MEMORANDUM

To:	Suzanne Bogdan
From:	Lanette Suarez
Date:	February 5, 2018
Subject:	Cybersecurity and K-12 Schools

GENERAL INFORMATION

- https://www.edtechstrategies.com/k-12-cyber-incident-map/
    - Public Schools - Interactive map that lists all of the K-12 Cyber Incidents. Last updated 1/30/2018.
- https://www.edsurge.com/news/2017-12-18-k-12-cybersecurity-the-end-of-innocence
    - "There have been nearly 300 cyber incidents experienced by K-12 schools from coast to coast in the last two years alone." – 2016/2017
- https://www.mediapro.com/blog/infographic-state-of-privacy-security-awareness-education/
    - Polled 904 employees at educational institutions: found that more than two-thirds of respondents could potentially put the personally identifiable information (PII) of students, faculty, and other employees in danger with risky behaviors.
    - 68% of respondents were classified as "risks" or "novices," meaning their actions could lead to a potentially serious cyber incident or data breach.
    - 45 % say lack of personnel and lack of budget are the biggest barriers to defending against threats.
- http://www.kajeet.net/extracurricular/ransomware-growing-threat-in-k12
    - The top four highest risk areas for educators are:
        - (1) Identifying phishing attempts (93 percent)
        - (2) Malware warning signs (86 percent)
        - (3) Social media (86 percent)
        - (4) Cloud computing (85 percent)

- http://statescoop.com/cybersecurity-k-12-education-schools-face-increased-risk-cyber-attacks/

    - Schools have a wealth of data that they routinely collect on students and store on their servers, from attendance records to medical issues.

    - Horror Stories:

        - In 2013, about 15,000 students at Sachem School District in Long Island, New York, had personal data, including school ID numbers and the names of those receiving free or reduced lunches, posted to an online forum. Cops later arrested a 17-year-old high school student in the district who pleaded not guilty, according to Newsday.

        - In Jersey City, New Jersey, a charter school last June was able to obtain names, addresses, phone numbers, dates of birth and possibly Social Security numbers of students attending traditional public schools to mail them registration forms, according to the Jersey Journal.

        - And teachers' data, including Social Security numbers, was compromised during an attack at Prince George's County public schools in Maryland — affecting 10,000 of the district's nearly 24,000 employees, the Washington Post reported last November.

- https://www.edtechstrategies.com/blog/how-should-we-address-cybersecurity-threats-facing-k-12-schools/

    - Article discusses the types of threats out there for schools and a framework for addressing k-12 cybersecurity threats.

TIPS/WHAT SCHOOLS ARE DOING

- ***How schools outsmart the hackers***, https://www.districtadministration.com/article/how-schools-outsmart-hackers

    - Discusses the different types of threats and how schools are combatting them.

    - *Distributed Denial of Service attacks (DDoS)* –

        - Attack in which a hacker intentionally crashes a network. There have been numerous incients of students paying hackers to stage such aattcks on school networks to postpone tests.

        - Defend against DDoS by employing a backup internet service provider to keep networks running and instruction uninterrupted.

- *Phishing (zero-day exploits)* –

  - Represents nearly 70% of all cyberattacks. It involves fraudulent emails that fool users into disclosing passwords or other private information, providing unauthorized access to a network or unleashing malware.

  - Defend against Phishing by having smart users! Train students and staff to look out for fraudulent emails. Further, instruct them to create strong password—involving more than a six-digit mix of letters, numbers and symbols—and to regularly change passwords.

  - Some schools have even implemented a two-step authorization, like Duo Mobile, which makes a person confirm each time they enter their password that it's them by providing a code that is either sent to them through a text, email, or a call to their phone.

- *Internet of things (IoT)* –

  - Hackers use the network of internet-enabled devices such as thermostats or lighting controls—to break into computer networks. Many IoT devices don't have built-in defenses against cyberattacks and can be hacked if not properly protected.
  - A good practice is to reset factory-installed passwords, making devices more difficult to compromise.

- *Tips for Schools*

  - Create a clear procedure for a ransomware attack and have a written plan beforehand. A ransomware response plan should include isolating infected computers, alerting other users, securing backup systems and notifying law enforcement. Afterward, all user and network passwords should be changed.

  - Some schools have created an internal cybersecurity advisory team that meets monthly to discuss policy, new threats, and raise awareness.

  - Many schools are moving vital student data to a cloud-based platform. This increases security, is reliable, and is cost-effective. The cloud also supports multifactor authentication—a multistep login process that increases security. Also, updates in state or federal cybersecurity standards get applied automatically.

- **Readiness and Emergency Management for Schools, *Cybersecurity Considerations for K-12 Schools and School Districts,*** https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF.

    - Extensive article that discusses the types of threats and how to prepare for them – before an incident, during an incident, and after an incident.

- ***3 K-12 Ransomware Threats and Solutions*,** https://www.eschoolnews.com/2017/01/18/k12-ransomware-threats/

    - **3 Measures Schools Can Take to Stay Ahead of Ransomware**

        - ***1. Training and Awareness***

            - Most ransomware attacks begin with an email containing a malicious link or attachment. Consequently, the single most important measure you can take to reduce the likelihood of a successful attack is to train yourself, your students, families and your staff to practice safe computing and recognize red flags that indicate a potentially malicious email.

            - Don't open suspicious emails. Pretty much anything unexpected or out of the ordinary is a potential attack, even if it comes from a trusted source. If possible, contact known senders separately to confirm the email is authentic before opening.

            - Learn to spot red flags. Some telltale signs of an attack include:
                - Unexpected grammar or spelling errors in a supposedly professional email
                - Odd, middle-of-the-night time of sending
                - Typosquatting, in which the "From" domain looks legitimate at first glance, but is actually slightly misspelled or has things added—"hacker@bankofarnerica.com," for example
                - Buttons and links in the email that connect to unexpected, suspicious URLs. To check this, hover the cursor over the link or button, and the URL will appear at the bottom left of your window. Train students and staff to do this reflexively.

        - ***2. Secure Your Network***

            - Effective user training can help stop a lot of attacks, but keeping your network free of malware also requires a combination of effective perimeter filtering, strategically designed network architecture, and the capability to detect and eliminate resident malware that may already be inside your network.

- Prevent threats from entering the network with a next-generation firewall or email gateway solution to filter out the majority of threats. An effective solution should scan incoming traffic using signature matching, advanced heuristics, behavioral analysis, sandboxing, and the ability to correlate findings with real-time global threat intelligence.

- Control and segment network access to minimize the spread of threats that do get in. Ensure that students can only spread malware within their own, limited domain, while also segmenting. For example – allow administration, teachers, and guests, each with limited, specific access to online resources.

- Clean house. Your infrastructure likely contains a number of latent threats. Email inboxes are full of malicious attachments and links just waiting to be clicked on. Similarly, all applications—whether locally hosted or cloud-based—must be regularly scanned and patched for vulnerabilities.

- ***3. Backup—Your Last, Best Defense Against Ransomware***

  - When a ransomware attack succeeds, your critical files—HR, payroll, grades, health records, confidential student files, email records, etc.—are encrypted, and the only way to obtain the decryption key is to pay a ransom.

  - But if you've been diligent about using an effective backup system, you can simply refuse to pay and restore your files from your most recent backup—your attackers will have to find someone else to rob.

  - Automated, cloud-based backup services can provide the greatest security. Reputable vendors offer a variety of very simple and secure backup service options, priced for organizations of any size.

  - For budget or other reasons, your organization may be committed for the time being to a legacy, on-premises backup solution. If so, you should certainly be planning to transition to a cloud-based system. In the meantime, be sure to configure your system to update backup files throughout the day, and be extremely diligent about moving your current backups to a secure, off-site location every evening.

- ***Ransomwhere: A Growing Threat in K-12,*** http://www.kajeet.net/extracurricular/ransomware-growing-threat-in-k12

    - Schools are keeping students safe online by educating them on what to look for to ensure that they don't unwittingly click on a phising email or web link from a school issued device that could take down an entire school network.

    - ***Tips for students:***

        - Improve information fluency and help students better evaluate the content they find online. With the proliferation of fake news and advertising posing as real content, students can easily click on an unsafe link.
        - Teach students good digital citizenship so they know how to protect themselves online and avoid potential dangers. Check out our earlier blog post and learn four strategies for teaching digital citizenship.
        - Use an interactive game, like the Google Be Internet Awesome platform, to help teach students Internet safety and how to keep personal information secure online.
        - Add an extra layer of protection. Student devices go through the school's filtering when on campus, but educators need to safely extend the classroom for those devices that go home.

- ***8 Cyber Security Tips for K-12 Schools*** - https://www.pivotpointsecurity.com/blog/cyber-security-tips-public-schools/

    - **(1) Segregate student networks from admin networks.** For school systems, segregating the student LAN/WLAN from the administrative LAN/WLAN is essential. Further segregation of the district's back office from each of the schools is also important.

    - **(2) Segregate the Student Information System.** Additional segregation of the Student Information System (SIS) is also warranted if it is hosted onsite. If it is hosted by a third party, then due diligence is essential to ensure the district's security requirements are being met.

    - **(3) Update your patches**. Keeping patches current is always important in any environment. This implies using only supported software and operating systems. Unsupported systems are sitting ducks.

    - **(4) Implement a backup program.** A solid data backup program can save the day if you're hit with ransomware. Some districts are investing in redundant systems with offsite server backup, so that services can be restored more quickly.

    - **(5) Take all possible systems offline.** This is one of the most effective strategies for reducing the attack surface. Anything that doesn't absolutely have to

be connected to the Internet should not be connected to the Internet – this includes printers, cameras, TV's, etc.

- **(6) Provide security awareness training.** Security awareness training for staff and other end-users is also critical to help them spot phishing attempts so they are less likely to introduce malware or ransomware on the network.

- **(7) Routinely test your vulnerability.** Periodically perform an external vulnerability assessment to preemptively identify your vulnerabilities before the bad guys do.

- **(8) Document your incident response plan.** Every school system needs to have a cyber incident response plan in place. If people know what to do in the event of a breach, its impact can be minimized.

- ***Security Drill: 3 Threats to Watch For,*** https://www.skyward.com/discover/blog/skyward-blogs/skyward-executive-blog/june-2017/security-drill-3-threats-to-watch-for

  - ***Phishing tips***: An uptick in phishing attacks has led to the launch and success of tools like KnowBe4, which – among other services – offers a platform for tech leaders to do a little faux phishing of their own. District employees receive mock phishing emails, and when someone clicks on a link, they are directed to a page that explains the dangers of phishing (with optional training videos or in-house follow-up). CTOs now have the data they need to assess the percentage of users who are "phish-prone" and follow up accordingly.

  - ***Pro tip:*** One edtech leader we spoke to stressed the importance of positioning this as a critical security drill, rather than a "gotcha" opportunity. After using KnowBe4's tools, he saw open rates plummet from 40% to 13% to 11% after just three sends. As staff learned to identify the signs, it became a competition to see who could spot the phishing emails and avoid getting duped, which is both fun and beneficial for the district.

- **Ion Goran, *Cyber Security Risks in Public High Schools,*** https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1002&context=jj_etds

  - Many cyber security threats facing schools are from the very students they serve. High school students have overridden school firewalls to tamper with their grades.

  - Actions and Measures for Schools to take – E-Security Approach ("ESA"):

    - (1) Data risk management regime: School IT personnel should establish and maintain an ESA or systematic methods for usage, incident, response, and risk management. The ESA should include development and means to promote and "Adequate Usage Policy." Handbook for the school's information technology in a handy and easy to understand format.

- (2) Protected Configuration: Hardware and software must be installed and maintained within guidelines for protected configuration. Guidelines for protected configuration must include keeping an inventory of all IT software and hardware. Further, a process should be developed to ensure procedures and policies are being implemented correctly and assure that all modifications are sanctioned, recognized and applied properly. This process must include procedures for checking that timely systems updates are applied as needed; e.g., when various software versions (comprising plugins, web browsers and operating systems) are installed, when "security patches" turn out to be accessible or when software or hardware expires/ Software, operating systems and hardware must be provided configuration protection to avoid access to services which can be employed to breach security of network, either accidentally or maliciously. For example, mobile phones provided to staff by the school should be secured to provide comprehensive password and locking guidelines.

- (3) Security of Network: Use effective firewalls! Filtering of website traffic over the network is required for avoiding websites that may introduce malicious material, checking for malware and antivirus, establishing and monitoring suitable interior configurations of security of network. Also, wireless networks require frequent password changes for users and network admins.

- (4) Management of privileges of students and teachers: Monitoring what students and teachers may and may not do on the system is an essential part of ESA. System privileges of students and teachers should be set so every user can acquire the services he or she needs while minimizing the prospect for accidental or deliberate network misappropriation.

    - "Password Management Processes and Policies" for user devices and programs must require and confirm both that PINs are strong and robust (that is to say they are not simple to predict either physically or by means a dictionary outbreak).

- ***Cybersecurity and Social Media Present Growing Concerns for School Security***, https://www.securitymagazine.com/articles/87208-cybersecurity-and-social-media-present-growing-concerns-for-school-security.

    - Santa Ana School District's approach to cyber security. Including what systems it used and educating students on social media.

- **Council of the Great City Schools, *Cyber-Security in Today's K-12 Environment,*** https://www.cgcs.org/cms/lib/DC00001581/Centricity/Domain/4/CGCS%20Cyber-Security%20Report%20FINAL.pdf.

    - Comprehensive report that discusses establishing a Holistic Cyber-Security Strategy for K-12 schools and the different areas that should be addressed for cyber-security issues.

- ***Cyber Security in K-12you're your School District Prepared?,*** https://www.frontlineeducation.com/Blog/March_2017/School_District_Cyber_Security.

    - Discusses the current state of K-12 Cyber Landscape, the government's response, and how to build a school's defense/key success factors.

- ***Integrating Cybersecurity with Emergency Operations Plans (EOPs) for K-12 Education,*** https://rems.ed.gov/Docs/K12_Cyber_Webinar_Final11_13_2014.pdf.

    - The Department of Education's PDF presentation that has a step by step way of handling cyber security threats.

PRODUCTS SCHOOLS HAVE USED

- **Safe Online Surfing** - https://sos.fbi.gov/

    - Launched by the FBI in 2012.

    - This is a free website where students can learn about cyber safety through games, videos, and other interactive features. It teaches kids in third through eighth grades how to recognize and respond to online dangers such as identity thieves, online predators, and cyberbullying.

    - Schools can compete with each other on a national level. Schools with the highest scores will earn an FBI-SOS trophy.

- **Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center -** https://rems.ed.gov/

    - The REMS Technical Assistance Center's primary goal is to support schools and school districts in emergency management, including the development and implementation of comprehensive emergency and crisis response plans. The Center disseminates information about emergency management to help school districts learn more about developing, implementing, and evaluating crisis plans.

- **Fortinet** - http://investor.fortinet.com/releasedetail.cfm?releaseid=929155

- **Ransim** - is a ransomware simulator tool that helps IT staff determine how vulnerable their networks are to ransomware attacks.