AERSTONE

Educational Cybersecurity

Protecting K-12 School Districts

Presented by Aerstone

2/11/2020

Table of Contents

UNIQUE PROBLEMS

Just as the K-12 public education sector enjoys a tremendous responsibility as a cornerstone of a healthy democracy, public education also faces a number of unique challenges that present a special set of cybersecurity concerns. With the rise of new technologies for teaching, learning, and administrative tasks in K-12 education, school districts have an increasingly arduous task of ensuring that adequate solutions are employed to address the unique cybersecurity concerns they face.

It's worth mentioning that there were more than 300 cybersecurity incidents reported by K-12 schools in the last two years alone; many more incidents were likely not reported. These breaches usually included the release of personally identifiable information (PII) students and teachers, which is not only a violation of the Family Educational Rights and Privacy Act of 1974 (FERPA), but can also damage educator and district reputations, and at the least will lead to a degradation in the quantity and quality of instructional time.

Aerstone has been working with educational institutions across the country for years, and has developed a unique understanding of the cybersecurity challenges facing K-12 school districts. Specifically, we have begun to see vulnerability and threat patterns emerge that ultimately represent risks on a number of different levels. In general, these risks represent potential failures to **confidentiality** (keeping private data private), **integrity** (keeping data from changing in unintended ways), or **availability** (keeping data and systems available). And whereas it is not a given that each of these parameters must always be maintained at any cost, it is critically important to understand how a loss of each of these factors in any given system might affect the district. Risks may then be mitigated, or accepted; they must not be ignored.

The remainder of this white paper is divided into two main sections:

- FIRST, we describe the core cybersecurity challenges we see across the K-12 public education sector. We've attempted to categorize these challenges into buckets that should immediately resonate with evaluators at all technical levels, and have specifically worked to avoid needlessly technical language. We also provide some specific vendor-agnostic recommendations within each area, to help mitigate risks we identify.

- SECOND, we provide a set of best practices for mitigating risks and enhancing cybersecurity posture across a school district enterprise in general. These best practices should be seen as a set of guiding principles, to help ensure the maintenance of proper cybersecurity posture across all service lanes and systems.

CORE CHALLENGES

Many of the challenges faced by the K-12 public education sector can certainly be found in other industries as well. And whilst no two snowflakes are exactly alike, we see remarkable similarities across different school districts. Size also doesn't appear to matter, although the risk level associated with some threats do increase as the size of a school district increases. These challenges, and the threats they pose – along with a few specific best practices – are delineated below.

INSIDER THREAT

School districts have an especially noteworthy risk: students, faculty and district employees. From the student's point of view, school networks represent an especially high-value target. This allure, combined with legendary lack of judgment, an enormous wealth of tools and "how-to" guides on the Internet for network cracking, and limited security budgets and auditing manpower, creates a perfect storm of risk for insider threat. To mitigate this risk, it is important to ensure that all locally-deployed equipment is properly secured, in locked cabinets. It is equally important to observe well-known security best practices, such as separation of duties and least privilege, strong password policies, and privileged account management policies. Access to non-common areas in both schools and administrative locations should be controlled via key card and PIN.

Schools should also work to apprise students of the consequences of network intrusion. Children have been known to hack networks purely for the challenge and thrill, without malicious intent, but sometimes with very expensive remediation consequences once systems are compromised. These thrill seekers should be actively dissuaded from taking these risks, and students who are nonetheless caught cracking school network security should face highly visible consequences, scaled to meet the severity of the intrusion.

IDENTITY MANAGEMENT

All school districts have an incredibly complex identity and access management (IdAM) problem. First, there is a wide array of constituents, including teachers, administrators, parents, and students – all of which may be thought of as organizational roles. There are also a variety of external persons of interest who may need anecdotal or occasional system access, such as vendors, board of education members, and law enforcement (to name a few). It's also important to note that the same flesh and blood person may serve multiple roles. Administrators may be parents. Teachers may also serve as administrators. Emancipated minors may act as their own parents. Any scholastic IdAM system must be designed to address this complexity in a secure and predictable way.

On the access side of IdAM, most school districts have a wide array of services and products to which access must be controlled. These services might be on-premises solutions, such as physical security systems, student information systems, school networks, and back-end office automation solutions. These services might also be cloud-hosted solutions of various kinds, including collaboration services, social media services, and scholastic tools. Access to these solutions needs to be supported from a variety of locations, including administrative locations, classroom locations, and student homes. And a variety of devices might be used to access these resources, including school laptop/desktop endpoints, student mobile devices, and home computing equipment.

The risks of a poorly designed IdAM environment include the possibility of granting improper access to applications or resources, as well as keeping legitimate users from accessing services or data. Given the high turnover in users from year to year, it is especially important that school districts develop well-thought-out IdAM policies, and deploy best-of-breed identity governance solutions. A single consolidated identity source should be considered authoritative for all identity management purposes, and wherever possible, applications should be integrated with a centrally-managed directory service to support single-sign-on. For applications that cannot be integrated in this manner, consider exploring other mechanisms for reduced sign-on, such as secure LDAP authentication or identity federation.

CONFIGURATION MANAGEMENT

Confirmation management poses a special challenge for school districts. First, for both performance and continuity of operations (COOP) purposes, school districts frequently position server equipment (especially for authentication, systems management, and core application access) in a distributed fashion, local to administrative and classroom locations. Second, the typical school year is filled with long periods of non-disruption, to support testing, grading, and other milestone-specific dates (such as the start or end of semesters and breaks). Third, there is a wide array of devices that must be supported, including fixed and mobile workstations, home computers, and mobile devices. This highly distributed ecosystem of devices significantly complicates the configuration management task, which in turn opens the school district's computing environment to higher than average risk, compared to organizations of similar size.

To mitigate this risk, school districts should seek to automate their configuration management mechanisms, alongside a formal change approval process. To mitigate the risk of compromised devices, network access control (NAC) may be used to quarantine any unpatched devices that attempt to connect to the network. Districts might also consider the use of technologies that streamline system patching requirements, such as virtual desktop infrastructure (VDI). With a VDI solution, only a single centralized system image is patched, and all workstations run copies of this central image on local thin client hardware.

DATA MANAGEMENT

School districts face a variety of risks with regard to data exposure. FERPA guidelines specifically protect the privacy of student education records; however, it is important for districts to have the chance to work through issues and policies prior to public release. All constituents, including students, teachers, administrators, and parents, may create or access data on a variety of devices. Data and files may be sent in motion in any of several different ways. And data and files can ultimately come to rest on any of a variety of systems, hosted on-premises, in the cloud, or privately.

In this regard, proper encryption for data both at rest and in motion is essential. Policies must be crafted around where data may be stored, both temporarily and permanently – and to ensure that student data is exposed only to authorized individuals. Districts might also consider multi-factor authentication for external access to student data. For protection of working papers, school districts should implement a classification management system for all internal documents and communications, as well as data loss prevention mechanism that blocks the transfer of information that either has not been classified, or which is inappropriate for a particular target enclave. Schools should also seek guidance on the legal data retention requirements for email, chat, and documents – then implementing a compliant data archival system across all relevant technology lanes.

SHADOW IT

Budgets are under tight pressure, scholastic results are under constant scrutiny, and expenses are rising across school districts. With this backdrop, it is unsurprising that free (and frequently unvetted) Internet-based services are being consumed by well-intentioned district practitioners. One axiom for online services, however, is that if you are not paying for the service, you *are* the service. Web service providers will not hesitate to sell student data, which may be a FERPA violation, and regardless may result in extremely bad press for the school system. There is also a concern that students will be targeted with inappropriate advertisements, and sexual predators may also target children on social media platforms that are shared with adults. And malicious websites may embed malware in the enterprise that result in significant financial loss. One example is the recent rise in ransomware attacks, which according to the FBI exceeded $1 billion in 2018 in the United States alone, with an average ransom demand of $116,000. In these attacks, a malicious software program gains a foothold in an enterprise that ultimately spreads to systems across the enterprise, encrypts system contents, and requires a payment as ransom for the file decryption key.

To help mitigate these risks, many school districts are already implementing processes that require educators to solicit "white list" pre-approval prior to using external web-based services. School districts might also consider implementing a cloud access security broker (CASB) solution, which has the ability to identify which web-based services are being used, to limit access to certain high-risk providers, and to control the ways in which data may be shared with approved services. Districts would further be advised to work to develop digital training for teachers, to ensure they follow school district policies and procedures with regard to external web-based services.

BEST PRACTICES

The way forward is in and of itself challenging. Cybersecurity is a process, and not a destination – and so cybersecurity posture must always be evaluated on a continuous basis, as technologies and threats and business models change. However, the ten recommendations below are largely threat-agnostic, and mainly represent best practices that any organization should follow to mitigate cybersecurity risk. The first five recommendations are the Center for Internet Security's "five tenets for effective cyberdefense," lightly tailored for the K-12 public education space. The second set of five best practices are specifically applicable to this space. All of these recommendations should resonate across the adult stakeholder community, including administrators, teachers, and parents.

TRAINING

Schools must invest in cybersecurity training for all constituents, including teachers, administrators, students, and parents. Educators must understand any risks they are taking with their own resources, and with student data. Parents must understand the risks of functioning in today's digital world, and collaborate with educators on setting prudent controls for students that are commensurate with age and maturity, and reasonable given the actual risks associated with cybersecurity threats.

PRIORITIZATION

Cybersecurity threats (i.e., the full set of all possible events) are not the same as cybersecurity risks (i.e., the subset of unmitigated threats that are likely to occur). Schools should work to prioritize remediation of cybersecurity risk based on a formal risk analysis, and tackle low-hanging fruit first. The Center for Internet Security (www.cissecurity.org) publishes an excellent list of twenty "Critical Security Controls" that organizations should prioritize above all others. This list of best practices is derived from that set of recommendations, tailored for the scholastic environment – however the full list is worth exploring.

METRICS

Without proper metrics, it's difficult to ascertain whether a cybersecurity program is effective. This is especially important from a budgetary point of view, where showing results to the administration, to the board of education, or to the parent community may make the difference between a fully funded program, and a half-hearted effort. Schools should gather metrics reported by security tools, such as viruses quarantined, invalid logons prevented, and systems patched. Schools should also note when highly public cyberthreats fail to affect the school's infrastructure, and when key events (like student testing) occur without interruption.

CONTINUOUS MONITORING

Amongst the most serious risks to any enterprise are system inventory and configuration, and vulnerability assessment and remediation. Implementing a policy of continuous monitoring for a subset of critical systems is vital for ensuring the maintenance of security posture across the network. Systems should be chosen for continuous monitoring based on the impact to the organization due to a loss of one aspect of security described at the beginning of this white paper: confidentiality, integrity, or availability.

AUTOMATION

Automating system defenses helps ensure system scalability and reliability. Automation also helps assure data hygiene, and helps protect against insider threat attacks. To the greatest extent practicable, security infrastructure should be configured to err on the side of automated standardization. For example, antivirus definition updates should be pushed to all systems automatically as they become available, and user accounts (with appropriate access rights) should be provisioned automatically based on a central identity management engine. This concept is sometimes described as "managing by exception," and works to ensure that any deviation from the norm is intentional and willful.

POLICY

The foundation of any working cybersecurity program is rooted in strong policy. The district administration must establish a set of rules and regulations that matches the organization's business rhythms, culture, and priorities. Any established policies must also be followed, with the backing of senior leadership. And systems must ultimately be implemented that follow policy guidance, with auditable configuration that can be tied back to policy decisions.

COMMUNICATE

Proper communication is also an essential element of a strong cybersecurity environment. This not only speaks to setting and enforcing policy, but also in communicating the status of plans of actions and milestones. It is understood that hardening and maintaining an organization's security posture is a process, and not a destination – and so there will always be open issues that the organization should be working to mitigate. The risks that accompany these issues should be communicated openly and clearly, to all adult stakeholders. This will limit the potential fallout from surprises, and also help ensure a robust cybersecurity budget.

ZERO TOLERANCE

As described in the Insider Threat section above, school districts are in a unique position with regard to its constituents. Some stakeholders (the board of education and parents) are actively monitoring for security infractions. Some stakeholders (teachers and administrators) are actively looking for ways to stretch funding dollars, and may be encouraged to "work around" policy for what they believe to be a good cause. Some stakeholders (cloud service providers) are just trying to make a buck, however they can. And some stakeholders (students) may actively work to defeat security controls for a variety of reasons. This delicate dynamic requires a zero tolerance policy for security infractions, with violators sanctioned to the greatest degree supported by policy and statute.

STANDARDS

While there is no specific policy for educational system security controls, enforced either by industry or government, there are a number of security standards that a school district might choose to help them achieve a strong cybersecurity posture. Some examples include:

- The Center for Internet Security controls, as mentioned above.
- NIST Special Publication 800-171, "Protecting Controlled Unclassified. Information in Nonfederal Information. Systems and Organizations."
- The ISO 27001 assessment standard for security techniques.
- The AICPA Service Organization Control SOC 2 or SOC 3 Assessments.

Regardless of which standard is chosen, the important part is that an organization give proper thought to the sensitivity of its systems, select an appropriate set of security controls, and work to ensure that the selected controls are implemented and maintained.

THIRD PARTY ASSESSMENTS

You're not in this alone! A third-party assessment can help jumpstart a new cybersecurity program, and also help validate the implementation of current or proposed systems and policy. Contact Aerstone for a free consultation, and advance the formal process of managing the security of your district's critical systems and data. Aerstone will work with your school district leadership to craft a cybersecurity program roadmap, and help as needed at any point along the way.

ABOUT AERSTONE

Aerstone (www.aerstone.com) is a service-disabled veteran-owned small business (SDVOSB) that provides subject matter expertise and software development services in the field of advanced cybersecurity. We are also a certified vulnerability assessor under the NSA's NSCAP CIRA program – one of just five companies in the world. Our commercial customers include medium and large organizations in the financial services, legal, utility, and education spaces, as well as a number of non-profit organizations. The company also provides exceptional support and cleared staff to a wide variety of federal organizations in the civilian, military, and intelligence community sectors.

ABOUT TRINITY EDUCATION GROUP

Material review of this whitepaper was kindly provided by Trinity Education Group (http://www.tegtech.io), a strategy and development company comprised of the most experienced experts in adult workforce learning, strategic competency development and learning analytics. Trinity Education Group helps educational agencies and school communities improve and support their educator workforce by providing learning solutions that build the efficacy, engagement and experience of an organization's human capital development.