Inside:
Can schools stay secure without a security officer?

John Morgan: a chemistry teacher bonds with technology

Are student data laws a blessing or burden?
Colleges and universities need a storage solution that can keep pace with digital transformation and the exponential growth of data. While hybrid environments are a popular stop-gap solution, they can be complex to manage. As an alternative, school IT leaders are finding that all-flash storage can provide the flexibility they desire and the simplicity they need.

All-flash storage from Pure Storage:

**LOWERS COSTS**

Pure’s Evergreen™ Storage model provides storage for a decade or more without any forklift upgrades. Maintenance costs stay flat for the life of the system.

**REDUCES DATA**

Flash storage is highly effective at removing redundant data. This frees space and increases performance speed, enabling easier management of data across the environment.

**SIMPLIFIES MANAGEMENT**

Pure Storage’s flash arrays can be installed in less than an hour. The instruction manual fits on a business card — it’s that easy.

To learn more, visit: [www.purestorage.com/education](http://www.purestorage.com/education)
COVER STORY: Building Policy
The Trump administration has said little about ed tech, but here's what might happen.
By Adam Stone

Who's in Charge?
Cybersecurity is one of the hottest tech issues, but few schools have someone dedicated to the problem.
By Jennifer Snelling

Feeding the Bandwidth Beast
Resident demand has exploded on college campuses, straining resources.
By Julia McCandless

Chemical Bond Technologist
John Morgan is capitalizing on his experience teaching chemistry to help other teachers mix technology into student learning.
By Jessica Renee Napier

Unintended Consequences
New student data notification requirements shift a heavier administrative burden on school districts, but state departments are stepping up to help.
By Julia McCandless
This year began with many transitions, including a new administration in federal government and the new Every Student Succeeds Act legislation that will be implemented in school districts across the country. During this period of change, we should keep in mind Thomas Jefferson’s position on education as the foundation of democracy and Nelson Mandela’s ideal that “education is the most powerful weapon we can use to change the world.” Today is the day to lay a foundation for an education vision where technology will play an essential role.

This issue of Converge is focused on igniting the next generation of education. We’ll introduce you to the major education policy priorities for 2017. We will also highlight the role technology plays in modern education by examining networks, cybersecurity and data privacy.

In one of our stories, we explore two states where laws have been enacted to protect student data: Connecticut and Colorado. This story shares the challenges and possibilities of ensuring student data are protected within the requirements of the law while still enabling school officials to utilize student data for decision-making.

Related to protecting student data are never-ending cybersecurity concerns. You will read about campuses that do not have designated security officers and how they manage security on a day-to-day basis. An essential component of next-generation education is connectivity on campuses around the country, and we have some fascinating stories to share about how colleges are supporting residents with connectivity. Finally, we highlight a leader in education technology who shares the challenges and possibilities of ensuring student data are protected within the requirements of the law while still enabling school officials to utilize student data for decision-making.

Dr. Kecia Ray
Executive Director, Center for Digital Education

As you begin your planning for the 2017-2018 school year, focus on developing a vision for next-generation learning and igniting new ideas for your campus. We hope you enjoy this issue of Converge.
Converge Newsletters

Keep up to speed on the latest technology trends, policies and issues in K-20 education.

Sign up today at www.centerdigitaled.com/newsletters
In December, as the White House prepared to sanction Russia for hacking, President Donald Trump said: “I think that computers have complicated lives very greatly. The whole age of computer [sic] has made it where nobody knows exactly what’s going on.” Some call this a nice summation of the situation facing those who wish to predict what the new administration may bring in the realm of education technology.

On the campaign trail, Trump offered few specifics about either education or technology. To plan for the coming year’s ed tech policy evolutions, advocates have had to search for signs and hints, scanning the track records of key leaders in Congress and on Trump’s leadership team. Some themes emerge. Congress may do something with higher education, and it will likely act on technical training. It may address technology training for educators, as well as broadband availability. The president may or may not encourage or endorse these efforts. Much remains unknown, but that hasn’t stopped the experts from weighing in on key ed tech issues.

In December 2015, President Obama signed into law the Every Student Succeeds Act (ESSA), a successor bill to No Child Left Behind that governs federal K-12 education policy. In Title IV Part A, the bill authorizes a range of activities, including the effective use of technology supported by professional development, blended learning and ed tech devices. Although Congress authorized $1.65 billion for Title IV, last year the House approved just $300 million with higher education, and it will likely act on technical training. It may address technology training for educators, as well as broadband availability. The president may or may not encourage or endorse these efforts. Much remains unknown, but that hasn’t stopped the experts from weighing in on key ed tech issues.

In December 2015, President Obama signed into law the Every Student Succeeds Act (ESSA), a successor bill to No Child Left Behind that governs federal K-12 education policy. In Title IV Part A, the bill authorizes a range of activities, including the effective use of technology supported by professional development, blended learning and ed tech devices. Although Congress authorized $1.65 billion for Title IV, last year the House approved just $300 million.
By Adam Stone

...million in this area, while the Senate would have budgeted $1 billion. No compromise was reached, meaning ESSA funding will likely come up for consideration in 2017. And education advocates want to see Congress dole out the full authorized amount.

ESSA does specifically address ed tech, and while it won't give every kid a tablet, it could help teachers become more tech savvy. “It is not intended to be used to purchase devices or software. It's meant to focus on professional development for teachers and administrators to effectively use technology for students,” said Tracy Weeks, executive director of the State Educational Technology Directors Association (SETDA), which supports the use of technology for teaching, learning and school operations.

Congress’ lack of action has been problematic to some, especially for school districts trying to write budgets without a clear understanding of future funding streams. That could change, but much will depend on whether the new administration opts to take up the cause. “Now it becomes about the Trump administration’s priorities,” said Jon Bernstein, founder and president of Bernstein Strategy Group. “The only thing we have heard from them about education is that they are interested in a giant school choice block grant — charter schools, vouchers for private schools, magnet schools. All of that could take money away from this program.”

Others meanwhile say the block grant nature of Title IV could make it appealing to Trump’s team, which has shown a desire to highlight the state and local role in education. It may be possible, for instance, to frame ESSA’s tech strategy to support that mindset by encouraging districts to use the funding for specific, local needs. “With ESSA’s emphasis around professional development, people...
Students increasingly need Internet access to do their homework, and yet a broadband gap persists. Some 5 million households with school-age children do not have high-speed Internet service at home, according to a Pew Research Center analysis, and low-income households especially black and Hispanic ones — make up a disproportionate share of that figure.

Last overhauled in 2014, the federal E-rate program is supposed to help close that gap by providing discounts to help schools and libraries gain affordable telecommunications and Internet access.

This year, the financial formula of $150 per student could come under review. The Federal Communications Commission (FCC) sets the formula and has lost E-rate champions Tom Wheeler and Jessica Rosenworcel.

Bernstein said, noting that FCC Chair Ajit Pai has shown support for the program, even while indicating that it could be run more efficiently.

Beyond the funding formula, experts are closely watching to see how much oversight the FCC chooses to exert. “It doesn’t make a lot of sense for the FCC to try to tell schools and districts how to use E-rate funds for ed tech,” said Mesecar, noting that the detailed work of implementing ed tech falls outside the realm of the FCC’s usual regulatory duties.

In fact, the program might benefit from a little more autonomy from the regulatory agency. “There is work that can be done to make those funds more usable and accessible, and the FCC’s views of how to handle the dollars don’t always line up with how money actually gets spent in the districts. It doesn’t always make practical sense. The FCC does what it does, and it ends up being a little too complicated for everyone who doesn’t live in that same world. It could be done more effectively,” Mesecar said.

Some see a way to bolster E-rate by putting it up alongside Trump’s clearly articulated desire to upgrade the national infrastructure. “If we are talking about roads and bridges, that discussion should also include a conversation about the telecommunications infrastructure,” said Reg Leichty, founder and partner of Foresight Law + Policy.

“The education community is saying: If you are going to invest in infrastructure, you have to invest in schools and libraries and health centers as hubs of connectivity. For students, we should invest in the infrastructure that allows them to do their homework at home,” he said. “We need to do better to make sure everyone is connected to high-capacity broadband, and the federal government could play a big role in that.”

The idea exists on paper, noted Russ Poulin, director of policy and analysis at the WICHE Cooperative for Educational Technologies (WCET), which advocates for technology-enhanced learning in higher education.

In his new role as FCC chair, Pai has made high-speed broadband access one of his top priorities, created a committee to provide policy recommendations and laid out plans for how to expand access. The Republican Party platform also calls for increased broadband availability, albeit without getting specific.

But the pendulum could swing the other way, for instance, with congressional action to scale down the Lifeline program, which subsidizes phone and broadband access for low-income households. “This program is not beloved by Republicans in Congress, who charge there is waste, fraud and abuse in the program. We think people will take a hard look at it,” Bernstein said. “We anticipate a fight coming.”
ASSOCIATIONS GEAR UP FOR 2017

PROFESSIONAL ASSOCIATIONS at the intersection of education and technology say they are gearing up to address a range of issues in the coming year as they seek common ground with a new administration.

The International Society for Technology in Education (ISTE), an education advocacy group, is looking to expand broadband access — perhaps through an infrastructure initiative — and to secure full funding for ESSA Title V Part A, according to Jon Bernstein, founder and president of Bernstein Strategy Group, who works on behalf of the group.

The Consortium for School Networking (CoSN), a professional association for district technology leaders, also has broadband front and center. “First and foremost, CoSN will work to help the new administration understand the value of E-rate as well as the recent changes to the Lifeline program. Those connectivity programs that are already in place are a big focus for CoSN in 2017,” said Reg Leichty, founder and partner of Foresight Law + Policy.

CoSN also has high hopes for ESSA funding. “The great thing is it has support on both sides of the aisle. Republicans like block grants, they like the flexibility; and Democrats like the focus of the program,” Leichty said.

At the WICHE Cooperative for Educational Technologies (WCET), which promotes technology-enhanced learning in higher education, Director of Policy and Analysis Russ Poulin is advocating on behalf of extending the Pell Grant program to cover year-round learning, a move he says would have deep technology implications.

“This speaks to distance learning, it speaks to adaptive learning, it speaks to competency-based education — all the places where the calendar is not the traditional calendar,” he said.
As an agenda item, a lot of pressure is building around higher ed in general. Sen. Bernie Sanders, D-Vt., made college costs a hot-button issue during his unsuccessful run for the Democratic presidential nomination. The administration also must find its feet on the complex questions of for-profit schools and the delivery of online for-credit classes. These policy questions, combined with corporate interests, could put higher ed and its associated technologies on the front burner.

At the same time, a number of unresolved questions exist surrounding the possible implementation of ed tech in higher education. In particular, observers wonder how tight a Republican administration will choose to hold the reins. “Will the feds take a step back and allow for more experimentation and innovation? Or will they continue to take a fairly narrow view of what it means to be accredited, making it more difficult for schools to explore these issues? Will there be a less heavy-handed approach to some of these issues?” Mesecar said.

This year. Alexander’s office told Converge that the senator will make it an early priority and will leave it up to local beneficiaries to decide what technology investments would make best sense in service of the act’s work-readiness goals. Foxx has likewise said that Perkins is a top priority.

This is one place where education and technology may most closely intersect because technology plays a pivotal role in so many fields that may fall under the heading of “career and technical education.” Many schools already have benefited from this, tapping Perkins funds as a way to access needed technology. “We want students to use technology in every class, but if this is a way to get it in the door, great, let’s start there,” Weeks said.

Perkins funds could, for instance, help to finance science, technology, engineering and math learning, along with virtual labs, online training or internships in technology companies.
More to the point, Perkins is politically viable, a rare issue that enjoys broad bipartisan support. “It’s not controversial and it does a lot of good, ensuring kids have the skills businesses want and need,” Bernstein said.

That practical aspect also may make Perkins appealing to a president who made jobs a key campaign issue. Technology-driven education could be positioned as means to bolster the workforce outside of the traditional higher education pipeline, Leichty said.

The fate of these diverse initiatives may rest largely in the hands of U.S. Education Secretary Betsy DeVos, an education reformer, Michigan billionaire and major Republican donor. DeVos was a leading figure in helping shape her state’s vigorous charter school efforts, and she has been a staunch proponent of vouchers. The National Education Association and the American Federation of Teachers opposed her for the secretary’s job. In a January letter to Alexander, 20 governors expressed their support for DeVos. Ultimately, in a dramatic moment, Vice President Mike Pence cast the historic tie-breaking vote on Feb. 7 to confirm her nomination in the Senate.

What’s not known are her attitudes toward ed tech. Some see opportunity in that ambiguity, a potential secretary whose views could be swung. “She wants every kid to have a quality choice in education. Well, education tech can provide some great choices for kids, whether they stay in their present school or choose a different one,” Mesecar said, suggesting that technology can be an avenue to educational excellence in any setting.

Some point to DeVos’ past support for blended learning, which relies partly on digital tools, as a potential positive sign, while others say they are looking for some indication of a deeper commitment.

“We are hoping to see an underlying fundamental belief that technology is an important piece of providing access to education — that it can be a way to help all our current schools to become schools of choice, if we are smart about how we do it,” Weeks said.

In an all-staff meeting, DeVos noted her willingness to learn: “I’m a door-open type of person who listens, here to serve with you.”

Any changeover in Washington comes with uncertainty, but longtime players say this round is different, that Trump’s opacity on key ed tech issues raises a host of unanswered questions. Those who see a place for technology as a key ingredient in education will be watching closely, and perhaps leaning heavily, as Congress and the president get down to work in the coming months.
PROTECTING YOUR FROM CYBER THREATS

CHALLENGES IN HIGHER EDUCATION

INCREASE IN DEVICES

THE AVERAGE STUDENT BRINGS 7 CONNECTED DEVICES TO CAMPUS.1

They can make the institution vulnerable to malware, phishing attempts and other malicious activities.

PHISHING IS THE NO. 1 DELIVERY METHOD FOR RANSOMWARE AND MALWARE.2

CONSTANT CONNECTIVITY

55% OF COLLEGE STUDENTS SAY THEY CAN’T LIVE WITHOUT THE INTERNET.2

Because of this, cybercriminals target campuses with DDoS attacks, which prevent students from accessing web sites for learning and personal uses.

DDOS ATTACKS INCREASED BY 71% BETWEEN Q3 2015 & Q3 2016.4

1. http://www.edtechmagazine.com/higher/article/2015/10/mapping-path-connected-campus
Akamai can help protect your campus from growing cyber threats. To learn more about Akamai’s suite of security solutions and services, visit: www.akamai.com

1. Assess your security landscape.
   Regularly assess your vulnerabilities, deploy new solutions and use third-party security audits.

2. Train staff and students.
   Malware and ransomware often find their way to your network via phishing attacks. Ongoing training can help prevent these attacks.

3. Opt for an as-a-service solution.
   Look for security-as-a-service solutions that provide a single, scalable platform capable of overcoming unreliable networks, congestion, inefficient protocols and malicious attacks.

4. Look to the cloud.
   A cloud-based security solution stops threats closer to the attacker and further away from your campus.

5. Partner with an experienced service provider.
   A trusted vendor can help your institution stay abreast of the latest threats, without taxing existing IT staff.

Web app attacks are the No. 1 source for data breaches.

By 2020, 33% of successful attacks experienced by enterprises will be on their own shadow IT resources.

Shadow IT — IT systems and solutions used inside organizations without explicit organizational approval — makes it difficult for central IT departments to protect applications.

Decentralized departments

Malicious attacks and phishing attempts are often the source of data breaches.

Train staff and students.

Look to the cloud.

Partner with an experienced service provider.

Assess your security landscape.

Train staff and students.

Opt for an as-a-service solution.

Look to the cloud.

Partner with an experienced service provider.

5 Steps to Mitigate Threats

Train staff and students.

Opt for an as-a-service solution.

Look to the cloud.

Partner with an experienced service provider.

Assess your security landscape.
Computer security in schools has come a long way since Ferris Bueller, the character from the hit movie of 1986, hacked the school’s network to change his absences. School districts are making progress, but with cybersecurity impacting every part of society from the election to Twitter and Netflix, it seems the education sector is still not as secure as it needs to be.

According to Verizon’s 2016 Data Breach Investigations Report, the education sector experienced 264 security incidents in 2015, including 29 with confirmed data loss. Those numbers have almost certainly increased over the last year. Likewise, education technology leaders showed a 64 percent increase in concern over privacy and security of student data since then, according to the 2016 IT Leadership Survey from the Consortium for School Networking (CoSN).

“Looking back and learning from the past, we can surmise that cyberthreats will continue and gain in sophistication,” said Steve Langford, a CoSN member and chief information officer at Oregon’s Beaverton School District. “School systems have much student and staff data that are valuable and, coupled with lean staffing levels, make us an attractive target for those seeking access and information. Regardless of size, school districts will need to invest in staff who are experienced in cybersecurity, now and into the future.”

Having a full-time staff person dedicated to cybersecurity is not possible for most school districts for several reasons. Few districts can...
afford to hire someone who has the skills and experience to run what has become a complex operation. Even those that have the funds are finding it difficult to hire skilled cybersecurity personnel because the demand for talent is at an all-time high. In 2015, more than 200,000 cybersecurity jobs went unfilled due to a talent shortage, according to the Bureau of Labor Statistics.

Schools are attacking the problem from a number of angles. After all, one simple solution doesn’t exist. Communities expect school districts to protect data the same way they protect a school building, but it’s a far more complicated process, said Aaron Barnett, IT director of the Moreno Valley School District and board member of the California Educational Technology Professionals Association (CETPA). “It’s like not locking your windows or doors,” he said. “Our systems should be locked so anyone from anywhere in the world can’t just walk in the school door.”

The Verizon report noted that most cyberattacks are about money. Cybercriminals pursue information they can use to steal identities or passwords to access accounts. Besides accessing sensitive personal information, cyberattacks can disrupt or devastate a school district in many ways. For instance, attackers overwhelmed Salt Lake City’s school district by an attack in 2015 that brought down its websites, phone systems and online grading system. In Minnesota, an attack disrupted student testing, and in New Jersey, extortionists shut down a district’s entire network and held it for ransom.

These are the most common types of attacks:

**Phishing, social engineering or other end user attacks:** Attackers attempt to infiltrate a system through the end user, such as a teacher checking email. With phishing, an email from a deceptive address tempts the recipient to click on a link and input private information such as credit card numbers or passwords. Likewise, social engineering attacks use psychology to trick users into breaking security procedures, allowing attackers access to sensitive information.

**Hacking:** An illicit coder, or hacker, modifies or alters computer software and hardware to steal information or disrupt usage.

**Malware:** Short for “malicious software,” malware is unwanted software installed on a computer without consent, and often with the purpose of gathering information or controlling the device. Viruses and worms are examples of malicious software that are often grouped together and referred to as malware.

**Crimeware:** This category of cyberattack covers the use of malware that doesn’t fit into a more specific pattern.

**Denial of Service:** DoS attacks use botnets, a “zombie” army of infected computers working in concert to overwhelm a network with malicious traffic, which can cause the entire system to crash.

**Ransomware:** Malicious software designed to block access to a computer system until victims pay a sum of money. Ransomware is one of the most popular attacks currently used against schools.

**Internet of Things (IoT):** Devices from the Internet of Things include webcams, security cameras, air conditioners, printers and anything connected to the Internet that can
be infected and turned into a botnet to drive large amounts of traffic and cause the system to crash. While IoT attacks are not common, the possibility of problems will increase as bases, sprinkler systems and other devices in a school district go online. The sheer size of some school districts makes them tempting targets for hackers, cyberthieves and online extortionists. Moreno Valley School District is one of California’s larger school systems, with about 34,000 students, 14,000 laptops and desktops, and 28,000 Chromebooks, but Barnett doesn’t have the staff to keep them all updated. That makes the technology more vulnerable to hacks and malware problems. “We think we’re at the little schoolhouse on the prairie, but we are running some of the biggest networks in the cities and becoming very vulnerable to cyberattacks,” he said.

Ten years ago, few technology departments, let alone school districts, had cybersecurity on their list of IT priorities. Today, just about everyone ranks it as one of the biggest problems facing information technology. And it’s not cheap. The Wichita School Board estimated the cost of implementing a proper cybersecurity program to be $2 million. Not many districts have that kind of cash on hand, making it hard to establish a robust set of cybersecurity policies and practices with up-to-date defenses. “The ideal would be to have a dedicated person for security, but districts might not be able to justify it,” said Laura Iwan, chief information security officer for the Multi-State Information Sharing and Analysis Center (MS-ISAC), an organization that facilitates collaboration and information sharing among members, private-sector partners and the U.S. Department of Homeland Security on cybersecurity threats. “That’s because their size and workload may not support the salary of a full-time security person, making it more practical to share a dedicated person across multiple school districts. “I look at security as somewhat like an orchestra and a conductor,” she said. “If you don’t have a conductor, everyone may be playing the same song, but not playing it well enough because they don’t have someone to guide them through the music. The key is that someone be responsible and accountable for establishing a cohesive program.”

MS-ISAC publishes a nontechnical guide to getting started in cybersecurity that focuses on institutional and organizational checklists for executives and managers. Schools can use the guide to recognize a problem, and then set up daily, weekly and monthly tasks to keep systems secure. Some states are trying to prod schools into action to prevent cyberattacks. Missouri performs audits to help schools in the state identify where they must improve. Kevin Carpenter is IT director at Boonville R-1 School District, which participated in Missouri’s Cyber Aware School Audit. Boonville R-1 has 1,500 students and five school buildings, and employs two IT staff, Carpenter and his assistant. The two are responsible for IT for the entire district, including monitoring cybersecurity. The audit spurred Carpenter to create some policies and procedures for monitoring and responding to cybersecurity threats. He developed a disaster recovery program, a comprehensive life cycle policy, incident response protocol, a regular forced password change and a minimum password length. This year, Boonville purchased a cybersecurity training video course for its staff.
While most school districts can’t afford a full-time cybersecurity position on an already-limited public education budget, they still have the responsibility to do the best they can with the staff they have, said Carpenter. “It’s the kind of thing that can be easily overlooked in the day to day without a clear policy and procedure,” he added. “You don’t want to be that district that makes the headlines for having an incident.”

The Orchard Farm School District is another Missouri district that underwent security auditing. IT director Bill Niemeyer oversees the district’s five schools and one full-time security administrator responsible for all computer and network security. School districts that lack a full-time cybersecurity employee can often get their district security administrator to work with contractors and automated systems to protect data, Niemeyer said. Orchard Farm utilizes a Security Information and Event Management (SIEM) architecture monitored by a third party. Niemeyer said SIEM has become a cost-effective and valuable tool for managing cybersecurity threats.

Even though Orchard Farm has several layers of technology in place to defend against attacks, the most important layer is the end user. “Security is everyone’s job,” he said, not just the job of one person in the technology department. “Districts need to create a culture that champions cybersecurity.”

Niemeyer recommends setting attainable goals for teachers, staff and students, such as a “clean desk” policy, regular password changes, and creating consistent engaging ways to incorporate cybersecurity topics into daily classroom use. Further, he suggests that all school districts should join CoSN and participate in its new privacy initiative called the Trusted Learning Environment (TLE) Seal, a set of best practices to safeguard student data.

WHO’S IN CHARGE?

California is an example of how one state provides assistance to its school districts as they beef up cybersecurity. Through a partnership between CETPA and a state-funded network connectivity program called K12HSN, California is offering free cybersecurity and network management professional development through the Technical Assistance Professional Development Program. It’s an approach that is gaining traction and one that IT education professionals say is needed. Moreno Valley’s Barnett said the program includes a combination of district IT staff policies and a subscription service. Having a third party who can come in and help districts recover after an attack will be an important part of the equation, he added.

While hiring a cybersecurity professional is, perhaps, the best answer to protecting a school’s data and networks, tech education professionals can follow several well-regarded procedures to reduce the chances of a breach or successful attack:

- **Constant vigilance**: Log files and change management systems can give early warnings of a breach. Also, encrypt data so that it is useless if stolen.
- **Back up regularly**: If your network is attacked, a recent backup can help you get back to full capacity quickly without having to pay a ransom to cybercriminals.
- **Good patch management**: The first goal is to keep a clean machine that’s free from infections. Keep software updated and religiously apply security patches. Also make sure your Web filtering, firewalls and intrusion prevention programs are updated.
- **Secure the humans**: This is perhaps the most important piece, said Barnett. Keep data on a need-to-know basis. Use two-factor authentication. Professional development that trains...
staff to recognize social engineering and phishing can go a long way toward preventing attacks.

Security awareness training has become critical as staff mistakes trigger more attacks. Chief Technology Officer Mark Finstrom of Highline Public Schools in Washington gave an example from his district, which enrolls more than 20,000 students and doesn’t have a cybersecurity specialist. A payroll technician received an email from superintendent@gmail.com that asked for employees’ names, addresses and payroll information. The employee complied with the message, releasing personally identifiable information from nearly 2,500 employees in that attack.

Finstrom points out that the employee should have noted a couple of things. First, the email address didn’t come from a district domain. Second, the superintendent does not ask for payroll information via unsecure email. He explains that people have just become accustomed to doing everything online without always confirming the veracity of the email request. Following the incident, Highline instituted a phone call requirement before employees can release payroll data.

Some districts have started training staff by sending fake phishing emails to them to see if they get hooked. If someone does, they are rewarded with a short video that explains what to look out for in future emails. Free applications such as SecurityIQ and KnowB4 offer such training.

Finstrom has offered some of his own recommendations: Consult with vendors, read online articles from specialists, talk with your peers, and always confirm the answer.

“Knowing that threats will increase and become more complicated in nature, I believe we need to be extremely diligent to provide training and cross-training for staff,” he said. “While some districts may not be able to afford a cybersecurity specialist, the analyses of requirements, tools, options and communication requirements becomes something that every district must invest in.”

Cybersecurity in Higher Education

While the stakes are high for K-12 education, cyberattacks on higher education institutions have some additional complicating factors. Consider the research data held on networks at the nation’s universities, as well as the vast number of unsecured devices brought on campus.

Educause, a nonprofit association whose mission is to advance higher education through the use of information technology, listed information security as the No. 1 issue facing higher education in both 2016 and 2017. Yet many institutions, particularly small colleges, face the threats without a dedicated cybersecurity officer. Educause has published a Free Information Security Guide to help these institutions.

John Bruggeman is the only certified computer security staff member at the Jewish Institute of Religion, where he serves as the chief technology officer and information security officer for the seminary that has four locations. But he has three network staff members versed in computer security fundamentals and incident response and remediation. Bruggeman trained through sans.org, which focuses primarily on the technical security training arena. Additionally, Bruggeman contracts with local vendors who can provide incident response assistance.

The Jewish Institute of Religion’s first incident was a denial-of-service attack in 2001. While the incident didn’t result in a data breach, it motivated him to become certified through sans.org, as well as to present at national higher education computer conferences on the topic of cybersecurity.

Bruggeman recommends other small schools focus on three primary steps:

- Define your risk. What data do you have that needs to be protected?
- Develop a security policy. The policy documents will define the who, what, when, where, why and how of your security needs.
- Recognize that IT security is an ongoing process and that the whole school is involved.

What I learned from that first experience was that we, the internet, are only as strong as our weakest link,” he says. “Small schools like us can do a lot without a lot of money or a lot of staff. This is not a “technology” problem so much as it is an attitude and awareness problem.”

Cybersecurity in Higher Education

While the stakes are high for K-12 education, cyberattacks on higher education institutions have some additional complicating factors. Consider the research data held on networks at the nation’s universities, as well as the vast number of unsecured devices brought on campus.

Educause, a nonprofit association whose mission is to advance higher education through the use of information technology, listed information security as the No. 1 issue facing higher education in both 2016 and 2017. Yet many institutions, particularly small colleges, face the threats without a dedicated cybersecurity officer. Educause has published a Free Information Security Guide to help these institutions.

John Bruggeman is the only certified computer security staff member at the Jewish Institute of Religion, where he serves as the chief technology officer and information security officer for the seminary that has four locations. But he has three network staff members versed in computer security fundamentals and incident response and remediation. Bruggeman trained through sans.org, which focuses primarily on the technical security training arena. Additionally, Bruggeman contracts with local vendors who can provide incident response assistance.

The Jewish Institute of Religion’s first incident was a denial-of-service attack in 2001. While the incident didn’t result in a data breach, it motivated him to become certified through sans.org, as well as to present at national higher education computer conferences on the topic of cybersecurity.

Bruggeman recommends other small schools focus on three primary steps:

- Define your risk. What data do you have that needs to be protected?
- Develop a security policy. The policy documents will define the who, what, when, where, why and how of your security needs.
- Recognize that IT security is an ongoing process and that the whole school is involved.

What I learned from that first experience was that we, the internet, are only as strong as our weakest link,” he says. “Small schools like us can do a lot without a lot of money or a lot of staff. This is not a “technology” problem so much as it is an attitude and awareness problem.”

Cybersecurity in Higher Education

While the stakes are high for K-12 education, cyberattacks on higher education institutions have some additional complicating factors. Consider the research data held on networks at the nation’s universities, as well as the vast number of unsecured devices brought on campus.

Educause, a nonprofit association whose mission is to advance higher education through the use of information technology, listed information security as the No. 1 issue facing higher education in both 2016 and 2017. Yet many institutions, particularly small colleges, face the threats without a dedicated cybersecurity officer. Educause has published a Free Information Security Guide to help these institutions.

John Bruggeman is the only certified computer security staff member at the Jewish Institute of Religion, where he serves as the chief technology officer and information security officer for the seminary that has four locations. But he has three network staff members versed in computer security fundamentals and incident response and remediation. Bruggeman trained through sans.org, which focuses primarily on the technical security training arena. Additionally, Bruggeman contracts with local vendors who can provide incident response assistance.

The Jewish Institute of Religion’s first incident was a denial-of-service attack in 2001. While the incident didn’t result in a data breach, it motivated him to become certified through sans.org, as well as to present at national higher education computer conferences on the topic of cybersecurity.

Bruggeman recommends other small schools focus on three primary steps:

- Define your risk. What data do you have that needs to be protected?
- Develop a security policy. The policy documents will define the who, what, when, where, why and how of your security needs.
- Recognize that IT security is an ongoing process and that the whole school is involved.

What I learned from that first experience was that we, the internet, are only as strong as our weakest link,” he says. “Small schools like us can do a lot without a lot of money or a lot of staff. This is not a “technology” problem so much as it is an attitude and awareness problem.”
School Broadband Breakthrough

School broadband access and affordability have come a long way in the last few years, thanks in part to the help of governors and service providers.

The second annual 2016 State of the States report from EducationSuperHighway revealed a 40 percent drop in what school districts pay for Internet service. The report includes analysis of data representing 10,499 school districts and more than 38 million students from the federal E-rate program that the FCC governs. E-rate provides discounts on telecom, Internet and Wi-Fi for school districts based on the financial needs of the students they serve.

Funding has had a big impact on speeding up broadband access while keeping it affordable. The FCC caps federal funding for E-rate at $3.9 billion. With state-matching funds and E-rate discounts, school districts and service providers have been able to work together to build fiber networks to handle high speeds for years to come.

The cost of broadband is dropping

$11.73 2015 median price for 1 megabit per second

$7 2016 median price for 1 megabit per second

The availability of high-speed broadband is increasing

30% of school districts met the FCC’s minimum goal of 100 kilobits per second for each student

88% of school districts met the FCC’s minimum goal of 100 kilobits per second for each student

---

The cost of broadband is dropping

$11.73 2015 median price for 1 megabit per second

$7 2016 median price for 1 megabit per second

The availability of high-speed broadband is increasing

30% of school districts met the FCC’s minimum goal of 100 kilobits per second for each student

88% of school districts met the FCC’s minimum goal of 100 kilobits per second for each student
Governors support broadband access and affordability

2015: **40 state governors** committed to promoting high-speed broadband in schools

2016: **34 of those** state governors acted on broadband access and affordability

---

**7 states** now provide matching funds for fiber network construction:

- California
- Massachusetts
- New Mexico
- North Carolina
- New York
- Oklahoma
- Maine

---

The number of schools **without a fiber-optic connection** has dropped significantly

- 2015: **9,500** schools without fiber-optic connections
- 2016: **3,723** schools without fiber-optic connections

The number of schools **without Wi-Fi** has dropped by half

- 2015: **31,959** schools without sufficient Wi-Fi in classes
- 2016: **15,092** schools without sufficient Wi-Fi in classes
Hardin-Simmons University in Abilene, Texas, has more than 2,400 students, and they require — and expect — a lot of network support. Gone are the days when students showed up on campus with just a PC to plug into the campus backbone. Today, the typical student might have multiple devices, most operating wirelessly and at all hours. In addition, they are watching TV, streaming video and using phones and other types of technology that operate across the college campus residential network. This network typically provides Internet connectivity for students living in residence halls, along with cable TV/video services, phone services and support.

To manage the increasing demands, Hardin-Simmons has turned to outsourcing. Apogee, which provides residential networks (ResNet) to college campuses around the country, manages all of the college’s residential network services and makes sure that students have the access points and bandwidth that they need. Hardin-Simmons’ situation is typical of what’s happening at colleges and universities, where 83 percent of campuses now provide a wireless connection, almost double from 45 percent in 2013, according to a 2016 study of ResNets by the Association for College and University Technology Advancement (ACUTA) and Association of Colleges and University Housing Officers-International (ACUHO-I).

That kind of rapid development has put a strain on resources. One fast-growing option is to outsource. Currently 44 percent of schools are outsourcing or considering outsourcing. Double the number from 2013, according to the State of ResNet Report.

Travis Seekins, the Hardin-Simmons associate vice president for technology services, notes that the decision to outsource was easy when they looked at what was at stake. “We can’t afford to not do this well. This is a key component in the world today in the lives of our students,” Seekins said. “We don’t have the personnel to handle all the students we have.”

A Doubling in Bandwidth Speed

In today’s high-tech, real-time world, colleges have to respond quickly to increasing demands for greater bandwidth. Nearly two-thirds of universities provide bandwidth of up
to 3 gigabit per second to the ResNet, up from 500 Mbps in 2012. The study also found that 83 percent of campuses provide a strong wireless connection, a figure that’s nearly doubled in the past four years. Yet the need for bandwidth and superior Wi-Fi connections continues to rise to keep pace with the range of devices students use.

Along with this increased demand, universities face a challenge to provide enough technical support for resident students. The ResNet study reported that only 13.6 percent of schools provide constant support, and the only resource available to students at more than three-quarters of schools is access to online resources, like a FAQ page. Most universities continue to offer onsite or call centers for support, and a growing number are incorporating support via live chat and social media.

Another key challenge is security, where many universities and colleges have gaps. In fact, the report shows that a fifth of colleges don’t have an information security and internal audit team, even though they say security is a high priority. Half of colleges have a security team of four or fewer staff, while a fifth of institutions have a team of five to nine staff members.

Funding the growing ResNet demand remains a huge challenge as well for most colleges and universities. An increasing number of colleges expect wireless costs to continue to increase, with half of institutions reporting a 5 percent or more expected rise in cost within the next two years. While 47 percent of institutions reported an increase in ResNet funding, that number is down 7 percent from last year. The annual ResNet budgets closely align with the size of the institution. About 44 percent of colleges and universities have an annual network budget of less than $750,000; one-third have a budget between $750,000 and $2.5 million, and 22.5 percent spend more than $2.5 million, according to the report.

Funding models differ depending on the size of the institution, with nearly 42 percent reporting that the money comes from central university funds because of its status as a core university service. Some universities levy a technology fee to cover the growing costs of ResNet services.

To stay ahead of the curve when it comes to providing ResNet services students want and need, college strategic plans have become critical...
Converge » SPRING 2017

To operational success. Over the past three years, the number of institutions that have a ResNet strategic plan has increased 24 percent. But even with plans in place, findings show they aren’t often updated, and transparency is limited. In fact, 36 percent of housing and business officers reported that they do not have access to benchmarking information. What’s more, nearly a quarter of business officers and 22 percent of housing officers reported they don’t meet with their IT departments at all.

To Outsource or Not

The rapid increase in mobile devices and the bandwidth-hungry apps that go with them has put a strain on the management of infrastructure, technology and the related costs, according to the ResNet report. The result has been an increasing appetite for outsourcing. As noted before, the number of institutions outsourcing or considering outsourcing their ResNet services has doubled in three years.

Georgetown University recently finalized a partnership with Verizon Communications to overhaul its entire wireless infrastructure over the course of five years. Judd Nicholson, vice president of information services and chief information officer at Georgetown, explained that this partnership will allow the university to not only update existing infrastructure from building to building throughout the campus, but will also provide added support to keep technical capabilities on the cutting edge. The second phase of the initiative involves connecting network devices to Verizon’s network operations center, which monitors and maintains the equipment around the clock. “This will enable us to keep internal network engineers focused on optimizing performance, research networking, and network cloud migration initiatives,” Nicholson said.

While outsourcing proves to work for larger campuses, smaller campuses with less demand are finding solutions internally. For example, two of the largest regional campuses at Indiana University house roughly 400 students in residence halls at each location. To keep up with wireless demand on one campus, the university provides students access to two separate secure wireless networks—one for academic work and another for gaming, streaming and other extracurricular activities. The other regional campus is simply equipped with hospitality access points within each residential unit because the demand for wireless is even smaller.

According to Elizabeth Van Gordon, who works in the Office of the Vice President for IT and CIO for Indiana University, all regional campuses operate under a 10-year life cycle replacement model, which helps the university stay ahead of the technology curve by at least three to five years. Those costs are accounted for through auxiliary services in residence halls and technology fees on main campuses.

Regardless of university location or size, student behavior indicates that the demand for efficient, accessible wireless services will only continue to increase. “I would speculate that demand will only become greater, especially as wearable technology begins to appear,” Van Gordon said. Students, teachers and staff often come to campus with multiple devices, sometimes up to four at once. With that in mind, there’s no doubt this will continue to be a critical issue within higher education. Or as Van Gordon puts it, “it’s not over yet.”
PROTECT YOUR IDENTITY BY PRACTICING SAFE HABITS ONLINE.

STOP other people from accessing your information by using strong passwords. THINK before you download apps you aren’t familiar with. CONNECT with friends safely online by checking your privacy settings regularly.

Visit www.dhs.gov/stopthinkconnect for more information on how to get involved with the Stop.Think.Connect. Campaign.

Homeland Security
John Morgan, a career in education was a natural fit. The director of educational technology grew up inspired by his mother, stepfather and grandfather, who also dedicated their lives to enriching students’ experiences. Today Morgan is impacting the minds of students and teachers through technology at Capistrano Unified School District in Southern California.

He graduated from the University of Delaware with a degree in chemical education, then taught chemistry in Edgewood, Md., before moving with his wife to Southern California to continue teaching. Morgan perfected the art of teaching science to students who hated it. But his natural ability to teach others was not the only thing that set Morgan apart as a technology leader. His approach to teaching a group of students is centered on individualized learning. The father of four said that he realized his children — ages 6, 9, 17 and 19 — all require different learning tools.

“When you get to a certain number of kids, you start to realize that none of them learn the same,” he said. “At the same time, there’s no reason none of them should not be successful. I think education technology allows you to differentiate for that.”

Morgan said he does not want to be the smartest person in the classroom — even as the teacher. The smartest people in the classroom should be the students. But they need technology tools to help expose them to knowledge outside of school and help them discover their genius.

During his time in the classroom, Morgan constantly requested new technology from his principal. At the same time, the district’s Chief Technology Officer Jeremy Davis was looking for 25 teachers to pilot Chromebooks in classrooms. Morgan made the short list.

“A chemistry class wasn’t my first choice,” Davis said. “But the principal said, ‘We know the chemistry department will ensure that they get used.’ John made an impression.”

John Morgan is capitalizing on his experience teaching chemistry to help other teachers mix technology into student learning.

By Jessica Renee Napier
Chemical Bond Technologist
About 20 months ago Davis appointed Morgan as the district's director of educational technology. Teachers can look to Morgan’s efforts during his teaching career as proof that it doesn’t require a technology genius to make new tools a success in the classroom.

When Morgan took on the technology leadership role, he helped teacher, social science teacher and English teacher. During the first school semester, Morgan's team conducted one technology lesson study with this group and then checks in with them throughout the semester. During the second semester, these four teachers regroup and add three additional teachers from each subject area to the cohort. With more interacting on Twitter, Shorr and Morgan met in person at the Center for Digital Education's 2015 Digital Education Leadership Conversation, where they facilitated a discussion.

Morgan has a way of making it easy for superintendents to learn about new ideas without feeling threatened or scared, Shorr said. And he also created a challenge for teachers so they could stay focused on instructional methods. For example, teachers could think of a tool such as Google Docs and come up with 100 methods to use that technology to support learning. After teachers narrow down that list of 100 possibilities, Morgan and his team support the teachers in implementation.

"What I love about John and his approach is that he and his district are really tightly focused on instructional experience first," Shorr said. "That comes in a) not buying stuff until you figure out that there's a hole and that a certain piece of technology could fill it; and b) taking the tools that teachers are already comfortable using."

Davis, who in addition to being Morgan’s boss is also his friend, shared Shorr’s sentiment about using technology to support education. He said that he and Morgan do not implement technology for the sake of introducing another piece of equipment; instead technology is introduced to enhance teaching.

"There’s no such thing as a technology lesson or a technology standard. It is 100 percent intertwined and integrated, which lets the teachers be awesome and lets the students learn amazing things."

"In order to get anything to stick, we can’t just be the best at technology — we have to be the best teachers."

John Morgan, director of educational technology at Capistrano Unified School District

Morgan’s Other Loves

- Riding bikes
- Being outside (he was even with his 6-year-old daughter at Rubiea Park while conducting the interview for this story)
- Working on cars
- Spending time with his family
- Finding problems to solve

Morgan couldn’t stand that, so he worked with two other staff members to get rid of most of the tech tools and simplified the program. Together, they developed a lesson study model in which teachers work collaboratively in cohorts at their schools. It begins with the principal at each school identifying a math teacher, science collaborators, the cohorts develop four to five lessons spaced and share one another. Over a year and a half, most of the staff members at the district’s middle schools completed the program, totaling 20 schools where teams of teachers are confidently changing education for the better. "I couldn't care less if we’re using the most innovative tools," Morgan said. "It’s about the innovative teaching practice. If you try to show someone some technology, they’ll say, ‘You can do it because you’re the tech people!’ In order to get anything to stick, we can’t just be the best at technology — we have to be the best teachers.”

This kind of outside-the-box thinking that caught the attention of Jeremy Shorr, director of technology innovation and early childhood education for the Teaching Institute for Excellence in STEM. After

After the overhaul, teachers would express interest in learning some type of technology. Then the education technologists would show teachers a host of different tools, hoping that some of them would stick. Teachers left the training exhausted, their minds spinning with all the tool choices for each lesson.

Morgan’s Other Loves

- Riding bikes
- Being outside (he was even with his 6-year-old daughter at Rubiea Park while conducting the interview for this story)
- Working on cars
- Spending time with his family
- Finding problems to solve
Thinking about student safety is more complex than ever before. Sure, kids need to be physically safe at school, but what about the safety of their personal information? That’s exactly what parents and civil liberties advocates have begun asking in Colorado and Connecticut as education becomes more dependent on technology services.

Denise Maes of the Colorado ACLU recently voiced her concerns to Colorado Public Radio, saying, “Once privacy is lost, it is almost impossible to get it back. Parents for the most part have no idea or remain largely unaware of how much data is collected about their children, with whom it is shared, if it’s shared at all, where it’s stored, how long it’s stored and why it’s even collected in the first instance.”

To address this concern, a growing number of states are passing significant student data privacy legislation to protect students and arm parents with more knowledge on data activities. While most agree the laws are a step in the right direction, they also come with challenges for local schools that state education departments are helping them tackle.

Unique reporting requirements

Last year, lawmakers in 15 states passed 19 student data privacy bills, according to the Data Quality Campaign, a nonprofit focused on improving the quality and utility of data in service of the public good.

New student data notification requirements shift a heavier administrative burden on school districts, but state departments are stepping up to help.
on the use of student data. Two bills in particular stood out for their reporting and notification requirements.

In Colorado, House Bill 16-1423 specifies additional responsibilities for the state education department, state board of education, local schools and contract service providers to follow, and outlines parents’ rights. For example, the state education department is responsible for sharing sample student information policies and contract language as well as training local school employees this year.

The training component is crucial. “Without training, all of the laws that have passed are just words on paper,” said Amelia Vance, policy counsel on education privacy for the Future of Privacy Forum. “They have to be implemented in schools every day as teachers are dealing with students and data on the ground.”

The Colorado law requires school districts to post online a list of the vendors they have contracts with, the actual contracts, the tools that educators use on demand and the types of personally identifiable information they collect so that parents and guardians can access them. They also need to list providers that they stopped using because of privacy reasons.

In Connecticut, Substitute House Bill 5469 includes a number of sweeping data privacy requirements, including a mandate that local and regional education boards sign a written contract with service providers whenever they share student data, and lay out what should be included in those contracts. It also specifies what education service providers can do with student data and establishes a security breach procedure for them to follow. The law created a student data privacy task force to study issues including development of a toolkit that local and regional education boards can use, and training strategies for educators and contractors that other states have used successfully.

The legislation requires local and regional boards of education to notify parents and students electronically within five business days about a new signed contract that affects them – a provision not usually found in other states’ privacy laws. These notices can number in the hundreds, flooding parents with emails, Vance said.

So far, that hasn’t happened in Connecticut. Dr. Kimberly Norton Butler, a parent advocate who pushed for the law, said she has yet to receive a single email, and is not aware of parents encountering an overwhelming amount of notifications. Jennifer Jacobson, a parent who lives in Fairfield County, agrees and has only received approximately five emails since the bill passed. Because compliance seems to waver from county to county, her biggest concern with the bill is ensuring that the mandated taskforce can help streamline implementation across the state.

Life under the new laws

With both the Connecticut and Colorado laws now in effect, schools and education departments are working through the implementation process, which has revealed some practical challenges.

In Colorado, one problem is how schools balance student privacy while encouraging teachers to find apps and Web tools that will work for their classrooms. Identifying all the apps and subscriptions that educators can use is a big undertaking because Denver Public Schools gives teachers flexibility and autonomy to pick their own, according to Kirk Anderson, the district’s former educational technology director and current director of MyTech, a district initiative designed to provide each sixth- through 12th-grader with a computing device to take home.

“Teachers are really unaware of this concern so far, and they’re just now getting up to speed,” he said. Anderson and Josh Allen, director of technical architecture, have developed an online catalog that includes tools that teachers report using in their classroom, as well as tools that the district has implemented. Based on the catalog, the team
generates a website for each school that outlines the tools and data being used so parents can easily access it. But for some parent advocates, this simply shifts the transparency responsibility to parents. Rachael Stickland lives in Colorado and is a co-founder of the Parent Coalition for Student Privacy. She was disappointed with many aspects of the law. “The passive, post-it-publicly approach assumes you have engaged parents in understanding that you need to look at these contracts, which can be challenging because they can be full of legalese and are sometimes 75 pages long,” she said. Instead, she sees a need for better enforcement of the law that establishes clear penalties for companies that operate outside of the law.

In Connecticut, Glastonbury Public Schools has taken a more restrictive approach when it comes to learning tools. Glastonbury's IT team provides iPads for students grades K through 12 and controls which apps they can access. While the digital solution makes it easier to report the paid apps and subscriptions they’re using in the classroom, it’s still not easy to track down the online services that teachers use after accepting the operator’s terms of service.

School technology specialists work with staff members to make sure they report the use of these services, explained Brian Czapla, director of educational technology in Glastonbury. Principals and curriculum directors have protocols to follow to make sure that educators go through the technology department for approval. The district also created a Data and Privacy Council, which developed a student data privacy toolkit for Connecticut school districts that helps them effectively implement the new data privacy legislation.

The law’s written contract requirement may put some students at a disadvantage if they use services that don’t require a contract. For instance, some services, which include dictation tools for students with special needs, ask users to click a button saying they accept the terms of service before using it. These students typically have an individual education plan that tailors learning objectives to their needs, and because their needs differ, they may need to use different services. “From a school side, having to negotiate an individual contract for each student is really time-consuming and not necessarily what they’re equipped to do,” Vance said.

States step up
In 2016, the Connecticut State Department of Education (CSDE) launched a Data Privacy Summit to share resources and information with districts about the new law. The CSDE has also partnered with the Commission on Educational Technology in the state's Department of Administrative Services to develop collaborative solutions such as statewide contracts for some of the most commonly used service providers in Connecticut, including Google and Microsoft. These groups are considering developing a statewide registry that allows operators to certify compliance with the data privacy legislation, said Abbe Smith, director of communications at CSDE.

In Colorado, the Department of Education has provided sample contract language for schools to use with vendors, along with annotated documents that tie the contract language to the new legislation, and guidance documents to ensure that educators fully understand the law, said Jill Stacey, the department’s data privacy analyst of information management systems. The department is also focused on outreach and plans to implement regular town hall-style meetings that cover privacy and security topics; it also serves as a platform to share and gather information on best practices.

Stacey noted that the department plans to launch some larger projects to provide long-term support, including a suite of more than 40 information, privacy and security policies that districts can incorporate as appropriate. A privacy and security training program is also underway for teachers, administrators, board members and executive team members.

State support to implement these laws is critical. “It’s hugely important that we provide these services to schools because they are challenged with resources, and the more we can help them, the better,” said Stacey.

“Protecting students, their parents and teachers are all very important.”