Issue Brief

School Network Moles and the Emotional Toll of Breached Data Security

Executive Summary

Be prepared for a wide gamut of emotions as a school executive if you find you have a data security breach. You can't just ignore it, that's against the law. Your first emotion will be horror. It gets worse from there. You could have a network "mole" from the inside of your network, something you may think there is nothing you could do about. As just one sordid example of the oversight, a breach may compromise some student's IQ scores causing bullying by fellow students, resulting in tears and sobbing by the affected student later in the principal's office as they plead for answers to this injustice. Then comes the lawsuit.

The thing about data privacy and security is that it is both personal, being as precisely real as our very name, and impersonal, because a name or number is a mere label of identity put out there on the Internet and blurred out of our reach. To our minds a digital identity

"The secret of education lies in respecting the students"

Ralph Waldo Emerson

In this Brief

Considering the high value of hacked data on the open market, the threat of an ever-present data breach is a fact of life for school districts. The effects of a data breach can be far-reaching, including the loss of privacy for students, the loss of financial records of employees, almost-irreparable damage to the district's reputation and the loss of millions of dollars to the defense of lawsuits. And that doesn't even include the emotional toll to the district's staff.

is a separate electronic blob of numbers and letters skittering around, a sort of mini-me existential threat connected by energized wires to anywhere. Companies whose networks or data practices are compromised serve as the conduit to undefined hacker malice and a general evil that cannot be easily fought against. They are big, and we are individually small, so we eat the stress of it whole and trudge on. Yet a school can be reached and fought against, being physically close with actual humans who can be screeched at, demoted or fired. With schools, there are dramatically heightened and focused emotions from parents. Because, after all, it's the safety and security of their children.

This paper is a primer on the data treasures you are really protecting as a school, the points of threat, handling the emotional human side, and what's next in practical network security steps.

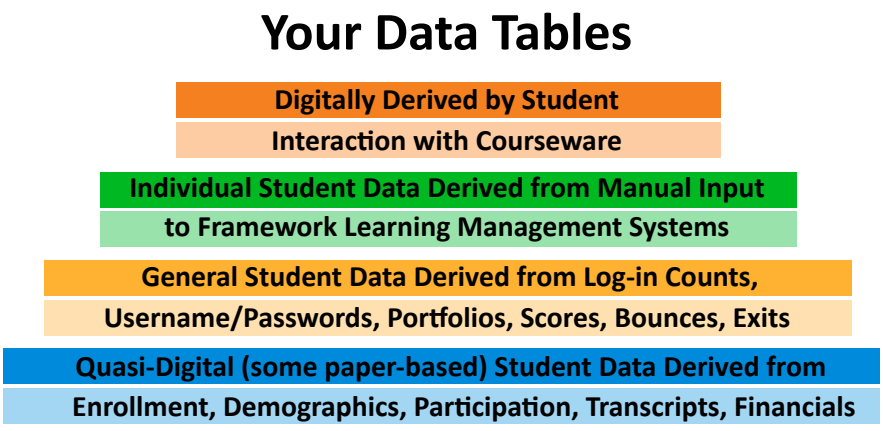
Your Data Treasure Described

What data do you hold as a school or district that is a risk? You'll be surprised to know the full depth of data you have would make hackers drool.

From enrollment, placement and testing, schools typically have data fields with age, demographics, financials, transcripts, what course or extra-curricular participations a student engages in, detailed health and psychological profiles, any special needs plans, donation records, credit card and social security numbers and even political affiliations. That's just the baseline.

Above that, your tech department has data fields related to all staff and student usernames and passwords, student submittal portfolios, scores, log-in counts and course bounces (incompletes) and exits from any courseware with time stamps. All of this data together can virtually track students for their location in real time.

If your school has a Learning Management System (LMS) or resources such as Google or Microsoft Office 365, you have a whole lot of manually input data that is important to the continued operation of a school. Those resources that exist in the cloud pose additional risk from that connection as well as loss to hackers targeting those entities. Google, for example, is not without breaches including one in 2017 that launched email phishing attacks virally across users. A bug found in 2018 in the Google+ platform gave third-party developers access to some 500,000 individual accounts with users' names, emails, birthdays, pictures, work history and relationship status since 2015. Google staff were aware but decided not to notify users according to the Wall Street Journal.



A final level of data being collected that should be concerning is being done inside the more sophisticated digital curriculum software that "sees" what a student is doing inside the software as they are doing it, how long they take to answer questions, what they may do poorly and more. These courseware systems are frequently subscription sites with a lot of data being derived from student interaction that could increase risk for them later in life in ways that are yet unclear.

Risks & Costs Described

Certainly not all school security breaches are reported in the media, but many are. An up-to-date list can be found at *https://k12cybersecure.co m*. The first risk is the fact that schools

can be victims of ransomware, email phishing scams and employees can misplace laptops full of important data. Student and unknown hackers can also gain access to systems to post misguided photos on school websites, change grades or erase data. Worse, students can end up going to jail over posting violent threats and pictures of terrorists, pretending to be faculty by hacking an email system administration, or using school networks to write threats to important political figures online thus bringing the attention of the FBI or Secret Service. Large numbers of financial records and personally identifiable data that includes names, addresses and social security numbers can be stolen.

What are the other risks and financial impacts of a security breach to schools?

Investigation

First, when a breach is suspected or confirmed, the school has to determine what caused it, what and how much information was disclosed and if the system is still compromised. To comply with state notification laws to people whose records have been affected, the school has to determine if there has been unauthorized access to personally identifiable information. This is tricky because access to multiple systems could disclose disparate data that hackers could match up, things like credit card data with home addresses and social security numbers that together are the trifecta for stealing identity. Laws you may not be in compliance with could include the Children's Internet Protection Act (CIPA), the Children's Online Privacy Protection Rule (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA). Other State and Local laws may also apply.

You will probably need digital forensic specialists to handle this type of investigation, an expense estimated between $10,000 and $100,000 or more.

Remediation

Your tech department may need to shut down all of your systems, purge all compromised files, reload any necessary operating systems and back-up files. Sometimes this results in days or weeks of lost data, and a requirement for totally new hardware if the forensic team cannot determine if the malware is totally purged. They must also confirm that the hacker's access is now blocked. All of this can be an operational expense in the tens of thousands of dollars.

Notification

With a confirmed data breach, schools should retain an attorney to assist with what to say about the handling of the breach and navigating the breach notification laws. Failing to

Your tech department may need to shut down all of your systems, purge all compromised files, reload any necessary operating systems and back-up files. Sometimes this results in days or weeks of lost data, and a requirement for totally new hardware if the forensic team cannot determine if the malware is totally purged.

If credit-worthiness for students, parents or faculty was put at risk, a school may need to provide credit monitoring

comply with the notification laws within certain timeframes (the norm is 72 hours) may subject a school to statutory fines that accrue on a daily basis, especially in California, Arkansas, Georgia, Indiana, Montana, North Dakota, and Washington where security and privacy laws do not exclude public sector agencies. Notification that can't be done directly to affected users must include posting on your website, emailing everyone affected, and telling major state-wide media. This cost can also be in the tens of thousands for schools.

Credit Monitoring

If credit-worthiness for students, parents or faculty was put at risk, a school may need to provide credit monitoring for a reasonable term for all whose information was disclosed in the breach. This cost could be in the several thousand to tens of thousands a year.

Understanding the Human Side of Breaches

When it comes to security breaches, the human element is often the most overlooked and least understood. John Connolly is Chief Technology Officer at Consolidated High School District 230 in Orland Park, IL. Connolly's team does all they can to prepare for possible security breaches, but says it is difficult to prepare for every scenario. "Our district has reviewed different breach scenarios, confirmed our insurance and legal obligations, and discussed communication and action items in the event of a breach," said Connolly. "Even with this in place, no organization can be fully prepared as each breach is unique."

Even the thought of a data breach can bring up strong emotions. "The emotion that comes to mind is feeling exposed and vulnerable...a feeling like there is a criminal in your house, your comfort place, trying to take all of your stuff." Connolly warns that if a breach does happen, it is important to be compassionate. "Empathy in our personal lives we have all been involved in a breach and let's face it, it will continue to happen. Understanding how we feel and what we expect can help a district or organization act when a breach occurs. Planning ahead of time with breach scenarios is one critical step."

Barbara Haeffner is the Director of Curriculum and Instructional Technology for Meriden Public Schools in CT. She is keenly aware of the impact that even the threat of a breach may have on her staff. "Most people become anxious – they thought it never would have happened to them. What data was breached? How will this impact other accounts or aspects of their lives? Also, people feel powerless, it is out of your control once it happens and all you can do at that point is mitigate damage. It is unsettling when you feel like you have very little control."

Haeffner feels confident in the way her organization would handle an investigation, managing public notification, and legal liabilities. "We have the necessary people and strategies in place," she said. "We have dealt with some situations on a smaller scale and have had success. The true test would be if there were a major breach."

When it comes to managing the human side of security of privacy breaches, Haeffner has the following advice: "Keep stakeholders informed. Be proactive and have users take steps to save their data to secure areas. Be supportive and listen if it happens. Though you may not be able to do anything at the time, knowing that you hear their concerns is extremely valuable."

Litigation
Despite being the victim, a school will incur additional expenses from any litigation costs, including settlements. Even successfully defending a case can run seven figures.

Penalties and Fines
A breached school may face fines and penalties from state and federal regulatory agencies, including but not limited Human Services (which regulates breaches of medical data).

The US Department of Education has stepped in and created the Privacy Technical Assistance Center to help educational institutions with data privacy and security practices. Among the center's resources is the Data Breach Response Checklist.

Human Cost
The human cost is harder to calculate but no less significant. A student who is bullied about having a low I.Q. because his or her individual education plan was hacked, experiences real emotional damage. The parents who now have to try to manage this pain for their child experience a sense of helplessness. A young girl who divulged an unwanted pregnancy in stolen email divulged publicly has her life robbed of private decisions. Ruined or fired staff over the whole ordeal feel victimized by something they couldn't control. IT staff feel attacked, overworked during the emergency, and resentful that they probably weren't given enough tech budget to more adequately prepare or avoid the problem. Administrators feel defeated over the costs redirecting important funds away from teaching and learning into investigations and liabilities. The human toll of a data breach is hard to put a price on, but it is present nevertheless.

They say that data is the new oil, a phrase designed to show the value of data in the new world economy. If that is true, then professional and amateur hackers alike have adopted the mantra of "Drill, Baby, Drill," attempting to fill their coffers with exabytes of black gold and Texas tea.

Every industry is up for grabs, and lately, education has been particularly vulnerable. Just look at California's San Diego Unified School District, which fell victim to a phishing attack that led to the theft of more than half a million social security numbers, the first and last names of students and staff, their dates of birth, mailing addresses, home addresses and phone numbers. In addition, the hackers got student enrollment information including schedules, discipline incident information, health information, attendance records, transfer information, legal notices on file, attendance data and even staff payroll and compensation information including viewable paychecks, tax information, direct deposit financial institution names, routing numbers and account numbers.

Other school data breaches this past year include Florida Virtual School, Irvington School District and Victoria Independent Schools. The data has considerable value, and much of it will be sold through the dark web, the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

School systems are particularly vulnerable because of the sheer number of users and the complexity of their data systems, often containing hundreds of interlocking programs and moving parts. And while no system to date is hacker-proof, there are some basic steps that districts can do to improve their odds against a criminal-initiated data breach.

First and foremost, education organizations need to establish clear policies along with consistent, ongoing training for all personnel. One good place to start is the Trusted Learning Network, whose SEAL program, created with COSN, helps schools understand and safeguard against data breaches. Another good source for information is PRIVO, an organization specializing in child data privacy compliance.

Districts may want to enlist the help of a cybersecurity firm to make sure their data is as safe as it can be. Cybersecurity organizations like The Center for Internet Security, The Internet Security Alliance and The National Cyber Security Alliance are all good places for information on reputable firms that can offer assistance.

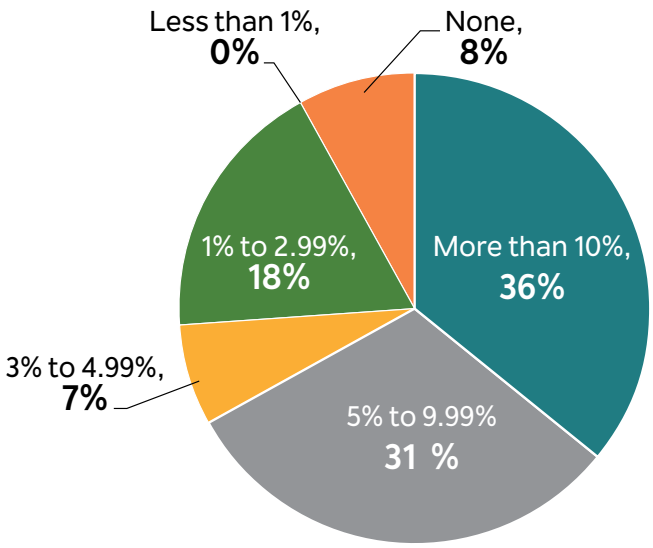
Moles and School Security

Schools are experiencing explosive growth in new threats with device roll-outs to students and teachers. Digital learning increases the total surface for cyber threats in a number of ways, and one of them is the least looked for and managed: the inside threat. The "moles" of school security are no less dangerous than marauding hackers managed at the front door by firewalls.

While most schools have at least some perimeter security like firewalls that detect outside threats or use policy to boot outside-in malicious email and viruses, that is not enough. Schools can stop threats faster by turning their entire internal district network into a firewall. Transforming the network into an adaptable enforcement domain enables the ability to detect threat behavior and shrink the time between detection and remediation.

Outside-In

Legacy networks are still prevalent in schools, with typical cyber threats somewhat managed like denial-of-service attacks, some email phishing, ransomware, spam, malware from viruses and other "outside-in" problems. Data shows spending on these sorts of security measures is increasing in schools (COSN Infrastructure Survey, 2018.) Still, 25 percent of schools spend next to nothing to less than 5 percent of their budgets on security measures. Keeping up with new hacker threats with an "outside-in" technology stance is hard because it is not designed to "see" internal application and user activity as untrusted. Schools are wide-open to a student or staff using USB memory sticks to introduce malware or other copying of infected files manually between users. Whole networks can be compromised when students use public hotspots or a home network that is unknowingly infected. As soon as that machine returns to the school network, it can infect all other machines because that traffic is not protected by the firewall. A new dependency on cloud-based services adds another risk because schools now have thousands of users logging into public environments where the use of perimeter security is less relevant as those services are "trusted" and allowed in.



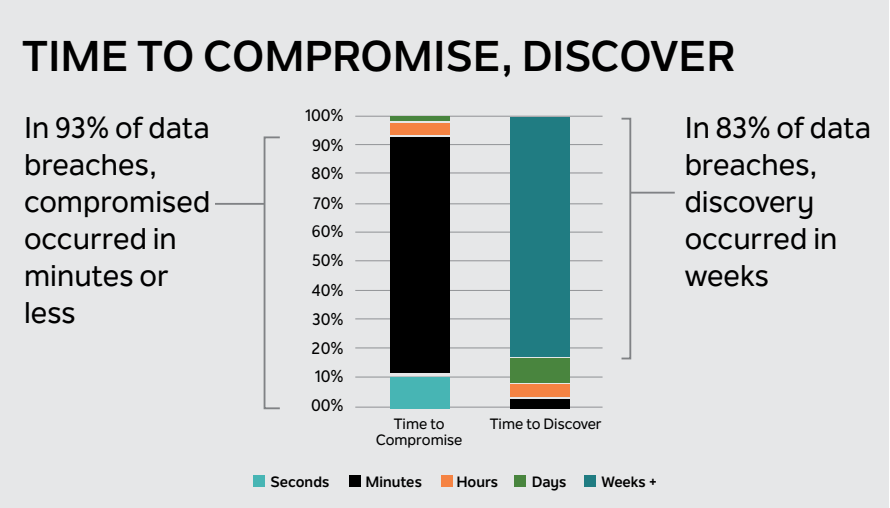
Technology Budget Allocated for Network Security

Source:CoSN Infrastructure Survey, http://cosn.org/infrastructure2018

Inside-Out

Schools now need to use their networks themselves as detectors of malicious activity, policing the inside traffic and not just the perimeter. This method is called Software Defined Secure Networks (SDSN) and makes every element on the network capable

of defending and enforcing policy. Because 93 percent of breaches occur in minutes or less while 83 percent of discovery takes weeks (Verizon 2016 Data Breach Investigation Report), risk and total loss to schools demands nothing less.

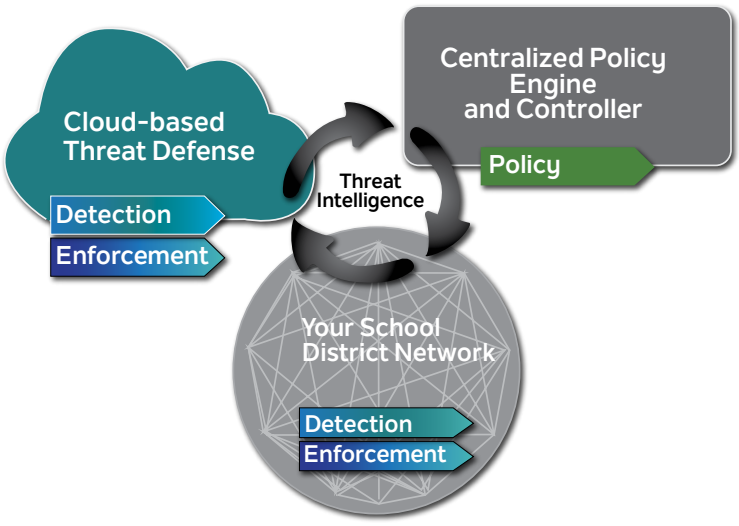


Source: Verizon 2016 Data Breach Investigation Report

With SDSN, all of a school's network switches, routers and firewalls do double-duty with inside enforcement. This amplifies the width of the "capture net" for malicious activity by harnessing more total "eyes" inside with a loop out to the "mind" of a cloud-based virtual, on-premise or blended scalable solution that analyzes all traffic. By minding what's happening on the inside of your school's traffic and combining it with threat intelligence reaped from a worldwide threat mitigation operation, your school can be fortified with software-defined policies before attacks even happen.

The gains from this sort of approach include:

- Leverage of a school or district's entire network and ecosystem for threat intelligence and detection, timelines and originations. This feature alone promises greatly reduced investigation costs, remediation and may reduce fines and penalties for breaches.
- Deployment of policy fortification to all points at once, including third-party devices such as multi-vendor network switches.
- Isolation of threats, which best utilizes typically scarce school security personnel.
- Adaptive and immediate protection, dramatically shortening timeframes between incidence and management of the threat. This feature promises a reduction of data losses and costs because previous to the complete offering of SDSN, security staff would have to work feverishly work to enforcing new security policies to each machine, switch or router manually. Total liabilities were exacerbated by these long and unnecessary-time intervals.
- Contextual and mobile-actionable alerts help school or district security staff stay on top of every new threat.



What to Do

Every school that relies on the Internet and computers for learning and administration is subject to a data breach or hack. It's not just a tech concern, but a human one fraught with emotional damage. From a purely financial perspective, it is good business to take reasonable precautions to prevent breach and have a response team ready for more than just the tech side. When regulators, staff and students start asking questions, a school can honestly say, "We took precautions and had a plan, and we understand how you feel." These things are not usually mentioned in response checklists, but where children are concerned, they can help mitigate the situation and lower the expense.

- As part of your incident response team, post someone to listen. Just listening to people's concerns can go a long ways in managing the fear and emotion your affected users will have.
- Consider saying "We're sorry." When the law already requires schools to notify users of the fact of a breach, there is no harm done in accompanying that with a clear statement of regret. Being human and not providing a "canned" and mechanical-sounding response also helps manage the emotions for your users. You are human, too.
- Get pro-active by holding annual pre-breach session for cohorts of staff and students on data privacy emotions to discuss real life effects, from bullying to financial to loss of identity. Treating breaches like social affronts will go a long way to heightening all user's sense of security importance.
- Manage moles. Look into how SDSN can help remove risks on the inside of your networks. The best security helps manage threats before they can cause damage. ■

Underwriter for this Brief

Juniper Networks simplifies the complexities of networking with products, solutions and services in the cloud era to transform the way we connect, work and live. Through engineering and innovation, we remove the traditional constraints of networking to enable our customers and partners to deliver automated, scalable and secure networks that connect the world. Additional information can be found at *www.juniper.net*

JUNIPER NETWORKS

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1. 408.745.2100
Fax: +1.408.745.2100
www.juniper.net

the LEARNING COUNSEL
Research and Context on the Digital Education Experience

The Learning Counsel helps our subscribing 215,000+ education professionals in the K12 and Higher Ed sector gain research and context on the digital education experience. Our mission is to help districts and schools reach real transformation through strategies for digital content & curriculum. Through consulting services and research, to events, custom publishing and online editorial, the Learning Counsel provides dynamic and diverse opportunities for private and public-sector leaders to collaborate for positive change.

LeiLani Cauthen
CEO & Publisher
the Learning Counsel

Well versed in digital content and curriculum change, the adoption process, successful strategies, and helping schools understand what's available and what will work, LeiLani often writes on the changes and future of the education space. She is a media, research, marketing and sales professional with 26 years of experience in the high tech, government and education sectors.

Charles Sosnik
Editor-in-Chief
the Learning Counsel

Charles has more than 30 years' experience as a journalist and editor, with a diverse background in magazines, newspaper, television, radio and digital media. For the past ten years, he has been immersed in education, helping to bring context to the ongoing narrative of education.

the Learning Counsel
3636 Auburn Boulevard
Sacramento, CA 95821
888.611.7709
www.thelearningcounsel.com