

California University Assesses and Improves Network Security Posture

Protecting student information and keeping the network safe are top priorities for this higher education institution – how did they stack up?

A private liberal arts and sciences university based in California faces the same IT security challenges that many higher education institutions must manage. A significant issue is that the university's IT department serves as the Internet service provider (ISP) for the entire student body of 4,500 students on seven regional campuses.

Another challenge for the school is segmenting the student body from the critical infrastructure and systems that house sensitive data. The university had implemented security features using its own IT staff, but wanted to test the current infrastructure to ensure the students and the school's assets were protected.

What was the best way to approach this challenge?

- Perform a network security assessment of the school's IT assets and environments.
- Assess current security posture compared with industry best practices.
- Identify vulnerabilities that could negatively affect the institution.
- Provided recommendations for remediation of any found issues.

PROJECT OVERVIEW

Organization Size:
4,500 students

Organization Industry:
A private California liberal arts and sciences university

Challenge:
To assess the university's current information security posture against industry best practice standards, and identify vulnerabilities that could negatively affect the institution.

IMPACT

- Identified strengths and weaknesses
- Reported key findings, deficiencies and implications
- Determined short-term and long-term remediation goals
- Provided comparative security posture analysis

SECURITY ASSESSMENT SERVICES:

Validating Security Measures



Asset Cataloging

To start, Optiv cataloged IT assets, then attempted to penetrate existing security mechanisms by using software tools and exploit scripts that are similar to those used by attackers.



Testing and Assessment

Optiv performed vulnerability assessments and penetration testing of Internet-facing devices, firewalls, operating systems and application platforms. They also completed wireless infrastructure and network architecture configuration reviews.



Analysis

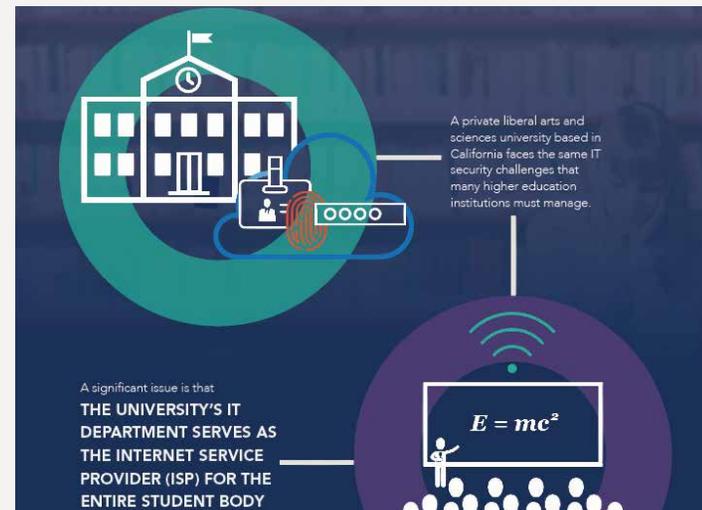
Optiv concluded that the university was at a low level of exposure. Though Optiv did not find any critical issues, they did identify low and medium criticality vulnerabilities relating to vendor technology.



Recommendations

Optiv recommended short- and long-term goals to address gaps such as systems in need of maintenance releases. Where not limited by vendors, the university could upgrade and apply security updates to lower the risk of unauthorized access.

- Determined short-term and long-term remediation goals.
- Obtained comparative security posture analysis.
- Identified levels of risk for third-party vendor technology.



[View the Client Spotlight Infographic at www.optiv.com/resources/library](http://www.optiv.com/resources/library)

Fully Maximizing a Product Investment

By partnering with Optiv to conduct an objective third-party security assessment of its IT network, this California university found that it is well above its peers concerning industry standards. However, Optiv discovered opportunities for the university to even better secure its environment and protect its important and confidential data. Due to a successful project, the client:

- Confirmed a low level of exposure with no current critical issues.
- Received key findings and information on deficiencies and their implications.



Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

1125 17th Street, Suite 1700 | Denver, CO 80202 | 800.574.0896 | www.optiv.com