CASE STUDY

SYSTEMSOFT TECHNOLOGIES™

Security Risk Assesment

STATE COMMUNITY COLLEGE

"System Soft is a high-value partner, providing critical services, insight and leadership in areas where we previously struggled." -Amy S.

Digital environments are an embedded part of any higher education institution. So, it's important to protect student data, faculty data and research data through regular security risk assessments. And do so while allowing space for effective collaboration.

However, cyber attackers constantly adjust their tactics at an alarming pace to combat any kind of vulnerability assessment. This keeps college and university chief information security officers (CISOs) and their security teams on high alert. These security experts face serious expectations from senior academic and administrative leadership to develop and support a sound cyber risk and governance regime.

System Soft Technologies helps colleges and universities become more diligent and deliberate in being secure and resilient. This is carried out through security threat assessments and vulnerability assessments, which focus on policies and controls to prevent the compromise of their most risk-sensitive assets and operations.

Here's a case study about how a state community college assessed the security posture of its applications, network and information systems. The results strengthened its cyber security posture and delivered remediation guidance for federal compliance.

Situation

A state community college acquired System Soft's security risk assessment expertise and services to assess the security posture of its applications, college network and Colleague Information System (CIS). The goal was to ensure the protection of student data and to identify and prioritize vulnerabilities, strengthening its cyber security posture. **As part of this audit, the community college required a detailed security threat assessment and reporting of:**

- Application, system and network vulnerabilities
- Gaps in IT security governance
- Patching methods
- Current network security capabilities and potential existing security incidents based on NIST 800-53 Moderate Security Controls limited to the NIST sections and subsections of Access Controls, Incident Response, System and Information Integrity
- Flaw remediation

Strategy

System Soft evaluated external and internally accessible systems, hosts and applications within each college environment. **The following security risk assessments were provided:**

- Application, system and network vulnerabilities, with an evaluation of current patching methods.

- Existing network infrastructure and configuration, including all interconnectivity and supported protocols and network services offered.
- Publicly available information and data accessible through the community college websites.
- Gaps in IT security governance, with recommendations for an incident management plan.
- Current vulnerabilities and evaluation of the current patching process, with recommendations for best practices.
- Existing security systems and components, including antivirus, firewalls and network monitoring, along with their effectiveness to prevent cyber attacks, data loss and misuse of IT resources.

The System Soft Security Team used the following security risk assessment methods:

- NIST 800-53 Rev 4 Moderate Controls Assessment to evaluate the community college'scyber security posture against the NIST 800-52 Rev 4 Moderate Security Controls.
- Operating System Security Assessment (OSSA) to assesses the configuration of a select host operating system (OS) against standardized configuration baselines, such as Security Technical Implementation Guides (STIGS).
- Network Penetration (PEN) testing to assess defenses against real-world attacks to gain system access or obtain sensitive information.
- External Penetration (PEN) testing to assess externally facing assets.
- Active Information Gathering to test public-facing systems, using manual methods and commercial scanning tools.
- Attack testing to exploit found vulnerabilities to gain system access and/or sensitive information.

System Soft supplied detailed reports on application and network key findings. Recommendations for mitigation best practices were also provided.

In addition, the team delivered remediation guidance and aided the community college in developing and executing an information security plan. This plan gave responsiveness and flexibility in managing any ongoing changes in the NIST 800-53 Rev 4 Moderate Controls regulatory requirements.

Outcome

System Soft fully assessed the security posture of the community college's applications, network and information system. This resulted in a stronger cyber security posture and detailed remediation guidance, ensuring compliance with NIST 800-53 Moderate Security Controls and federal cyber security regulations.

Conclusion

As you evaluate your networks and applications to improve your organization's security posture and ensure regulatory compliance, consider partnering with a trusted IT security risk assessment and technology advisor.

The System Soft Security Team has extensive experience working with state governments, education systems, financial institutions, and many others, enhancing security posture and achieving regulatory compliance. All done through concrete guidance for implementing optimal security controls.

When considering a third part security provider, it is important to look for a company with end-to-end security services and solutions and trusted advisors who can help you navigate the ever-changing cybersecurity landscape to ensure you have maximum threat protection and comply with regulatory requirements. If you have questions about enhancing your security posture and achieving compliance, contact **System Soft** today.