What is Cybersecurity?

Understanding Digital Best Practices

The US Cybersecurity & Infrastructure Security Agency (CISA) defines cybersecurity as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." Implementing a robust cybersecurity plan is the best way to protect your educational community from cyber attackers, who often see schools as a treasure trove of personal and financial data ripe for the taking.

The COVID-19 crisis did not do schools any favors in this regard, as it forced a hasty transition to remote learning that lacked time for careful cybersecurity planning, introducing students, teachers, and parents, along with schools themselves, to new cyber risks overnight. A report from the K-12 Cybersecurity Resource Center reveals some of the resulting vulnerabilities. They report that K-12 schools experienced an 18% increase in cyberattacks in 2020 over 2019, and that 377 school districts across 40 states suffered a record-setting 408 publicly disclosed cybersecurity incidents, with phishing, data breaches, and ransomware being the most common attacks (Samberg, 2020). This change could be here to stay, as schools may remain a target for cybersecurity incidents and cyberattacks. Understanding common cybersecurity threats and how to address them is your first step in reducing the chance that your community will be impacted by a cybersecurity incident.

Top Cybersecurity Threats for Schools *(* indicates separate article available)*

Social Engineering*

Social engineering attacks like phishing use seemingly legitimate communications to entice users to reveal confidential information or click on links that install malicious software. In 2021, over 85% of cyberattacks started with a person unwittingly granting attackers access to a system (Verizon, 2021). Training staff to detect and report suspicious emails is the first and most important step to addressing social engineering attacks. Make sure you have a well-known process in place for reporting suspicious e-mails. When a staff member clicks on a malicious link, immediate action is necessary to quarantine malicious software before it spreads. Make sure your staff feels safe reporting such mistakes immediately to avoid delays resulting from embarrassment or avoidance. Configure firewalls and email systems to automatically block suspicious attachments. For additional information and guidance on how to avoid becoming phish bait, check out our article, Social Engineering and Cyber Attacks

Ransomware

Ransomware is a type of malicious software (malware) that collects and encrypts a targets data. In most cases, cyber attackers require a ransom to be paid in order to regain access to the data, but they sometimes further threaten to release sensitive data publicly unless a ransom is paid. In the case of schools specifically, ransomware attackers may broaden their campaign by including parents and students on emailed threats, informing them of the ransom being demanded from their school.

Ransomware can be crippling for a Member's IT infrastructure. The best response to regain access to data is to backup data on a server that is not accessible by the rest of the network and therefore not vulnerable to the ransomware encryption agent. Policies should be in place in advance to address ransomware should it occur.

Denial-of-Service (DoS)

A denial-of-service attack (DoS), also known as a distributed-denial-of-service, occurs when a server or network resource is deliberately flooded with too many requests to carry out. Schools tend to lack the security protections

used by corporations, and as such, many schools are not as vigilant about connectivity. When facing a DoS attack, access logging servers are sometimes switched off as a memory saving measure, allowing attackers to retrieve the confidential data without a trace. Because these attacks often rely on sheer volume rather than sophistication, students may be able to carry out an attack on their own schools, creating a difficult discipline situation.

Though DoS attacks cannot be prevented, it is possible to purchase cloud services that do traffic scanning and analysis to mitigate the attack. For instance, cloud mitigation could be focused on protecting the underlying internet connection or to protect the higher-level web servers. Members should focus resources on cloud services that meet your specific needs and monitor your network to detect threats early. Additionally, ensure you have specific procedures in place that include key information and contacts to help resolve a threat before data loss occurs.

Data Breaches

A data breach is a leak or theft of sensitive, protected, or confidential data from a secure to an insecure environment that are then copied, transmitted, viewed, stolen, or used in an unauthorized manner. For education, data breaches often occur with confidential information, such as students' records, that may be inappropriately viewed or used by an individual who should not have access to the information. Attackers often target schools because their systems hold a significant amount of sensitive and confidential data about students, teachers, staff and even parents. Data Loss Prevention (DLP) solutions can help detect and prevent data breaches, though these tend to be expensive. Members should:

- Train end users in what data they are responsible for protecting and how to handle data.
- Use encryption services for any data that needs to be sent via email.
- Train staff on security procedures and ensure everyone feels confident they won't be punished for protecting data.
- Establish processes for what to do if a data breach occurs.
- Consider insurance to cover the cost of mitigating the damage in the case a data breach should occur.
- Consider getting a 3d party to audit your security systems.

IoT Vulnerabilities

IoT (Internet of Things) devices include Member owned equipment such as security cameras and other devices that may be student or teacher owned such as watches or cloud-based voice service devices. These devices often lack security or are not updated on a regular cycle. Consider isolating devices on a separate VLAN (Virtual Local Area Network) where they can be watched and don't have access to the rest of the network. Always change the default password to IoT devices.

Outdated Software

When software and hardware are unpatched or outdated, they are much more vulnerable to attackers looking to obtain access to networks and systems. While patching and updating systems are the most straightforward attack prevention methods, schools frequently lack adequate funding and dedicated cybersecurity staff, making them more prone to leaving some vulnerabilities unpatched. Vulnerabilities occur when unpatched or outdated software has not been updated to include the latest software updates; thus, unauthorized users can gain access to networks and systems. Many operating systems offer automatic updates. If this option is available, you should enable it.

Weak Passwords

Most people base their passwords on personal information so they are easy to remember. However, that also makes it easier for an attacker to crack them. Once you've come up with a strong, memorable password it is tempting to reuse it—don't! Reusing a password, even a strong one, endangers your accounts just as much as using a weak password. Once attackers discover or mine passwords, they often attempt to use those same passwords on different sites, meaning you could suddenly have many accounts at risk!

The following password best-practices are all steps towards better password security:

303.722.2600
www.csdsip.org
: @CSDSIP

- Enable multi-factor authentication
- Use different passwords on different systems and accounts.
- Use the longest password or passphrase permissible by each password system.
- Develop mnemonics to remember complex passwords.
- Consider using a password manager program to keep track of your passwords.
- Do not use passwords that are based on personal information that can be easily accessed or guessed.
- Do not use words that can be found in the dictionary and do not use proper nouns.

Additional Best Practices and Resources

Cyber attacks are becoming more frequent and sophisticated, making cybersecurity an important area of focus for good risk management. Your approach to this threat should be robust and two-fold, both technical and procedural. The following best practices by the FBI, CISA & CSDSIP, are a great place to get started.

- Promote cybersecurity awareness and train staff students (end users) annually and/or throughout the school year.
- Ensure that policies and practices follow the Family Educational Rights and Privacy Act, the Children's Online Privacy Protection Act, and other privacy regulations.
- Incorporate cybersecurity policies into the school or district's Emergency Operations Plan.
- Review policies regarding the use of technology and distance learning and ensure policies address requirements for informational security. Ensure that the entire school community is aware of the policies.
- Ensure staff understands the process for having new tools, such as software, applications, browser extensions, plugins, add-ons, etc. approved.
- Back up sensitive data regularly on an external device that is not connected to the internet. If a ransomware attack occurs, the backup data will not be encrypted if it is separate from the network.
- Use virtual private networks (VPNs) to encrypt traffic if possible.
- Require multi-factor authentication – Check out The Importance of Multi-Factor Authentication
- Use email spam filters to prevent phishing emails from reaching end users.
- Ensure that content filtering works off campus. School issued Wi-Fi hot spots should have content filtering enabled.

Resources

https://www.cisa.gov/cybersecurity

http://dev.cosn.org/sites/default/files/Top%205%20Cybersecurity%20Threats.pdf

https://k12cybersecure.com/resources/

https://www.fi.ncsu.edu/resources/cybersecurity-in-k-12-an-overview-of-the-threat-landscape/

https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF

References

Samberg, M. J. (2020). *Cybersecurity in K-12: An Overview of the Threat Landscape.* Friday Institute for Educational Innovation. http://friday.institute/7721

Verizon. (2021). *2021 DBIR Master's Guide.* Verizon.

303.722.2600
www.csdsip.org
: @CSDSIP