The Legal Intelligencer

NOT FOR REPRINT

Click to Print or Select '**Print**' in your browser menu to print this document.

Page printed from: *The Legal Intelligencer*

Eastern District

Protecting Against Cyberattacks on Colleges and Universities

Peter F. Vaira, The Legal Intelligencer

May 19, 2015

Colleges and universities are increasing targets for cybercrime operators. Rutgers University and Fairleigh Dickinson University were both recently hit in cyberattacks. Both schools' networks were shut down for nearly a day. In 2014, Indiana University and the University of Maryland were victims of cyberattacks. Indiana had 146,000 records exposed and Maryland had 300,000 records exposed. Colleges and universities face cybersecurity challenges similar to those faced by government and major commercial institutions. Investigators in this area describe the attack techniques on educational institutions as the same level of sophistication as used in international espionage. What does this mean for the institutions and the law firms that represent them?

The basic cyberprotection problem with colleges and universities is the nature of the institutions themselves. Government and commercial institutions often prohibit employee access to certain Internet sites—such as social media or gambling and pornographic sites—or they limit access to professional technical websites. Educational institutions, however, tend to be more open as they want to provide their students with online resources to support the school's academic mission. Therein lies the problem. Once admitted to the university, students are granted access to the school's Internet system. Unlike an employee for a government agency, where access is limited to certain sources, the students, especially those working on research projects, have almost unlimited capacity to contact and download numerous websites from the Internet. This is especially true when the student utilizes his or her own computer. Many of those websites are easily infiltrated by hackers. If those infiltrated websites are downloaded to the university system, the virus travels within the website, and then can enter the university or college computer system. Thereafter, the hacker is free to roam about looking for opportune targets. Many departments within the institutions have extra protection, but because of the nature of the academic institution, some departments are easily breached. As a result, the security postures of an institution's different divisions—academic, administration, student life and athletics—have direct impact on each other. Poorly maintained and unpatched systems in one network could lead to the compromise of other systems across the school's entire internal system.

We are not talking about hackers who want access to prove their skills; the propriety information in certain university departments is valuable on the black market for big money. There is an immense amount of personal information about applicants and students that are supplied every year. Social Security numbers and personal addresses are valuable to people seeking to establish bogus credit

cards for purchases of valuable property or for cash advances. There are thousands of research grants at universities that produce new products, drugs and medical devices. The research material from these projects can readily be sold on foreign markets. Many research projects do receive increased protection within the school's system, although often not enough.

For a practical explanation of various technical aspects of cybersecurity, I obtained the assistance of Charles Bartel, assistant vice president and chief information officer of Duquesne University in Pittsburgh. Bartel utilizes the combined efforts of four full-time positions to manage Duquesne's information process. I also consulted with Dave Reis of the cyber-investigation firm, Cloud, Feehery & Richter, who said that a college or university's cybersecurity strategy should address three key disciplines: prevention, detection and response.

Prevention involves taking proactive measures to ensure that attackers cannot breach the cybersecurity of the enterprise. The first step is an initial filtering system. Duquesne University employs a system provided by Microsoft to maintain a level of initial filtering of all email traffic to the university. Bartel said the system filters out 80 percent of the traffic received by the university every day, as junk mail, spam, or potential malware.

The major effort in prevention generally involves conducting regular patching. This means examining the network for possible problems arising from the constant updates. Duquesne utilizes new patching systems each year in response to the changes the system is undergoing. Another technique in prevention is the updating and deploying of firewalls. A practical way of looking at this entire process, Reis explained, is similar to taking your car in for alignment after so many miles of use and repairs. The network needs to be regularly aligned in a similar manner.

An important aspect of prevention is segregating servers that host critical data or services from the internal network. This means that very critical material should be kept on separate servers and not mingled with less critical material. Duquesne University is considering utilizing virtual computers of 10 to 20 computer systems, with no connection to each other. And lastly, as one would go to his or her doctor for an annual physical checkup, cybersecurity people advise getting a regular audit by outside professionals.

Detection seeks to identify any threats that are attempting to exploit cybersecurity weaknesses within the institution's systems. Early detection of cybersecurity threats is crucial to breach prevention and minimizing the costs of a breach. The more prompt the detection the better the chance to limit the damage. Detection controls include network security monitoring (NSM), intrusion detection systems (IDS), and log aggregation/security information and event management (SIEM) solutions. Good detection practices include regular checks and proactive breaches, often referred to as penetrations. Duquesne University conducts periodic penetrations of its systems throughout the year. Ideally this should be done by an outside agency, and one that is not employed by the university on a regular basis.

Breaches can and will occur, despite preventive and detection controls and measures. In the event of a breach, response activities are critical to a school's operations. First, the breach must be identified and rectified to prevent its spread. Second, the damage must be assessed. It is very important to preserve or identify as much of the information that was taken as soon as possible. According to Reis, this often will help identify the source of the breach. Moreover, it might be necessary for prosecution of the culprits and for civil suits to follow. Thirdly, ensure that the system is not simply shut down, but institute preventative measures on that aspect. Above all, give the client a reasonable expectation of the prospective damages. A good executive will ask, "OK, we have been breached, now what can we do to minimize the damages, how far is this going to go,

and what is it going to cost the school?" You need qualified people to answer these questions. In some cases, response activities can be as simple as implementing a firewall. In other cases, incident response can be lengthy, complex, complicated and resource-intensive. Here, an institution should have a reliable, trusted partner that specializes in digital forensics, malware analysis, isolation of individual systems or entire networks, and recovery and remediation operations.

What are the legal implications of these cyberattacks? For outside and in-house counsel to the educational institutions, it will be necessary to get to know the systems employed and how they work. Determine the legal standard of care for a university or college regarding the safeguarding of personal material supplied by students, and material contained in research work of faculty members. Insurance companies are demanding a demonstration of expertise for safeguarding student and research material in this area. There is adequate notice to educational institutions that the information they hold may be subject to cyberattack that they owe a degree of care to the owners of such information. Michael Gebhardt, Temple University general counsel, said the standard of care for protecting the students' personal information is whether the university was negligent in failing to provide proper care of the material. For example, plaintiffs brought a class action lawsuit against the University of Miami's health care system after the school's computer storage system, containing the plaintiffs' personal information, had been breached. The case settled.

Gebhardt said the standard of care for protecting information in a research project funded by an outside entity is that which is applied to a breach of contract. Each research grant should contain a clause guaranteeing safety of the results of the research. These contracts will become more specific as the threats of cyberattacks on colleges and universities become more publicized. The area of legal responsibility will be the subject of a future column.

Peter F. Vaira *is a member of Greenblatt, Pierce, Engle, Funt & Flores. He is a former U.S. attorney, and is the author of a book on Eastern District practice that is revised annually. He can be contacted at p.vaira@gpeff.com.* •

Copyright 2015. ALM Media Properties, LLC. All rights reserved.