STATEWIDE TERRORISM & INTELLIGENCE CENTER ILLINOIS

School Safety Newsletter

Volume 6, Issue 2 September 2018

When 12-Year-Olds Can Breach School IT Systems, Who's Responsible?

Doug Levin, EdSurge, September 15, 2018

https://www.edsurge.com/news/2018-09-15-when-12-year-olds-can-breach-school-it-systems-who-s-responsible

Like moths to a flame, curious and tech-savvy students have always pushed the limits of what educators deem 'acceptable use' of school technology. This is in no way a new phenomenon. We provide them with access to powerful, general-purpose computing devices, access to the internet, and time—and at younger and younger ages. They explore, tinker, make, express themselves, push back, pursue their interests, and act out.

What's different in recent years is that in doing the unexpected with school technology, students can affect not just their own education and that of their classmates, but the operations of entire school districts (and even far beyond). Schools and edtech vendors take (some) steps to secure their systems and limit student access to the more powerful administrative features of school technology devices and systems, but time and again and again students demonstrate their ability to circumvent these controls.

When students break school rules related to the acceptable use of school technology, they are subject to being disciplined. For some, it results in a slap on the wrist, coupled with a redirection of youthful energies (for instance, to computer science courses or to assisting the school IT department in providing training or technical support). Many an IT professional's career has been spurred by such actions.

For others, it results in expulsion from school and a federal criminal record. For those students who are caught (not all are), there appears to be little consistency across schools in how these disciplinary policies are applied.

Since schools don't report detailed statistics on suspensions and expulsions, data are not available about the prevalence of student computer-related disciplinary actions. Based on the evidence I've reviewed and experts I've spoken to, I think these incidents are commonplace. In fact, I think our default assumption probably should be that there are students in every middle and high school in the nation routinely probing their school IT systems and edtech apps for exploits.

Given the fact that minors (pre-teens even) seem to so regularly and—in some cases—so thoroughly bypass school digital security controls, one can't but be left questioning whether school leaders and edtech vendors really grasp the many and significant issues at hand. Adding insult to injury is the fact that there exist no universally accepted school IT security standards, weak enforcement mechanisms for 'reasonable security' practices of schools and vendors, and a systemic lack of attention to the issues of digital security even as state and national policymakers (and private philanthropy) push schools to "shift to digital."

Coupled with the pervasive and often automated collection of data on students, families, and school staff, school technology is uniquely powerful and sensitive. What was once stored in locked file cabinets in an administrator's office—if it was even feasible to collect at all—is now stored on a computer network designed to enable broad internal and external access.

With the choice to deploy digital records and communication systems should come responsibility for security and consequences for poor or negligent practices. And while some can be quick to excuse schools' actions as they

Protecting our future through information sharing

In This Issue

When 12-Year-Olds Can Breach School IT Systems, Who's Responsible? (Continued)

aspire to modernize (getting by on a shoestring budget, biased toward deploying free-of-cost technology, often with understaffed or underskilled IT departments), we would do well to remember that districts are also big business, overseen by elected and appointed representatives, and charged with managing annual budgets of tens or even hundreds of millions a year. Digital security is a leadership issue.

To wit: when 12 year-olds can breach the IT systems of organizations with $100 million-plus budgets, how should we assign blame? Penalties and disciplinary actions for students who violate acceptable use policies are established, but what of the consequences to school districts? At what point could district leadership be considered negligent? What obligation do schools have to be forthright with their communities about their digital security shortcomings? How might schools react differently to these incidents, in ways that are more proactive and even humane?

These are hard questions, no doubt, but given the frequency of 'students hacking their schools' incidents, I believe it is time we more forthrightly address this complicated issue.

The Case of 'Joseph Jones' and the Rochester Community (Michigan) Schools

The Rochester Community School District—with an annual operating budget of $160 million–employs more than 1,500 staff members at more than 20 'nationally recognized, award-winning' schools. External accounts of the district suggest many things going well. While technology upgrades have been a focus of the district (like in many other districts across the nation), the district is not high-tech relative to others across the country (e.g., while the district provides laptops to all teachers and makes computers on carts available to classrooms, the district does not support a 1:1 program).

In June of this year, I was alerted to a heretofore undisclosed "student hacking" incident in the district by a parent I will call Mrs. Jones. Her son, whom I will call Joseph Jones, was in the midst of computer-related disciplinary hearings and she was seeking information and help. (Note: I have changed the names of the individuals involved to protect their privacy). An internet search brought her to the K-12 Cybersecurity Resource Center and to me. I have spoken to her lawyer, and to her and her son on multiple occasions and at great length. This is a story they have approved and want to tell, even as it has not been completely resolved.

Three years ago, when Joseph Jones was 12 years old and a 7th grader in middle school he and another school friend stumbled upon a permissions issue on a computer in the school library intended for student use. A simple glance at the directory structure of this public computer revealed that it was logged into an account with access to several shared folders. Within those shared folders was the real surprise: in one was a file that listed all student usernames and passwords in an Excel document in clear text; in another, was an application that provided the ability to change usernames and passwords for any person–student or staff–in the district without restrictions.

> "This was so easy to find. It was like three clicks and you were in. That's how simple it was. Go to the file explorer, open up the…[shared drive], and click on the Excel document." - Joseph Jones

To make matters more concerning, the username and password for the account running on that public computer was written on a note taped to the side of the screen for all to access and use. (Joseph reports that this was a common practice in the schools he attended in the district.) He and his friend soon figured out that this account was accessible not only on the public computer in the school library, but at any computer within the district network, including over the internet via a remote access application provided by the district (MyRCS) for student, parent, and staff use.

> "I was unsure of what I needed to do upon discovery of the password list. I felt as though I'd be quickly dismissed by the media center staff since I was only 12…at the time. Additionally, I was afraid to mention this to anyone since I would likely be in immediate trouble. There was no one to ask and no clear procedures in place by the school for a discovery of this kind, so the easiest thing to do was to keep quiet about it." - Joseph Jones

This discovery was not an act of malicious or even sophisticated hacking, but the act of two curious boys with above-average technology skills. However, instead of coming forward at that point, the boys kept the secret (mostly) to themselves and—like moths to a flame—over the following three years gingerly explored the district's internal IT systems, always keeping a low profile but still expecting to get caught at some point by district IT security.

And, on May 18 of this year, get caught they did. When approached by school administrators, they came clean, including turning over their personal computing devices to law enforcement. Joseph was expelled, and he still faces the risk of criminal charges, which the district is actively pursuing.

The final straw for Joseph's exploits—and what likely indirectly led to his questioning by school administrators who were tipped off by another unnamed student—was the sharing of a technique to bypass the school's internet filters. One friend told another, and like wildfire soon too many students were visiting supposedly blocked websites for school staff to miss. While students across the country avail themselves of a variety of techniques to circumvent network filtering, Joseph's technique involved using the still-active but unmonitored account of a retired teacher who had not been employed by the district for several years. It turns out that teacher accounts are not subject to the same internet filtering as student accounts.

His other offenses in the district's eyes—once all the cards had been laid on the table—included:

Monthly Webinars!

First Wednesday of Every Month

at 10 am

(Except January, July, and August).

Next Webinars

Wednesday, October 3, 2018

Each webinar has a round table discussion at the end. Questions are always welcome!

To participate, you must be a vetted member. For more information please email schoolsafety@isp.state.il.us

- Not disclosing his original discovery of the permissions issue on the district servers;
- Being aware of and assisting his friend with the installation of Monero (cryptocurrency) mining software on a district server, but not disclosing this to district officials; and
- Disrupting a different friend's classroom, which was engaged in a teacher-led Kahoot! session. (That friend texted Joseph his class's game PIN which Joseph used to spawn a bot that flooded the game with fake users. Note: such bots are plentiful, found via simple online searches, and trivially easy to use.)

There have been no allegations of grade changing, online harassment, deleting or manipulating student or personnel files, denial-of-service attacks, or defacing school website properties. Joseph had no other record of disciplinary issues with his schools. Whether he and his friend were the only people to exploit the district's security practices is unknown, but one thing is clear: a truly malicious actor could have caused irreparable damage.

It Takes Two to Tango

That Joseph broke school policy and would be disciplined—even harshly—was never really in contention. Joseph admitted he knew that he'd likely end up suspended or expelled for his actions.

> "I was a ticking time bomb at that point. I knew that by the time I got to high school that if I got caught it was [not] going to end [well]. If I were to recommend anything to other students if there is something wrong with their network, they should tell somebody. I regret that I didn't." - Joseph Jones

At the same time, he was increasingly incredulous about the security practices of the district. His mother agrees:

> "Students and parents shouldn't just be upset with [Joseph] but upset with the school district about the lax security. Anyone within the district could come along and do this…[and] there is going to be somebody else. They should insist that the [district's] security gets tightened up, because their stuff is at risk—all of their kids' information, their health records, grades—all of it is at risk. It's not at risk because we have smart kids like [Joseph] that start out as curious, it is at risk because the security policies that are in place are outdated…and nobody is looking at them." - Mrs. Jones

The Jones family maintains that the district has been excessively adversarial in its dealing with Joseph. The district has aggressively pursued expulsion—they denied them the option of withdrawing Joseph from school—and he expects to face still-pending criminal charges.

The irony of the situation–from the Jones' perspective–is two-fold. First, based on their interactions with the district about this incident, the family lacks confidence in district leadership's understanding of the underlying security issues plaguing the district. Based on my understanding, these issues include:

- Misunderstood or misapplied administrative account permissions;
- Poor password generation, storage, and management practices, including not de-provisioning the accounts of former employees; and,
- Not maintaining visibility into internal network operations, including account access and capacity/usage logs over time.

As such, Joseph and his family believe it likely that any of the new software the district may have purchased in reaction to this incident is either targeted to other threats (unrelated to the existing vulnerabilities Joseph exploited) or should have already been in place as part of a baseline cybersecurity program for a responsible organization. They find district claims of costs related to rebooting school computer equipment to be evidence of the degree to which the district is reaching to substantiate their claims.

The second irony is that one of the reasons the district offered for Joseph's expulsion was to make an example of him to the wider school community. Yet, as of today, the only notice the district has made related to this incident was a cryptic suggestion posted on their website in early June that students have the ability to change their passwords.

This post will be news to the school community (and–upon its publication–the incident will be added to the K-12 Cyber Incident Map found at: https://k12cybersecure.com/map/).

The District Responds

Prior to this story's publication, I reached out to Rochester Community Schools for a response. In addition to giving them the opportunity to preview the article (as I had the Jones family), I also asked a handful of questions. A district spokesperson responded with the following information:

Is the district pursuing criminal charges against any of the suspended or expelled students? Why or why not?

"At Rochester Community Schools, we take the safety of our students and staff very seriously. Protecting our family is always our top priority. As such, we are prepared to prosecute to the fullest extent of the law anyone associated with dangerous and malicious activities, including those associated cybersecurity breaches."

When 12-Year-Olds Can Breach School IT Systems, Who's Responsible? (Continued)

Has the school community been informed of the incident(s)? If not, why not?

"The Rochester Community School District works with local law enforcement to investigate all threats, including those associated with cybersecurity. When there is an ongoing investigation, we cannot publicly share details that could have a negative impact on the investigation."

What steps has the district taken to shore up the security of IT systems (based on what was learned from the district's investigation of this incident)?

"The Rochester Community School District uses various tactics to mitigate cybersecurity risks. Building awareness, encouraging employees and students to strengthen their passwords and keep them secure, and having restrictive permission policies are important steps in the process. Other tactics remain confidential to the organization so as to keep our network and student and staff information safe."

Being an impartial outsider to this situation, I can't help but see this story as emblematic of the complexity surrounding the larger issue of "students hacking their schools." Indeed, it is among the tamer of the dozens of such incidents I have documented since 2016.

> "If they think I am the only kid who is going to do stuff like this, I don't think so. There are going to be kids coming who know as much—if not more—than me, and who knows if they have malicious intent." - Joseph Jones

Stories like this one will continue to occur in districts across the country if and until the issue of K-12 cybersecurity risk management commands more attention and resources from district leaders. Schools and their vendors must become more intentional in designing their systems for use by students who may not always behave in ways that are expected. And ultimately, school leaders and vendors should be held to account for not ensuring a minimum baseline of security controls. On its face, it seems hard to argue that any $100 million enterprise has in place adequate security controls when a couple of 12 year-olds can bypass them and trivially so.

When a student does cross the line, schools should consider long and hard whether the most appropriate response is to expel the student and criminalize that behavior, versus viewing it as a unique teaching moment and a chance to shore up internal security practices. (Many organizations, in fact, pay good money for penetration testing services and/or offer bug bounties as part of their security compliance programs). Given the emphasis on STEM careers and the importance of computer science for the broader economy, it would seem that we'd want to embrace and channel the energies of those who show an interest and facility in computer operations…even when it may be in unanticipated ways.

I don't think there are easy answers, but I am certain that this story is far from unique. My hope in sharing it is to kick start a movement to find a common sense middle ground that leads to better school cybersecurity practices, while at the same time celebrating–yes, celebrating!–student ingenuity with and interest in computers. It is my sincere hope that this isn't too much to ask.

E-cigarette Warnings To Arrive in High School Bathrooms Nationwide

CNN, September 18, 2018

https://www.cnn.com/2018/09/18/health/e-cigarette-fda-prevention-campaign/index.html

The US Food and Drug Administration will stage a massive education campaign aimed at the nearly 10.7 million teens at risk for e-cigarette use and potential addiction, the agency said September 16, 2018.

For the first time, the agency will take the message that vaping is dangerous into high school bathrooms and social media feeds of those at-risk youth to stop what the FDA calls an epidemic of e-cigarette use by minors.

The trend was flagged in a 2016 report from the US surgeon general, which cited a 900% increase in e-cigarette use by high school students between 2011 to 2015. More than 2 million middle and high school students used e-cigarettes in 2017, the FDA said.

"We're in possession of data that shows a disturbingly sharp rise in the number of teens using e-cigarettes in just the last year," FDA Commissioner Dr. Scott Gottlieb said. "In short, there's no good news."

While applauding the FDA's move, Linda Richter, director of policy research and analysis for the nonprofit Center on Addiction, said that if the agency had taken action when the trend was first identified, "we probably could have avoided the surge in the use of child-friendly, high-dose nicotine products that we're now seeing among kids as young as 12 years old."

"Today's teens were on the cusp of being the first generation to broadly reject cigarette smoking but instead have become hooked on nicotine due to a decade of lax oversight over e-cigarette products," she added.

The dangers of e-cigarettes

E-cigarettes work by heating a pure liquid called e-juice -- composed of flavorings, propylene glycol, glycerin and often nicotine -- until it vaporizes. Popular flavors like tutti frutti, cotton candy and sour gummy worms have attracted younger users to e-cigarettes, which now often look like USB devices that are easy to hide and use without detection.

Recent studies have shown that e-cigarettes are a direct gateway to traditional cigarettes and have a number of health issues beside the addictive

E-cigarette Warnings To Arrive in High School Bathrooms Nationwide (Continued)

properties of nicotine. A study in the journal Pediatrics, for example, found five cancer-causing toxins in the urine of 16-year-olds who inhaled e-cigarette vapor.

"No youth should ever use e-cigs," Surgeon General Dr. Jerome Adams said in a video during Tuesday's announcement. "We must make it crystal clear that e-cigarette use can expose them to dangerous chemicals that can cause lung damage when inhaled."

Bathrooms are a first for FDA

The new campaign is an extension of the The Real Cost Youth E-Cigarette Prevention Campaign, which the FDA says is a nearly $60 million effort funded by fees from the tobacco industry.

The campaign will launch on digital sites and social media platforms popular with young people, such as YouTube, Facebook and Spotify, with videos that show disturbing pictures of damaged lungs and zombie-like students with vaping products glued to their mouths.

In addition, the campaign will place posters in the bathrooms of at least 10,000 high schools across the country, the first time the FDA has placed ads in bathrooms.

"For the first time ever, we are bringing the campaign into high schools to the point of contact where they are doing the behavior," said Kathy Crosby, who directs the Office of Health Communication and Education at the FDA's Center for Tobacco Products.

In addition, she said, the ads will be on school education platforms such as where teens check their grades or sports scores.

"Flavored vape juice may not be as sweet as it sounds," one video says as the strawberries on the screen rot into dry fungus.

"Strangely enough, some students come in here to put crap into their bodies," one bathroom poster reads.

The need for this aggressive approach, Center for Tobacco Products Director Mitch Zeller said, is due to the fact that while young people may never consider smoking a cigarette, "about 80% of youth see no problem in the use of e-cigarettes."

More startling, Crosby added, is that use is growing because teens are encouraging their friends to use e-cigarettes, a behavior officials have not seen for years with tobacco products.

The campaign used focus-group testing with young people to maximize the impact of the ads, Zeller said. The testing found that highlighting specific health messages such as chemicals and dangers was more effective than a general message that vaping is bad.

To view the 30 second ad titled, “An Epidemic Is Spreading”, visit: https://youtu.be/zYuyS1Oq8gY

"Vaping can put dangerous chemicals, like diacetyl, into your lungs," one poster says.

"Vaping can deliver nicotine to your brain, reprogramming you to crave more and more," another reads.

"The stalls may have #1 and #2," another bathroom poster says, "but vapes may have #24, #28, and #82." The small print beneath explains, "Vapers can inhale toxic metals into their lungs -- like these from the periodic table: chromium, nickel, and lead."

Richter said it might be more effective "if the target audience included kids younger than 12, since many 12-year-olds already are vaping," adding that the message should also be presented by trusted teachers and other peer and adult role models.

Matthew Myers, president of the nonprofit Campaign for Tobacco-Free Kids, said, "I think the ad campaign is extraordinarily positive and courageous for the federal government, and it will make some difference. But the vaping industry has used a deadly marketing campaign combining kid-enticing flavors and marketing on social media that has also been very effective.

"Voluntary action by companies has never been a solution," he added, "and the FDA must prohibit their social media marketing and crack down on the use of flavors."

Gottlieb pledged Tuesday to do more, referencing warning letters sent last week to more than 1,300 retailers that illegally sold Juul and other e-cigarettes to minors.

At that time, the FDA also gave e-cigarette manufacturers 60 days to show how they'll keep the devices out of the hands of young people or face regulatory action.

"I am meeting with largest manufacturers myself, and I won't stop until this problem is solved," Gottlieb said. "It may be the most important thing I do in my time as commissioner."

U.S. Frats Opt for Stricter Booze Policy in Wake of Deaths

USA Today, September 4, 2018

https://www.usatoday.com/story/news/2018/09/04/u-s-fraternities-opt-stricter-alcohol-policy-wake-deaths/1196674002/

Hundreds of fraternity houses across the US will no longer allow frat members to serve hard liquor, according to a self-governing policy announced September 4, 2018, in the wake of growing outrage over alcohol-related hazing deaths.

The North-American Interfraternity Conference (NIC) policy effectively means that most of the nation's fraternities cannot dole out strong booze unless it is served by a licensed third-party vendor.

“At their core, fraternities are about brotherhood, personal development and providing a community of support," Judson Horras, CEO and president of the NIC, said in a statement. "Alcohol abuse and its serious consequences endanger this very purpose. This action shows fraternities' clear commitment and leadership to further their focus on the safety of members."

The NIC is an umbrella organization for fraternities. The group said the new policy was reached in a near-unanimous vote and must be adopted by more than 6,100 of its chapters by September 2019. Those chapters are located on 800 campuses throughout the country.

Chapters have autonomy to set their own policies and rules, but the NIC has oversight over some broader policies, such as how the fraternities must implement alcohol rules at parties.

Fraternities in several states have been under fire in the past year for horrific deaths related to heavy drinking during hazing rituals and frat-house parties in general. Among them was the February 2017 death at Penn State of 19-year-old sophomore engineering student Tim Piazza of Lebanon, New Jersey.

Piazza died of severe head and abdominal injuries after falling several times at the Beta Theta Pi house the night of a bid acceptance ceremony.

Security video recovered from the house showed the sophomore and other pledges being plied with alcohol, and authorities later estimated Piazza had consumed three to four times the state’s legal limit for alcohol.

Piazza's parents, Jim and Evelyn Piazza, have been vocal proponents for stricter laws against hazing. Jim Piazza said Tuesday night that the new alcohol policy is "a good start."

"It should make a meaningful difference," Jim Piazza said. "There are other reforms they need to put into place, and there's still work to do. But this is a beginning."

Jim Piazza said other possible changes that he and other families of hazing victims would like to see include serving only beer at frat parties and ID checkers at parties to ensure everyone attending is of legal drinking age.

He said NIC representatives have been working with his family and others and "they've been listening to us."

"Our aim is to make overall college life safer," Jim Piazza said.

The first of more than 20 defendants charged in connection with Tim Piazza's death was sentenced to house arrest last month. Ryan Burke, 21, of Scranton, Pennsylvania, was sentenced to three months house arrest in Lackawanna County, 27 months of probation, 100 hours of community service and fined $1,000.

In June, Burke pleaded guilty to hazing, four counts of unlawful acts relative to liquor, malt and brewed beverages and licenses, and one count of purchase, consumption, possession or transportation of liquor and malt or brewed beverages.

Burke was originally facing charges of involuntary manslaughter, aggravated assault, simple assault, reckless endangering another person.

The NIC said in a statement that its new alcohol policy will prohibit "the presence of alcohol products above 15% ABV in any chapter facility or at any chapter event, except when served by a licensed third-party vendor." Most beer and wine is below 15% ABV.

Mia Ray Langheim

School Intelligence

Officer