CASE STUDY

The University of North Florida Leverages BitSight to Improve Overall Security Performance Across Campus Ecosystem

BITSIGHT

CHALLENGES

- Understand how to assess and remediate gaps in their security processes
- Continuously monitor the security performance of their third party vendors

SOLUTIONS

- BitSight for Security Performance Management
- BitSight for Third-Party Risk Management

KEY BENEFITS

- Allocate limited resources and prioritize security efforts and initiatives
- Identify, monitor, and reduce risk before contracting with third parties

ABOUT THE UNIVERSITY OF NORTH FLORIDA

Established in 1972, the University of North Florida is a public university located in Jacksonville that features six colleges of distinction, nationally recognized flagship programs, 56 bachelor degree programs, and over 75 areas of concentration. It is part of the State University System of Florida and is accredited by the Commission of Colleges of the Southern Association of Colleges and Schools to award baccalaureate, masters, and doctorate degrees.

THE CHALLENGES

Maintaining the security posture of a university can be complex given the number of departments, types of technologies, size of student and employee population, as well as volume of devices on campus. The University of North Florida was tasked with understanding their security performance from an external perspective, remediating potential cyber risk within their organization, and reporting on security performance improvements made over time.

In addition, they wanted to reduce the amount of time it took to conduct a technical review of a potential vendor's security posture before getting into a contract process with that third party. Their goal was to use an external tool to monitor the security performance of their third party ecosystem that was well documented, efficient and required less work for their team.

THE SOLUTIONS

To effectively understand their security posture, the University of North Florida utilizes BitSight for Security Performance Management to quantify their cyber risk exposure and measure security program success.

BitSight helps organizations take a risk-based, outcome-driven approach to managing the performance of an organization's cybersecurity program from a central department. Through broad measurement, continuous monitoring, and detailed planning and forecasting -- security and risk leaders are using BitSight for Security Performance Management in their efforts to continuously assess and measurably reduce cyber risk.

The University of North Florida Case Study

In addition, to help monitor the security performance of critical third parties (who have access to employee and student data), the University of North Florida is utilizing BitSight for Third-Party Risk Management to identify, quantify, and mitigate inherent risk involved in sharing sensitive data with vendors and business partners. This automated service analyzes, rates, and monitors the security performance of third parties, all from outside the organization.

THE RESULTS

By using BitSight for Security Performance Management, the University of North Florida leverages the data to start planning future cyber security projects. Jeff Gouge, Assistant Director of IT Security at the University of North Florida, expressed how "visibility is one big thing that BitSight does holistically, whether it is our security performance or of our third party ecosystem. I appreciate the holistic view BitSight provides to me and my team."

The University is also using the BitSight Portfolio Risk Matrix to operationalize and prioritize their organization's third party risk management process based on their third parties' criticality and security risk. The Portfolio Risk data is integrated into their workflow process for building out the University's external view of third party vendor risk. From that workflow, all new and existing integrations from products and services that require the sharing, generation, or storage of university data are vetted by the data stewards first to ensure the data is approved to be integrated. Data stewards cover various data domains such as HR, student, finance, etc.

After being approved by the data stewards, the security team leverages the BitSight matrix to make a risk determination based on the data classification and the BitSight Security Rating. In some cases, compliance documentation is then required from the vendor based on the established matrix. In rare cases where the matrix calls for it, the team may stop the contract process and avoid business with the third party. This streamlines the process and reduces the human error involved with assessing risk while giving a firm footing to push back against integrating university data with poorly secured third parties.

> "We heavily utilize BitSight. Our external website highlights how the BitSight Security Ratings data is used to help determine what we are going to do with a vendor, if we are going to do anything at all."

-- JEFF GOUGE, ASSISTANT DIRECTOR OF IT SECURITY, THE UNIVERSITY OF NORTH FLORIDA

ABOUT BITSIGHT

BitSight transforms how organizations manage cyber risk. The BitSight Security Ratings Platform applies sophisticated algorithms, producing daily security ratings that range from 250 to 900, to help organizations manage their own security performance; mitigate third party risk; underwrite cyber insurance policies; conduct financial diligence; and assess aggregate risk. With over 2,100 global customers and the largest ecosystem of users and information, BitSight is the

FOR MORE INFORMATION

BitSight
111 Huntington Ave
Suite 2010
Boston, MA 02140

www.bitsight.com
sales@bitsight.com