

**RAPID7 CONTINUES EDUCATION MARKET MOMENTUM BY ADDRESSING COMPLEX UNIVERSITY VULNERABILITY MANAGEMENT CHALLENGES**

University of Pennsylvania, Virginia Tech and University of Mary Washington among others join Institutions Using NeXpose to Assess and Remediate Threats without IT Burden

BOSTON, Mass. – March 9, 2009 – Rapid7, the leading provider of unified [vulnerability management](#) solutions, today announced the addition of multiple leading universities to its roster of educational institutions using Rapid7 NeXpose as a key step in their defense-in-depth security strategy. The University of Pennsylvania, Weill-Cornell Medical College, University of Miami, Virginia Tech, Norwich University, Carnegie Mellon, and the University of Mary Washington are now leveraging NeXpose to locate, assess, and eliminate numerous vulnerabilities across networks, Web applications, servers, and databases.

According to the Identity Resource Center, 20 percent of the 2008 data breaches occurred within the education market. With small IT departments and thousands of student, faculty, and staff records housed and accessed across multiple assets, universities require the deepest level of vulnerability scanning coupled with a prioritized remediation plan. Rapid7 NeXpose locates vulnerabilities across all vital resources and chains those vulnerabilities together to detect real threats and reduce false positives. NeXpose then delivers prioritized reports and remediation plans that highlight the most critical vulnerabilities for immediate remediation. Using NeXpose, educational institutions can also achieve compliance to a variety of industry standards when handling specific sensitive data.

For the University of Mary Washington, NeXpose's accurate scan results and prioritization of threats enable the school's limited IT security department to eliminate manual processes when finding vulnerabilities, such as [SQL injections](#) and cross-site scripting ([XSS](#)), and determine the risk of each issue. At the same time, NeXpose checks the school's security configuration of servers and other network equipment to ensure that the security settings are correct and that patches are updated.

Many universities have complex environments with IT administrators dispersed throughout the campus, and Rapid7's role-based administration enables a centrally based resource to broaden the use of NeXpose. As a result, departments can perform self-scans of critical systems and take immediate action in response to vulnerabilities, limiting exposure and damage. For example, the University of Pennsylvania, one of the nation's most selective and competitive universities, is comprised of four undergraduate and 12 graduate and professional schools, with multiple departments under each. Its decentralized IT environment requires that, in many cases, its local department IT personnel have the ability to scan their systems consistently, in addition to the periodic scans conducted by the central IT department of critical hosts and other vital systems during IT audit and security work.

“Providing each department with the ability to run self-scans in addition to our work in central IT results in more frequent vulnerability scans,” said Melissa Muth, senior information security analyst at Penn. “And, since NeXpose tests each vulnerability to reduce false positives, our results are also more accurate. Combined, these features have reduced our overall risk of exposure, as well as the time and cost of managing and remediating vulnerabilities.”

NeXpose plays a vital role in Virginia Tech’s Technology Security Reviews, a major initiative to ensure that the university is in compliance with PCI-DSS when handling payment data, as well as other compliance standards, such as HIPAA and GLBA. The role-based administration feature within the product enables each department to audit its IT infrastructure through security self assessments, to determine vulnerabilities and to understand remediation next steps. NeXpose then provides reports - both compliance-based and customized policy - that document and demonstrate compliance to both internal and external auditors.

“In 2008, the industry saw a significant number of data breaches occur at educational institutions, leaving many students and faculty at risk for identity theft and universities in jeopardy of exposing intellectual property,” said Mike Tuchen, president and COO. “NeXpose is the best solution for organizations, including educational institutions, seeking to locate and remediate vulnerabilities across all assets, a critical component of complex IT infrastructures.”

About Rapid7

Rapid7 is a leader in [vulnerability management](#) and compliance, delivering a single unified solution across an organization’s entire infrastructure. Rapid7 NeXpose helps securities professionals to reduce their attack surface by providing actionable insights into the real threats from vulnerabilities across their entire IT infrastructure. Rapid7 NeXpose is the only solution that provides in-depth coverage of vital Web and database systems in addition to networked devices, servers, and operating systems. The NeXpose A.I. and Reporting Engines synthesize large quantities of raw data to provide direct insight into the vulnerabilities that represent the most risk to the business. From this insight the product delivers a set of prioritized remediation recommendations that help security professionals get protection fast. Organizations, including Black & Decker, Trader Joe’s, Florida State University, the *New York Times*, and the City of Philadelphia, continually rely on Rapid7 products and services to mitigate risk and remain compliant. For more information, visit www.rapid7.com.