TECH BRIEF

Education security: Lessons for IT pros

ESET

ENJOY SAFER TECHNOLOGY™

EDUCATION SECURITY: LESSONS FOR IT PROS

By Lysa Myers, ESET Security Researcher

As every education IT pro knows, schools are much more than just places where people work and learn.

Today's educational institutions can include health clinics, research labs and retail stores, while dorms add the characteristics of an apartment complex or hotel. Many schools share partnerships with government agencies or healthcare organizations, while others host students from abroad.

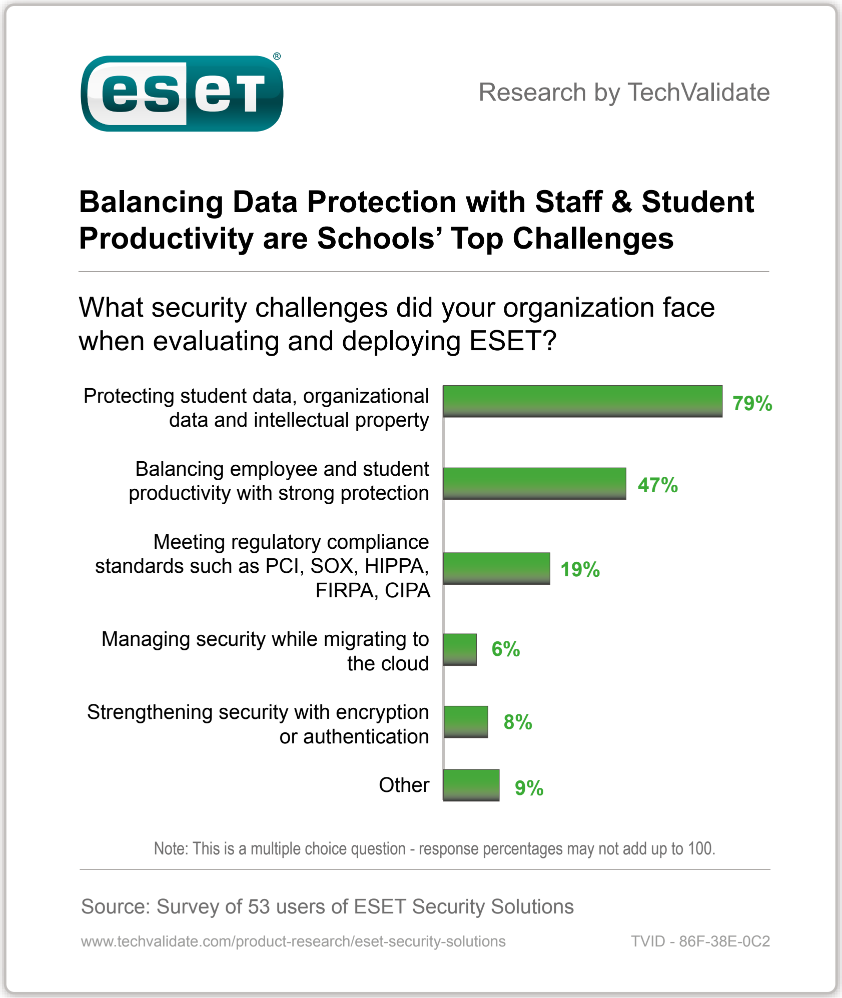
One thing is common to schools of all sizes: the desire to operate with openness and freely share information in the spirit of communal learning.

That, combined with the amount of data generated in the course of normal operations, means enormous data security responsibilities for the IT staff.

Survey says?

TechValidate, a respected third-party research firm, recently asked customers in the education sector about the biggest security challenges they faced.

The top challenge? Four out of five respondents cited protecting student and organizational data and intellectual property. But 47% also cited the challenges of implementing strong security without reducing employee and student productivity or restricting openness.



Balancing Data Protection with Staff & Student Productivity are Schools' Top Challenges

What security challenges did your organization face when evaluating and deploying ESET?

Note: This is a multiple choice question - response percentages may not add up to 100.

Source: Survey of 53 users of ESET Security Solutions

www.techvalidate.com/product-research/eset-security-solutions TVID - 86F-38E-0C2

How can IT professionals achieve these seemingly mutually exclusive goals – locking down information while keeping it available for legitimate use and maintaining an open environment?

Openness – within reason

Cyber security experts recommend "openness within reason," a policy that helps ensure that staff, students or parents who need the information can get it, while restricting access for others, with three simple steps:

Step 1: Segmentation

Decide "who needs what" – determining which individuals or groups need access to which particular data, online tools or networks. For example, students need to access their own grades online. But they don't need to access others' grades – or others' healthcare, personal or financial information, for that matter. Use the "principle of least privilege" during segmentation:

> Give a user access only to the information and resources he or she absolutely must have for legitimate reasons, and nothing more. You can apply this principle across user groups, machines or networks as well. It's like deciding who needs the keys to your house: the fewer people, the better.

Step 2: Authentication

OK, you've decided who can access what. Now, make sure users are really who they say they are by using authentication.

Authentication starts with passwords. Educate staff and students about choosing a strong password (at least eight characters and a mix of letters and numbers, upper- and lowercase). Have them change passwords regularly – at least every three months. Remind them not to use the same password for multiple sites or access points.

On the IT side, implement both hashing and salting to give more protection for your users' passwords. For stronger authentication on more sensitive areas of your network, implement two-factor authentication, such as ESET Secure Authentication, which sends a one-time key to your users' cellphones.

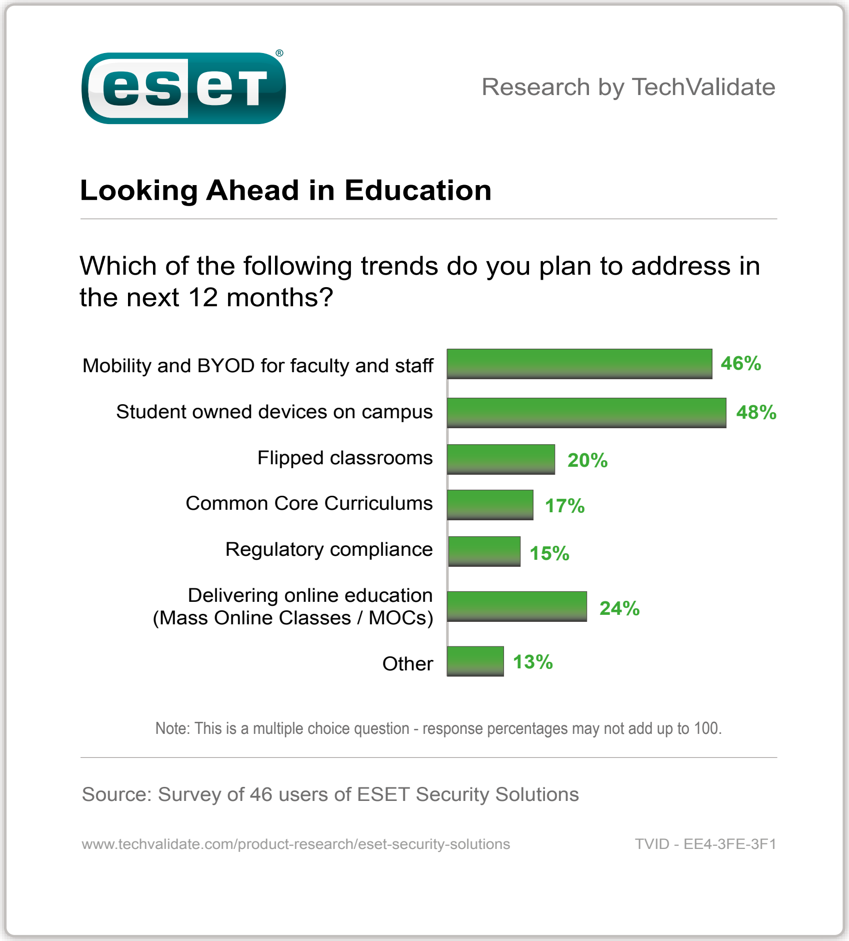
Step 3: Encryption

You've already improved your security posture through segmentation and authentication. Now, harden your defenses even further: Protect sensitive information such as Social Security numbers or personal health records by encrypting it, both at rest (files and folders stored on hard disks or in the cloud) and in motion (while it's being emailed, posted to the Web or sent to the cloud). By using a product such as DESlock+ data encryption to convert information into encoded text, you've added an extra layer of protection in case of a breach.

Mobile? Keep an eye on it

Another factor that complicates data security in schools is the ever-increasing number of mobile devices. They're easily lost or stolen; are notoriously difficult for IT to manage and control, and contain valuable data.

The TechValidate survey found that almost half of all respondents intended to make changes within the next 12 months that would help address the presence of mobile devices brought by students, staff and teachers onto their network.



Research by TechValidate

Looking Ahead in Education

Which of the following trends do you plan to address in the next 12 months?

Note: This is a multiple choice question - response percentages may not add up to 100.

Source: Survey of 46 users of ESET Security Solutions

www.techvalidate.com/product-research/eset-security-solutions

TVID - EE4-3FE-3F1

Your IT takeaway:

Take some time to review your mobile security and Bring Your Own Device (BYOD) policies. With hardware and software changing all the time, your security strategy is probably due for an update. If possible, revisit policies every three to six months.

Consider switching faculty and staff from a BYOD environment to a Choose Your Own Device (CYOD) policy. By letting employees choose from a selection of IT pre-approved devices, you'll gain better control of these endpoints and ensure the latest (and most secure) release is being used. At the same time, by providing a choice, you're still fostering that sense of openness and freedom schools strive for. It's a win-win situation!

Looking for additional resources on cyber security for the education sector?

Visit the ESET blog, WeLiveSecurity.com, for breaking news and in-depth research on security issues.

Visit Educause.edu for information and resources provided by IT leaders and professionals committed to advancing higher education.

Visit SecuringoureCity.org for news and resources for getting teachers, students and families involved in cyber security.

For more information on protecting your mobile devices for both business and home,
visit eset.com/us.