

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

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.



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



- Education
- Jacksonville, Florida
- 1000+ employees

Challenge:

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

Solution:

Bitsight Security Performance Management
Bitsight Third-Party Risk Management

The challenge

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 solution

To effectively understand their security posture, the University of North Florida utilizes Bitsight Security Performance Management (SPM) 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 SPM in their efforts to continuously assess and measurably reduce cyber risk.

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 Third-Party Risk Management (TPRM) 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.

Key Benefits

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

The results

By using SPM, 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.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ)

RALEIGH

NEW YORK

LISBON

SINGAPORE

BUENOS AIRES



BITSIGHT