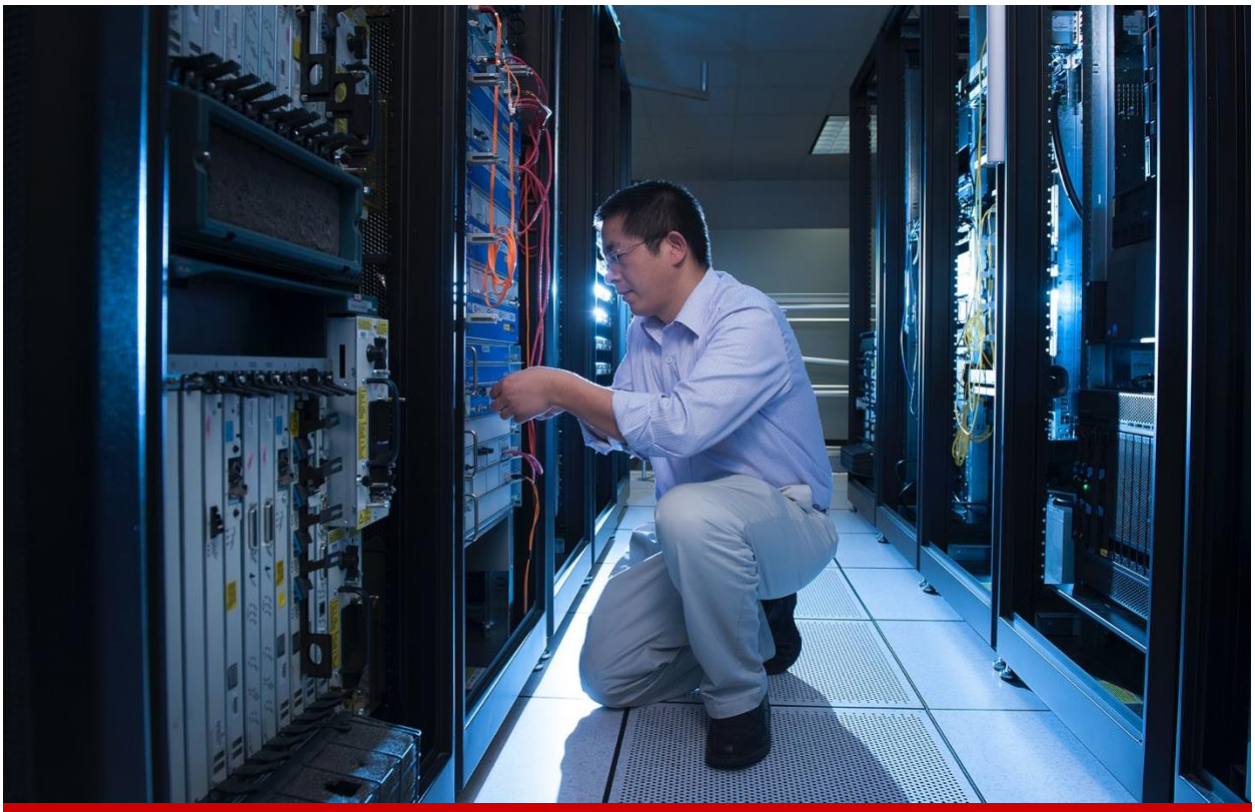

Cybersecurity in K-12

An Overview of the Threat Landscape

October 2020

Mark J. Samberg, Ed.D.

The William and Ida Friday Institute for Educational Innovation
North Carolina State University
Raleigh, NC

NC STATE UNIVERSITY
College of Education
Friday Institute for Educational Innovation

For years, many people have thought of K-12 schools as too small a target for ransomware attacks. In reality, schools host a treasure trove of personal and financial data that identity thieves and malicious actors would love to leverage in a cyberattack. In fact, hospitals, schools and governments are very popular new targets for ransomware. The K-12 Cybersecurity Incident Map lists over 1,000 cybersecurity incidents since 2016 in K-12 public schools—more than one incident each day. In addition to the data available to attackers on school computer systems, school networks are large, open networks that are difficult to secure. This is compounded by challenges schools face in recruiting and retaining network personnel with the experience to secure schools against the cybersecurity threats they face. Cybersecurity incidents are not necessarily large and destructive events. Many cybersecurity incidents often go unnoticed for extended periods of time before they are identified and resolved. Cybersecurity events can be everything from a data breach to a ransomware attack. Awareness, combined with policy and technical actions, can minimize the damage that an attack can cause, and many actions can completely prevent cyberattacks.

> **Cybersecurity Incident**: An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.
>
> *-National Institute of Standards and Technology*

Threat Actors

A person who is wholly or partially responsible for a cybersecurity incident is known as a *threat actor*. Threat actors are classified as internal or external actors. Threat actors may knowingly or unknowingly cause a cybersecurity incident. Sometimes these incidents are malicious and destructive, other times they are accidental and benign.

Internal Actors

Internal actors include your employees and students but also anyone who may have physical access to your network including service technicians, volunteers, contractors and often members of the public at large. Because these actors are internal to your organization, there is often some amount of trust and access granted to these individuals by virtue of their role (even if this is only physical access to the building).

A significant number of cybersecurity incidents caused by internal actors are a result of user error or poor training. Examples of this type of error would include:

- A user moving a file with personally identifiable information (PII) to a public server or sharing this information with users who do not and should not have access.
- A user being granted access to a system they should not have access to.
- A field trip form that asks for medically sensitive information with no data security process in place for requesting, securing, storing or sharing these data.
- Users sharing passwords or credentials with other users.
- "Technical Debt" – vulnerabilities created by insufficient funding and staffing to keep systems patched, updated and secured or cases where a technical fix is implemented with the intent to "fix it later".
- Lost or damaged devices resulting in data theft or loss.

However, internal actors can also cause malicious harm to your cybersecurity infrastructure. This may include malicious data theft or manipulation, password or credential theft, device theft or a malicious device placed on the network for the purpose of inflicting harm. Because there is often some amount of trust with internal actors, they are often provided physical access to places without question (i.e., someone dressed as a copier repair person could access parts of a school building unsupervised and place a device on the network). Additionally, because there is a certain amount of trust with internal actors, few organizations have dedicated efforts in place to detect or to mitigate threats from internal actors.

External Actors

External actors are those who are outside of your organization who are attempting to engineer a cybersecurity attack. These attacks generally fall into four categories: social engineering, theft, leveraging code vulnerabilities and malware. Oftentimes, an external actor will use multiple methods to launch their attack.

Social Engineering

Social engineering attacks are not technical in nature. They rely on an external actor convincing an internal actor to take a certain action. Many of these attacks are simple to deploy and rely on human nature to be trusting and accommodating. Consider, for example, the morning drop-off time. School is busy, students are entering and leaving the building constantly. An unknown person approaches the school and attempts to walk in the door. The person in front of them holds the door open as a courtesy, without asking for the typical identification that may occur another time during the day. That combination of circumstances is an example of social engineering.

A cyberattacker may rely on similar techniques, asking for bits of information by phone or email that by themselves are harmless but in combination could give an attacker the information they need to launch a cyberattack. Oftentimes, cyberattackers will send an

email disguised as someone else to create trust. For example, in one cyberattack, a school finance officer received an email that appeared to be from their auditor asking for a copy of all W-2 forms for all employees in the district. The attacker reviewed board meeting minutes to get the name of the auditor and company and then contacted the audit company to get that auditor's email address. They then sent an email to the auditor requesting information and were able to get their signature from the reply. Using all of these pieces of information, the attacker was able to craft a realistic-looking email to the finance officer requesting this information. Because the district did not have policies in place to vet these requests or proper data handling protocols in place, the finance officer sent this information unencrypted over email to the attacker and released data for all employees in the district. Attackers will also use social media and tools like LinkedIn to learn about their potential target and how to construct phishing schemes that are likely to be successful.

In another incident, an attacker created a fake login page to the university HR system. They subsequently sent an email to employees asking them to log in to validate their information. Once employees entered their username and password in the box, they received a fake "site is down" message while the attacker captured their username and password. They were able to use that information to log in to the self-service portal to the actual HR system and enter new direct deposit data, effectively redirecting paychecks for a significant number of employees.

Theft

Beyond social engineering, some cyberattacks result from outright theft—an external actor manages to steal credentials via social engineering or steal a physical device. Once they have hands on a physical device, they can access the hard drive and all unencrypted data on the drive (and if they have credentials, encrypted data as well). Even if they don't steal the device permanently, they can infect a device with malware hardware such as keyloggers or copy data from the device and return it without anyone ever noticing it was missing.

Leveraging Code Vulnerabilities

A code vulnerability is a coding error or oversight that enables a software package to be used in a way that is not intended. In some cases, attackers can leverage vulnerabilities to infiltrate a system or execute code to grant access to a system, disrupt it, or manipulate or steal the contents of a file. These intrusions may often go undetected until an actor decides to take malicious action, such as leaking stolen data, disrupting network services or deploying malware. Known vulnerabilities can be found on the Common Vulnerabilities and Exposures website or by using a tool such as Shodan or the Qualys Vulnerability Scanner. Software developers often release patches to mitigate vulnerabilities, though new vulnerabilities pop up as fast as developers can patch them.

Malware and Ransomware

Malware is short for "malicious software", software that is designed to cause disruption to a computer system and potentially cause damage, gain unauthorized access or steal data. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software and scareware. As of March 2020, Google detected around 600-800 malware-infected sites per week, and that number is increasing.

Malware can be deployed to a computer or network system in a variety of ways—by social engineering or encouraging a user to click a link or download a file, by leveraging vulnerabilities in a system or by being loaded by a malicious actor with physical access. Malware can also sit invisibly on a computer, doing things such as logging keystrokes and cursor movements, or it can cause damage by stealing data, deleting data or incapacitating systems.

A specific type of malware, called *ransomware*, has gained traction in the past few years. According to Lotem Finkelstein of Check Point Software, "hackers are swarming on ransomware because others have done it successfully." In fact, in the first quarter of 2020, 284 school districts and colleges had fallen victim to ransomware. Ransomware is a specific type of malware that encrypts the files on a drive such that they are unreadable and inaccessible without paying a ransom in the form of Bitcoin or another cryptocurrency to get the decryption key. New ransomware variants will also delete the data such that it becomes unrecoverable after a certain amount of time has passed or may exfiltrate (steal) the encrypted data. Ransomware will often spread across a network via a combination of stolen credentials and code vulnerabilities, encrypting shared storage but also critical systems such as financial databases, phone system files and other critical operational components. If backup drives are attached, ransomware can also spread and encrypt backups such that they cannot be used for recovery. Ransomware may also infect user workstations to encrypt local data or spread the ransomware off-site.

Ransomware attacks, especially if no recovery strategy is in place, can cripple a school district's IT infrastructure. Several school districts, hospitals and other local government agencies have been taken offline through ransomware attacks for extended periods of time because of ransomware. If data needs to be rebuilt from other records, the recovery time can take months or years.

Mitigation Factors

While schools are under consistent risk of cybersecurity incidents and cyberattacks, there are many policies, procedures and technical measures that schools can undertake in order to reduce the chances of being impacted by a cybersecurity incident.

Policies and Operational Procedures

- Monitor physical access to school buildings.
- Monitor and log access to networking equipment in each school building, keeping access to a minimum number of staff.
- Create data governance policies to identify what data elements can be collected and accessed by staff based on their role and where data can be stored.
- Require strong passwords for all staff and require staff to change passwords yearly.
- Enforce two-factor authentication (2FA) on systems with sensitive data. Two-factor authentication requires users to enter a one-time passcode or respond to a push notification on their phones in addition to entering a password. Two-factor authentication can be up to 90% effective at stopping targeted phishing attacks, and up to 100% effective at stopping bulk attacks.
- Remember the **principle of least privilege**. The principle of least privilege states that a user should not have any more access than they need to do their job. This way, if an employee account is compromised, they only have access to limited amounts of data, and no one set of credentials should have access to everything.
- Conduct routine and consistent training on phishing and data governance. Some school districts may simulate phishing attacks against users as a training exercise.
- Create policies for staff to validate emails that they're unsure about.
- Create a "Bring Your Own Device" or personal-device use policy that includes how staff can access resources like Google Drive and OneDrive from their personal devices including their phones.

Technical Measures

- Leverage managed services for critical infrastructure. Managed services are services in which the vendor who provides a software or service also hosts the service and ensures availability and security. This ensures that these systems remain available and recoverable if your network is breached, shifts the burden of patching and securing these systems to the vendor, and reduces your organization's attack surface.
- Not all systems can be hosted off-site or can be procured as a managed service. For systems that must be hosted on-site, leverage security trainings to develop staff capacity, leverage security expertise available from your Internet Service Provider, state/local governments and professional organizations, and consultants to ensure security in your network infrastructure.
- Ensure networks are segmented such that a device on the network cannot discover devices across the entire network. This will prevent malware from spreading.
- Use network tools to restrict unknown devices on the network and use tools to associate devices on the network with users.
- Encrypt data on staff computers using at-rest encryption such as FileVault and Bitlocker to prevent data breaches.

- Use privilege separation: users with administrative access should not use their administrative account for day-to-day usage. Create privileged accounts that are separate from primary accounts.
- Keep servers, network switches and all devices on the network patched and updated. Create a plan to keep infrastructure routinely patched.
- Create a backup strategy and ensure that one backup per week is kept disconnected so that it cannot be accessed by ransomware. Ideally, a weekly backup should be kept off-site to reduce exposure from cybersecurity incidents and natural disasters.
- Use a log monitoring service to log and monitor system access and configuration changes.
- Restrict open ports on your district's external firewall only to services that need to be publicly accessible. Do not open ports for third party services (use VPNs instead) or use insecure methods of data transferal (i.e., FTP, Remote Desktop).
- Conduct a quarterly firewall audit to review and reassess configurations and open ports.
- Use a VPN for off-site access to applications.
- Use antivirus and anti-malware systems on servers.

Responding to an Incident

The best way to respond to a cybersecurity incident is to avoid them. But in the event something does happen, quick response is the key. Ransomware can spread through a network in minutes. The first step in responding to a cybersecurity incident is to shut down any impacted systems or change any compromised accounts. From there, you should immediately refer the incident to district leadership and applicable law enforcement agencies based on local laws and procedures. Law enforcement and state departments of IT will assist you in determining if any data breaches have occurred and what steps need to be taken to restore access. You should also consult with your legal counsel about communication with communities.

About the Author

Mark Samberg, Ed.D., is the director of technology programs at the Friday Institute for Educational Innovation at NC State University and an assistant teaching professor in the NC State College of Education. In this role, he manages the Friday Institute's web services and conducts research and outreach in the areas of school infrastructure including technology infrastructure. Prior to joining the Friday Institute, Mark worked for over a decade managing K-12 programs in several North Carolina school districts.

About the Friday Institute for Educational Innovation

The Friday Institute for Educational Innovation brings together researchers, practitioners and policymakers to lead the transition to next-generation education systems that will prepare students for success in the digital-age world. We conduct research, develop educational resources, provide professional development programs for educators, advocate to improve teaching and learning, and help inform policymaking.

In our work we connect thought and action. We think creatively and act thoughtfully to improve educational outcomes for all learners. Much of our work results in tangible and impactful products, services, and applications. We educate in order to empower policy makers, educators and learners. We innovate to transform ideas into actions. We inspire and motivate others to promote systemic change.

The Technology Programs and Technology Infrastructure Lab teams at the Friday Institute bring over 100 years of combined experience in IT and network infrastructure including over four decades of combined experience in K-12 infrastructure. In partnership with the North Carolina Department of Public Instruction, the Friday Institute developed the North Carolina School Connectivity Initiative and the North Carolina Digital Learning Plan.

Suggested Citation

Samberg, M. J. (2020). *Cybersecurity in K-12: An Overview of the Threat Landscape*. Friday Institute for Educational Innovation. http://www.fi.ncsu.edu/