Security Scorecard

CASE STUDY

Higher Education

Higher Education System protects valuable research data with SecurityScorecard

Security team reduces the risk of supply chain breaches from the university’s expansive attack surface

The Challenge

Academic endeavors are open and collaborative to advance knowledge, encourage interdisciplinary research, and ensure rigorous peer review. By design, this expands the university's cyber attack surface while creating opportunities for malicious actors to gain access to valuable information. Although the university had a technology vendor review program whose aim was to prevent third-party breaches from exposing research data, its effectiveness was limited due to time-consuming processes and lack of validated security insights.

INDUSTRY	HEADQUARTERS	PRODUCTS
Higher Education	United States	Third-party Cyber Risk Management, Security Questionnaires

The university is a Tier 1 research institution with around 12,000 students and 3,000 faculty and staff, spread across two main campuses and several satellite campuses. Its cybersecurity operations are managed by a small, dedicated team. This team handles a wide range of responsibilities, including security architecture, vulnerability management, incident response, cybersecurity awareness training, third-party risk management, and technology reviews, collaborating closely with other IT teams to protect the university's diverse and sensitive data.

KEY BENEFITS

- Reduced risk of third-party data breaches
- Increased productivity of security reviews
- Continued adherence research funding requirements

> Vendor reviews used to take one hour, **now they take 10 minutes.**
>
> –Director for Cybersecurity Operations

The Solution

Implementing SecurityScorecard brought significant benefits for the university's cybersecurity operations. The platform streamlined the process of assessing and verifying vendor security practices, saving time and increasing reliability. With SecurityScorecard's automated and comprehensive vendor questionnaires, the university could quickly cross-reference vendors' security claims with their actual security performance, reducing the need for manual checks. For example, if a vendor responded to a questionnaire stating that they have an active vulnerability management program, SecurityScorecard's findings about unpatched vulnerabilities can help determine if additional reviews with the vendor are required. This efficiency allowed the small cybersecurity team to manage their workload better and focus on critical tasks.

The university chose SecurityScorecard for its flexible design and intuitive outputs. SecurityScorecard's ability to easily create or modify security questionnaires enabled the university to continue working with the Higher Education Community Vendor Assessment Toolkit (HECVAT), a framework specifically designed for measuring vendor risk at higher education institutions. In addition, SecurityScorecard's A through F cyber risk grading methodology enables non-technical stakeholders, like vice chancellors or the Board of Trustees, to understand the value of security investments.

The Result

The university's resilience against threat actors who target attack surface weaknesses has increased while maintaining the institution's need for an open and collaborative working environment. The security team has gone from being swamped by vendor reviews, potentially creating unseen security gaps, to being able to perform security reviews before a contract is executed, which allows the university to prevent or contain risky third-parties who interact with university networks. These risk management improvements bolster the university's ability to comply with government agencies that are a major source of funding for research, allowing the university to maintain its status as a tier 1 research institution.priorities forward.

Reduced risk of third-party data breaches

The ability to instantly evaluate a technology vendor's security posture using SecurityScorecard enabled the university to implement security reviews at the start of procurement processes. The security team is now a partner during vendor procurement and is able to offer solutions that meet the university business needs while not compromising security standards. This reduces the likelihood of "shadow IT" which, when unchecked, can create gaps in the university's preparedness against supply chain cyber attacks.

> "
>
> The single pane of view for both attack surface and third-party risk management is **very user friendly.**
>
> - Director for Cybersecurity Operations

Increased productivity of security reviews

Vendor reviews have been reduced from one hour per review to 10 minutes. This increased efficiency has not come at the expense of security scrutiny. The university continues to use the HECVAT security framework, with over 300 questions, during its review process. Using SecurityScorecard they have shifted from manually reviewing spreadsheets to an automated system where responses are validated against independently collected attack surface data, allowing the team to focus their time on the responses that conflict with findings.

Continued adherence research funding requirements

Many compliance regimes that a university must adhere to, including cyber insurance, require third-party risk management capabilities. As a tier 1 research institution, it is also essential to remain compliant with the Cybersecurity Maturity Model Certification (CMMC) 2.0 model in order to continue to receive high levels of funding from the United States government. SecurityScorecard helps the university secure its own systems and monitor its subcontractors, which are the two key prongs of CMMC 2.0 and other compliance frameworks.

SecurityScorecard Solutions

Third-Party Cyber Risk Management

The university can instantly evaluate the security posture of any third-party using an intuitive A through F grading methodology that is highly correlated with breach likelihood. Organizations with an F rating are 13.8 times more likely to be breached than those with an A rating. In addition, they are able to maintain visibility of supply chain risk by continuously monitoring vendors for exposure to zero-day vulnerabilities, disclosed breaches, or issues that are indicative of poor security standards.

Security Questionnaires

The university implemented the HECVAT questionnaire framework within SecurityScorecard and they can easily create custom questionnaires for specific security needs. Questionnaire responses are validated against real-time attack surface data, which helps the security team prioritize vendor outreach and have more effective discussions. They are able to communicate directly with vendors within the platform which reduces the inefficiencies of back and forth email communications. In addition, vendors can provide documentation like SOC2 reports for gaining additional context into the vendor’s security performance.

> “
>
> SecurityScorecard makes it easy because you can tell if a vendor is secure and why.
>
> - Director for Cybersecurity Operations

SecurityScorecard