Major University Achieves Sustainable GLBA Compliance Program

Note: CampusGuard is complying with this university's policy for not appearing to publically endorse a particular product or business and therefore all references are presented anonymously.

A leading land grant university with multiple campuses, this major land grant institution with an enrollment of nearly 30,000 students is distinguished as R1 by Carnegie Classification of Institutions of Higher Education, the highest research category for an institution. The university conducts a variety of educational, administrative, research and outreach activities, and is subject to compliance with multiple regulations.

Developed initially for financial institutions, the Gramm-Leach-Bliley Act (GLBA) was enacted to protect consumer financial privacy and limit disclosure of their non-public personal information (NPI). GLBA defines financial institutions as businesses that offer financial products and services. Although the university is primarily an educational institution, it is significantly engaged in brokering and servicing loans to its students. Therefore, it meets the definition of a financial institution under GLBA and is responsible for implementing appropriate controls to safeguard NPI associated with those activities.

Challenge

Compliance is a complex and time-consuming process, especially in an institution with multiple campuses across the state. The university's information technology services department coordinates all elements of the information security program and works closely with multiple campus stakeholders to identify the nature of activities that may be in scope for compliance. The Chief Information Security Officer is responsible for not only protecting sensitive and private information of students, faculty and staff, but also for considering what might be on the horizon for compliance. Even though the university had not received notice of an impending audit, "I knew the day would come when we would be asked what we have done for GLBA compliance," said the CISO.

GLBA guidelines require that the university implement a comprehensive written information security program that includes administrative, technical and physical safeguards to protect information collected in the brokering and servicing of student loans. The university needed a formal evaluation to demonstrate its effectiveness in assessing risk, and once risk is estimated, take action to manage identified risk elements.

For more than ten years CampusGuard has been focused on the complex information security needs of higher education and, even more importantly, the implications of compliance with the myriad requirements of government agencies and industry sectors. The university had previously engaged CampusGuard for PCI DSS compliance, resulting in a mature program and partnership that includes an annual support agreement. When CampusGuard's Customer Relationship Manager suggested they could take advantage of the program to work on GLBA compliance, the university readily agreed. "Because of our prior experience with CampusGuard we knew their approach, and what the deliverables would be. I took them up on it," explained the CISO, "because I knew that sooner or later someone would be auditing our compliance."

Approach

CampusGuard staffed the project with a Customer Advocate Team comprised of the Security Advisor and Customer Relationship Manager who had previously supported the university's PCI compliance, continuing the close partnership. This team organized an interactive approach to align timelines, maintain a responsive stream of communication and ensure smooth coordination over the course of the assessment. With the right team in place, and a solid communication plan, the groundwork

CAMPUSGUARD®

was established for the assessment and follow-up activities.

CampusGuard conducted the GLBA risk assessment and analysis against the requirements of NIST Special Publication 800-171, a key criterion of the university. "My one request was that CampusGuard's findings would be delivered cross-referenced against the NIST SP 800-171 framework," explained the CISO. The university had previously made the strategic decision to start working towards being NIST SP 800-171 compliant. All compliance audits are cross-referenced to 800-171 controls.

The Assistant Director of Governance, Risk and Compliance (GRC), led the efforts to prioritize activities and develop remediation plans. One of the key objectives was to define the scope of GLBA compliance and document where NPI was collected. "We needed to understand where to focus our efforts by identifying the specific activities we conduct that are in scope of GLBA compliance," explained the Director. Through this approach, the university and CampusGuard determined that Student Financial Services would be the primary focus. Even though other departments may be collecting student NPI, it is not for the purpose of facilitating student loans.

Results

After conducting on-campus interviews and reviewing relevant documentation, CampusGuard delivered a comprehensive report identifying the greatest risks to the institution and where initial remediation efforts should be focused. A second section detailed findings of risks that were found across multiple departments, and the third provided a breakdown for each department so a more focused approach could be applied where necessary. As a final deliverable, CampusGuard provided an executive-level scorecard highlighting overall results and interpreted gaps in relevant terms for the university's executive leadership team.

"The report and recommendations CampusGuard provided have allowed us to achieve that objective and enabled the university to assure that sensitive student information is protected."

An Executive Steering Committee assigned a project manager to coordinate activities between the multiple university groups participating. The initial goals were to identify findings that could be remediated quickly, as well as to establish a plan for sustainable operations of a GLBA compliance program. Over the course of a few months, approximately a third of the assessment findings were remediated, and another half are in flight. An unanticipated result was establishing better communications between information technology and business offices. Instead of dictating activities to them, GRC developed a partnership with Student Financial Services and worked together to achieve compliance with minimal disruption to business operations.

The recommended remediation strategies provided by CampusGuard enabled the Steering Committee to make decisions about security-related initiatives to accept, reduce or eliminate risks. They also support long-term strategic risk management activities to ensure the protection of NPI.

Awesome Coincidence

The university had planned for a federal audit, but it came from an unexpected direction. Soon after the assessment was completed and CampusGuard had delivered its report, the state auditor's office announced plans to audit all higher education institutions for GLBA compliance. "We had the CampusGuard assessment, and the state accepted it without question as documentation of our progress toward compliance," said the CISO. "Sometimes an idea just works out perfectly." The university was the only state institution to pass the security section of the audit, in part due to the GLBA assessment that CampusGuard had performed.

Going Forward

The goal of the initiative was to provide an assessment that helps the university's information technology department understand activities that come under GLBA and provide direction for identifying, qualifying and mitigating risks in collecting NPI. "The report and recommendations CampusGuard provided have allowed the university to achieve that objective and enabled the university to assure that sensitive student information is protected," explained the Director.

Information technology services uses a comprehensive Governance Risk and Compliance system to analyze what is needed to address and prioritize activities and continues to collaborate with CampusGuard to review progress on areas identified for remediation. "By combining CampusGuard's assessment with our existing compliance tools and initiatives, we have reduced the scope, risk and expenses related to GLBA, and we are progressing rapidly to full GLBA compliance while also meeting state requirements," added the CISO.