School Information Security

By John N. Stewart, Cisco Vice President and Chief Security Officer

Protect the network, use the network to protect students

Your schools use a growing amount of networked information and devices as an essential part of teaching and administration. Research on the Internet, laptops in class, distance learning, and online homework are some of the official technologies that your students use. Unofficially, this list extends to mobile phones (with cameras), digital music and video players, blogs, instant messaging, social networking sites, and networked or online gaming. Behind the scenes are databases with student information, class schedules, attendance records, copies of exams and answers, financial transactions, and even video surveillance. All of these rely on a robust and secure network infrastructure.

Whether in grade school, high school, or college, our children's learning environment should be safe and secure, and their personal information should remain personal. But digital information and networks bring new dimensions to the threats and risks you grew up with, from bullying and cheating to social predators and serious physical threats. Embarrassing moments that otherwise might be quickly forgotten, like "did you see Jane and Joe kissing," are captured as photos or videos, then posted and forwarded to the point of humiliation. Insults and bullying become cyber-bullying, and angry notes are now harassing texts and blog posts, able to reach victims well beyond the school grounds. Anyone can try to break into your school, and they no longer have to be at the school to do so. And they want to steal more than copies of an upcoming test.

Your students' and your school's information has value to someone, and that someone may try to steal it, copy it, or change it. This information includes copies of exams and answers, class schedules, grades, even personal data. Credit card information from online payments or donations is a target, as is data collected by university researchers. By protecting that information and the network that provides access, you also protect the people who use it.

Resourcing your school's security

The safety of your students is vital, but in most schools your time and your budget are limited. With security, you can't afford to do everything, nor should you do many things halfway. You have to be surgical to protect the most important parts of the network and information infrastructure.

The important question to answer is, what threats are you trying to protect against? In grade school, supporting the school's physical security and protecting students from inappropriate content may be priorities. In high school, it could be managing the proliferation of electronic devices, protecting information from student hacking, and supporting emergency response and notification systems. In university, it is more like security in a small town, with the competing challenges of offering a range of information and network services, ensuring public safety, and protecting the privacy of a diverse population.

Security decisions are ultimately threat and harm decisions. What is the probability of the threat and how serious is the consequence? For example, the possibility of a shooting incident may be very low, but the consequences catastrophic. An integrated emergency communications system that can quickly notify security officials as well as teachers, students, and even parents has become a priority for some school districts. Once installed, these systems can also support services that are more mundane. Automatic notification of snow days, school closures, or student absences can produce operational cost savings that help repay the initial investment.

An overall risk management strategy is very helpful to direct security efforts and identify areas you may choose not to address that would otherwise consume time and budget. Without the resources to do everything all at once, you can begin by implementing one or two capabilities and adding others later. In secondary and post-secondary schools, you can also look to the students for help.

Let the students help

People in network security may have to contend with users who understand and use the electronic capabilities better than you do. You may not be using Twitter and Facebook, hanging around hacker websites, or experimenting with how to use a cell phone camera and USB key to cheat. Students like testing boundaries, pushing the limits, and exploring new paths. They are also are growing, exploring, learning about themselves and their friends—and insecurities can sometimes cloud their judgment.

Involving the students and making them part of your network protection can be a learning experience for everyone. Encourage them to share stories about their experiences. Use social media such as Facebook or blogging to initiate the dialogue, as your generation's approaches may be dismissed as lame or archaic. Students may be ultimately responsible for their online activities, but you can provide a forum for them to discuss with you the risks and consequences. Students often want to share what they know, and the prospect of working with you may prove exciting to them. Facilitating their help gets you engaged and will help your strategy as you learn what they know and can do. It can even help them with future education or work opportunities, and that's a win-win scenario.

You make the rules

Letting students help does not mean relinquishing control. You still make the rules and policies that guide security. First, consider the requirements, the things you have to do for regulatory compliance. There is a growing body of state and federal legislation dealing with security and privacy subjects. These range from acceptable-use policies for students to video surveillance and payment card security (PCI DSS), to child (CIPA) and family privacy (FERPA). Some are still evolving and may have vague or poorly understood conditions. Keep current with these policies to understand how the changes affect your institution. The threat landscape is also changing. There are numerous online services, such as IntelliShield Alert Manager offered by Cisco, that provide an up-to-the-minute view and mitigation for security threats and vulnerabilities.

Once you have addressed what you legally must do, you can prioritize the remaining time and dollars. Security essentials include up-to-date antivirus and firewalls on all computers, network access control, policy servers, and intrusion detection and prevention systems. The Cisco SAFE architecture provides detailed configuration guidelines for securing a networked environment. Your peers in other schools are a great resource for learning and sharing leading practices. Because many computing and networking activities move from older to younger children, you can look to the next schools in your students' path for information and guidance on issues that may be heading your way.

Running multiple services on your network, including phones, video surveillance, and building sensors, is cheaper than operating multiple networks and opens up additional service and cost-saving opportunities. However, collecting and storing the resulting information not only increases the importance of privacy, but also may increase your institution's risk. Effectively protecting the network and maintaining a strong security posture will help protect the people, property, and information in your school.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**