their own applications, separate from the rest of the university and IT department. The university had also not completed a more recent and formal assessment of their network security and compliance levels. Lacking more up to date policies, practices, and information placed the university at risk for compliance violations, ransomware threats, and malicious malware attacks.

Solutions

The IT director contacted the experts at Cenetric Network Services to ensure GLBA compliance for an upcoming audit, and to improve the university's overall security posture. A leading managed network and security services provider in the Midwest, Cenetric offers support for businesses ranging from small teams to large enterprise firms. Cenetric's team has earned an excellent reputation for offering 24/7 managed services.

With over 200 industry certifications, Cenetric brings to bear a wealth of knowledge and expertise, which has resulted in a 99.98% customer satisfaction rating. Cenetric met with the university's IT director and the heads of over a dozen departments to analyze core applications, security provisions, data retention policies, and user access levels. Cenetric generated a comprehensive WISP that identified twenty-five core security categories and eighty-three policies with underlying controls. The WISP was compliant with the National Institute of Standards and Technology (NIST) 800-171 guidelines. The Cenetric team then evaluated potential risks for twenty-one distinct natural and man-made disasters including fires, floods, tornadoes, civil unrest, and pandemic related areas. They analyzed 111 security controls and twenty-two critical applications for potential failure points and provided the university with sixty-five action items with detailed steps and implementations to ensure full compliance.

Based on the initial analyses, the Cenetric team installed a network auditing appliance to monitor and log activity across almost one hundred servers, a core Enterprise Resource Planning (ERP) system, and Microsoft Active Directory with more than 15,000 objects in the university's Office 365 environment.

Results

The university was extremely satisfied with the results delivered by Cenetric. They passed the GLBA audit conducted by an outside independent agency with "flying colors" and no negative findings. Today, with more effective and thorough security policies and systems in place, the university has far less risk and fewer concerns related to ransomware, malware, and compliance failures. With Cenetric's continued assistance, the university can now focus on incremental changes and updates to maintain compliance while continuing to improve cybersecurity at a comfortable and affordable pace. This ensures that thousands of students, faculty, and alumni remain safe and secure to continue their educational and professional endeavors.

CENETRIC

Cenetric Network Services, Inc.
401 South Clairborne Road, Suite 200
Olathe, KS 66062 (913) 210-1950
www.cenetric.com info@cenetric.com