K-12 CYBERSECURITY COST REPORT

FALL 2019

CoSN
LEADING EDUCATION INNOVATION

K12 CYBERSECURITY COST REPORT

Fall 2019

This report was made possible by the generosity of our partners, ENA and Juniper Networks.

1325 G St. NW, Suite 420 | Washington, DC 20005 | 202.861.2672
communications@cosn.org | cosn.org

CONTENTS

EXECUTIVE SUMMARY

CoSN's *2019 K-12 IT Leadership Survey Report*, released in April 2019, identified cybersecurity as the number one priority for school system technology administrators. Following up on this finding, CoSN conducted the *Cybersecurity Costing Survey* between May and June 2019 to identify cybersecurity challenges school systems are currently facing, and cybersecurity costs that might be good candidates for expanded E-Rate funding in the future.

Since the E-Rate program was created as part of the Telecommunications Act of 1996 it has helped ensure that eligible schools and libraries have affordable access to the Internet. The 2014 E-Rate modernization orders (July & December 2014) continued this commitment. However, network access and Internet connectivity are no longer enough. While E-Rate funds help level the playing field by defraying school system costs for Internet access and network infrastructure, the very nature of the Internet has changed since the program's inception. The Internet is now an essential communications and data transmission conduit for education, government, business, and personal activity. In addition, it is also host to a wide range of nefarious hackers, identity thieves, and criminal and nation-state sponsored organizations utilizing networks to steal data, disrupt network activities, and destroy data systems.

The risks to school systems are only increasing as the number of data breaches and cyberattacks increase every year. According to USA Today, billions of people were affected by data breaches and cyberattacks in 2018 – 765 million in the months of April, May and June alone.[1] In addition to data theft, ransomware attacks continue to pose a very real threat to school systems. This was recently demonstrated by the rash of ransomware attacks in Louisiana school systems in July 2019 which caused Louisiana Governor Edwards to declare a state of emergency. Louisiana's experience is not an isolated incident; in 2018 there were over 204 million ransomware attacks worldwide.[2]

The *Cybersecurity Costing Survey* was made available to CoSN member and non-member school systems across the United States. The survey was not an exhaustive review of all cybersecurity tools and defenses available in the industry or implemented in school systems as the vast array of tools and ever-changing defense options are so numerous. Instead the survey focused on twelve of the most common defenses and automation of those defenses.

Subsequent to completion of the survey, a subset of participants volunteered to participate in a more in-depth conversation about the cybersecurity funding challenges and opportunities they face. These interviews contributed additional context to the data collected in the survey and resulted in the identification of three consistent themes. Representatives from the survey sponsors, ENA and Juniper, were also interviewed and their observations and experiences were consistent with the themes identified by the survey and interviews with school IT personnel.

E-Rate, as currently structured, builds networks and provides Internet access but does not provide essential funding to protect and secure those networks. This leaves school systems with significant funding limitations at risk of being unable to fully protect the networks they manage and subsequently the students, teachers, and administrators they serve.

1 USA Today, 12.28.2018

2 Statistica.com, "Annual number of ransomware attacks worldwide from 2014-2018 (in millions), https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

KEY THEMES

THEME 1 ▶ Consistent deployment of basic cybersecurity tools in school systems is heavily influenced by the requirements and limitations of the E-Rate program.

School systems almost uniformly deploy basic firewall systems, web content filtering, spam filtering, and anti-virus/anti-malware endpoint security to manage security risks. The majority of their cybersecurity funding goes to basic ingress/egress filtering firewall systems which can be funded by E-Rate, and to web content filtering systems required by, but not funded by, the E-Rate program. While no data is available on how this requirement impacts E-Rate participation, this unfunded mandate may prevent some school systems from participating. In addition, the lack of funding support for cybersecurity tools may be increasing risk and exposure to participating districts who lack funding to invest in the rest of the infrastructure necessary to protect their networks.

THEME 2 ▶ School systems encounter significant funding limitations that prevent them from deploying more advanced cybersecurity tools to protect their networks, systems, and Internet access.

While school systems are consistently doing the basics in cybersecurity, funding constraints limit the deployment of more advanced cybersecurity tools that are becoming mainstays in other industries. This includes technologies such as intrusion detection/prevention (IDS/IPS), advanced threat protection (ATP), data loss prevention (DLP), distributed denial of services (DDoS) mitigation services, encrypted traffic inspection, comprehensive encryption of data at rest and on mobile devices, multi-factor authentication (MFA), and security information and event management (SIEM).

THEME 3 ▶ School systems face ongoing staffing challenges in implementing, managing and monitoring the cybersecurity of their networks and systems.

School systems consistently identified staffing as one of the top two challenges in their efforts to secure and protect their networks, systems and Internet access. Staffing challenges take several different forms including a lack of positions allocated to cybersecurity, the inability to find and hire staff with cybersecurity skills and training in a competitive marketplace, and the concentration of cybersecurity responsibilities on a single staff member who "wears multiple hats" and is not a dedicated cybersecurity resource. School IT leaders are concerned that where they do have cybersecurity tools implemented to monitor and notify of cybersecurity attacks, they do not have staff to consistently monitor and respond to the threats. They may also not have adequate training or resources to respond when a threat is identified.

OPPORTUNITIES AND RECOMMENDATIONS FOR THE E-RATE PROGRAM

While E-Rate should not be expected to cover all aspects of school cybersecurity, several simple changes to the E-Rate program would have a very profound impact on the ability of school systems to protect and defend their networks and systems from cyberattacks.

1. **Expanding the range of firewall services that can be reimbursed through E-Rate would significantly increase perimeter and data transit security for school system networks and Internet access.** This would include expanding the definition of covered firewall equipment and services in Category 2 beyond the current basic firewall functionality of ingress/egress traffic management to encompass advanced protections such as intrusion detection/prevention systems (IDS/IPS), advanced threat protection (ATP), anti-virus/anti-malware filtering, SSL encryption, encrypted traffic inspection, data loss prevention(DLP), and spam filtering. These are examples of additional functionality available on next generation firewalls that are not currently funded by E-Rate.

2. **Expanding E-Rate to cover advanced security services provided by a school system's Internet Service Provider, including DDoS mitigation and the same advanced firewall features recommended to be added under Category 1, would both enhance school system cybersecurity and remove the burden of finding staffing to support these systems.**

   Currently, E-Rate will discount basic ingress/egress firewalls provided by the Internet Service Provider, if that is part of the ISPs basic service package. However, this is limited to the most basic of firewall functionality. Expanding the definition of covered firewall services that an ISP could provide would allow school systems to contract with their ISP for advanced firewall features to protect their networks, and have the ISP be responsible for operating and managing these systems, reducing the burden on school systems to find positions and qualified staff to do this work in house. Many school systems use the same ISP provider, being able to purchase advanced firewall functionality through the ISP could be more cost-effective and leverage economies of scale driving down the price as more school systems purchase additional cybersecurity services.

   E-Rate does not currently offer discounts for distributed denial of service (DDoS) mitigation services that help school systems maintain connectivity and availability when faced with a DDoS attack. Where school systems have been able to find funding for DDoS mitigation provided by their ISP, this has been an effective method to mitigate the impact of DDoS attacks on teaching and learning and deter future attacks. Those districts have found the rates of attempted DDoS attacks decrease once attackers discover DDoS mitigation has rendered this attack vector ineffective.

3. **Clarifying or updating the definition of "basic firewall" to align with technology industry standards would enable school systems to align their cybersecurity defenses with recognized industry standards and provide improved protection of their networks.** E-Rate currently funds "basic firewall" services in both Category 1 and Category 2, and "basic" has been interpreted to be limited to ingress/egress traffic management. As noted earlier, this leaves school systems with inadequate firewall defenses.

   This definition of "basic firewall" no longer aligns with technology industry standards. A "standard" firewall across the technology industry is typically a next generation firewall (NGFW) or unified threat management (UTM) appliance or service that offers, but is not limited to, the following protections:

   - Advanced threat protection (ATP)
   - Anti-virus & anti-malware protection
   - Data loss prevention (DLP)
   - DDoS mitigation
   - Intrusion detection/protection (IDS/IPS)
   - SSL inspection
   - Virtual private network (VPN)
   - Web filtering

As new cybersecurity defense technologies become available, the definition of discounted firewall services should expand to encompass current protections.

4. **Making managed security services and/or security operations center (SOC) services for the purposes of monitoring and responding to cybersecurity attacks and incursions eligible for E-Rate funding would significantly improve the ability of school systems to monitor and defend their networks.** Managed security services and SOCs leverage economies of scale to monitor and respond to security incidents across multiple organizations' networks. The ability to fund participation in these services through E-Rate would expand school system access to cybersecurity tools and trained resources, removing staffing and technology funding challenges from the cybersecurity equation.

5. **Adding web content filtering to the list of discounted services would remove a significant financial burden from school systems.** The implementation of web content filtering is required for participation in the E-Rate program but is not a covered expense. The FCC's 2014 E-rate Modernization Order reiterates, citing to the 2001 Children's Internet Protection Act Order, the agency's position that the Children's Internet Protection Act prohibits the use of Universal Service Fund resources for filtering. We believe Congress's intent was for that prohibition to apply to other appropriated funding, and not E-rate funds, and we urge the FCC to work with Congress to address this issue. [3]

By expanding Category 1 and Category 2 to cover the cybersecurity tools and services identified above, the E-Rate program could help school systems better leverage their limited funds to securely harden their networks and reduce threats to educational services, business continuity, and confidential student and employee data.

The E-Rate program has the opportunity to significantly improve the cybersecurity stance of currently funded networks and Internet access. An E-Rate program that does not address the lack of adequate funding for school cybersecurity equipment, services and personnel is putting schools and their communities at risk.

The recommendations above do not include expansion of E-Rate funding to include user and end point protection technologies such as anti-virus/anti-malware endpoint protection, multi-factor authentication, mobile device management, and identity and access management. Those technologies are targeted toward end user devices and access, and as such, are less directly correlated to E-Rate's goal of providing network and Internet connectivity and access to schools. The recommended changes focus on providing responsible and secure network and Internet connectivity and access to schools.

3 1 See Federal-State Joint Board on Universal Service, Children's Internet Protection Act, CC Docket No. 96-45, Report and Order, 16 FCC Rcd 8182, 8204 at paras. 54-55 (2001) (2001 CIPA Order).

DETAILED SURVEY ANALYSIS

Overview

The CoSN Cybersecurity Costing survey addressed school system adoption, implementation, management and funding of the following cybersecurity tools and systems:

- Anti-virus/anti-malware endpoint security
- Data loss prevention (DLP)
- Encryption of data (in transit, at rest, on mobile devices)
- Encrypted traffic analysis (SSL decryption)
- Firewalls (traditional, next generation, cloud, software)
- Identity and access management (IAM)
- Intrusion detection/intrusion prevention systems (IDS/IPS)
- Mobile device management
- Security information and event management (SIEM)
- Spam filtering
- Web content filtering

The survey also included questions about automation of cybersecurity functions and responses.

CoSN made the survey available online between May and June 2019 and invited both CoSN members and non-members to participate. Sixty-five school systems completed the survey nationwide and twelve participated in follow-up interviews. While the survey response group was relatively small, the themes that emerged from the survey and follow-up interviews were very consistent. Survey participants represented a cross-section of school systems both in terms of size and type.

School system participation by size:

Number of Students/ School System Type	% of Respondents
< 1,000	12%
1,000 – 2,500 (small)	27.5%
2,501 – 9,999 (medium)	21.5%
10,000 – 49,999 (large)	12%
> 50,000 (mega)	6%
Declined to identify	21%

School system participation by developed environment:

School system location	% of Respondents
Rural	32%
Suburban	31%
Urban	15%
Declined to identify	22%

The results of the survey consistently demonstrated that school systems are striving to perform due diligence in protecting their networks and systems from cyberattacks and leveraging their limited budgets and staffing to the best of their ability in the face of increasing cyber threats. However, lack of funding is a major driver behind the gaps in school cybersecurity preparedness.

Areas of consistent cybersecurity system deployment and strengths in school systems

The CoSN survey identified that most school systems responding have basic cybersecurity systems in place. IT staff are consistently utilizing firewalls, spam filtering, web content filtering, anti-virus/anti-malware, and encryption-in-transit, and mobile device management deployments to manage basic security risks.

Firewalls

Firewall implementations are a good example of where school systems are hitting the basics. All survey respondents indicate that they are using firewall technologies to monitor and block network traffic. The majority of school systems (65%) report they are utilizing next-generation firewalls that conduct traditional packet inspection in addition to providing advanced capabilities such as enhanced traffic monitoring, encrypted traffic inspection, web filtering, and email filtering. A number of school systems (26%) report using a combination of traditional rules-based firewalls and next-generation firewalls. Only a few school systems (6%) report using only traditional rules-based firewalls, and an even smaller number (3%) have migrated to utilizing cloud hosted firewalls as a service.

Firewalls represent a significant line item expense for school systems. Districts with over 50,000 students report spending from $100,000 to more than $150,000 year on firewall hardware, maintenance and subscriptions. Small, medium and large districts report spending between $25,000 and $100,000 a year on their firewalls. Cost did not necessarily correlate to the size of the school district. Only the smallest districts were consistently spending less than $25,000 per year on their firewalls, likely due to lower network complexity and lower throughput requirements on those devices. Overall, firewalls represented a significant portion of school system cybersecurity costs.

During follow up interviews with school districts, it became apparent that K-12 IT leaders have several concerns with their firewalls. First, they don't consistently have enough staff time and expertise to monitor and respond to firewall issues. Second, although they may have traditional ingress/egress rules-based access management and some level of intrusion detection or intrusion prevention systems functioning on their firewalls, they may not fully utilize the equipment capabilities because the licensing costs for add-on services, such as data loss prevention and encrypted traffic monitoring, are beyond their budgets.

Web Content Filtering

Web content filtering, which restricts or controls the content an Internet user can access, is the second area where school systems are strong in implementation and costs are high. All survey participants report having web content filtering deployed to protect their networks and staff and students using those networks. However, costs for web content filtering range widely and can cost larger school systems in excess of $100,000 per year, with the largest systems reporting that they spend over $150,000 per year.

Web content filtering is consistently implemented because compliance with the Children's Internet Protection Act (CIPA) is required to participate in the E-Rate program. As described above, we urge the FCC to revisit its interpretation of CIPA's funding limitation provision and, if necessary, work with Congress to permit USF funding to be used for this purpose.

While IT leaders agree with the need to implement web content filtering, every participant in the follow-up interviews asked why web content filtering is required for participation in E-Rate but is not covered under E-Rate Category 2 equipment and services.

Spam Filtering

Spam filters are used to detect unsolicited, unwanted, and potentially dangerous email messages and prevent those messages from reaching the end user. School systems almost uniformly (98.5% of respondents) report having implemented spam filtering on their email systems.

A deeper look at spam filtering indicates that 68% of school systems are utilizing spam filtering provided by their cloud hosting email service. IT leaders who participated in post survey interviews indicated that spam filtering provided as part of their cloud email service frequently did not fully meet their needs, nor did it consistently protect their networks from the onslaught of phishing attacks being experienced across the country.

Anti-virus/Anti-malware Solutions

Anti-virus is also consistently implemented in the school systems participating in the survey. Anti-virus/anti-malware solutions encompass software programs program designed to prevent, detect and remove viruses and/or other malicious software from computer systems and over 95% of respondents indicated they have implemented anti-virus on school system-owned devices.

There are some nuances to school system implementation of anti-virus. According to respondents, implementation of anti-virus protection on end user devices, desktops, laptops, and tablets, is very consistent. However, the implementation of anti-virus protection did not consistently extend to protecting servers. Only 81% of survey respondents specifically reported implementing anti-virus protections on school system servers. Also, not all anti-virus/anti-malware software is equivalent in capability. Only 65% of respondents report using anti-virus/anti-malware protections that can be centrally managed and monitored. Additionally, only 65% of respondents report using anti-virus/anti-malware systems that provide automated response and remediation of the threat once identified.

Cost was cited in interviews as the major reason for this decision. More advanced anti-virus/anti-malware end point

protection tools that offer central management, automated response and remediation, and machine learning to adapt to the threat environment also are often expensive. Anti-virus/anti-malware tools represented one area in which school systems, regardless of size, were able to allocate the least amount of funding. 78% of respondents representing districts in all size categories indicated that they spend <$25,000 per year on anti-virus/anti-malware defenses.

In follow up interviews with school district technology leaders, anti-virus/anti-malware implementation was identified as an area where school systems sometimes choose to utilize vendor solutions included in the base licensing for end user systems in order to cut costs. However, there is a significant tradeoff: these solutions don't provide centralized tool management and oversight to identify, remediate, and resolve infections as they occur. This can leave school system networks vulnerable and without a central accounting of viruses and malware threats. School systems often compensate for this challenge by annually re-imaging endpoint devices during summer, so they start the academic year clean and infection free. While this process limits the amount of time an infected device can remain on the network, it does not provide the comprehensive protection of centralized anti-virus and anti-malware tools

Encryption-in-Transit

Encryption-in-transit, utilizing technologies such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS), protects communications as they travel across networks between systems. For example, communications between a web client and the school's Student Information System (SIS) are often protected by SSL.

School systems reported high rates of utilization of encryption of data in transit between systems. 86% of survey participants report that they use SSL and/or TLS encryption services to encrypt data in transit. However, many respondents report significant staffing and cost concerns with encryption. 78.5% reported that they lack the staffing to implement and/or manage encryption of their data in transit ongoing and 62% of respondents lack the funding to either implement or maintain encryption services for data in transit. Despite survey responses indicating that school systems are encrypting data in transit, there are strong indications from the follow up interview process that school systems cannot always afford to encrypt all data in transit. In these situations, they prioritize and focus on encrypting the most critical and sensitive data moving across their networks.

Mobile Device Management

Mobile device management (MDM) solutions allow for the centralized administration and management of mobile devices, such as smartphones, tablet computers and laptops, including being able to remotely lock or wipe the device if it is compromised, lost or stolen.

Many school systems deploy a large number of mobile devices to district staff and students. In many cases, 1:1 student device implementations have greatly increased the number of managed mobile devices on the network. Implementation of MDM solutions not only allow remote locking or wiping of lost devices, but also provide platforms from which to manage and distribute system and application patches critical for continued security of the devices.

Currently, 86% of survey participants have some form of MDM implementation. As with other security controls identified in the survey, school systems struggle with staffing (67%) and funding (75%) to adequately implement and/or maintain their MDM systems. Systems with large 1:1 deployments generally face higher MDM costs than those who are not supporting 1:1 environments. In the largest school systems of 50,000 or more students, MDM costs can easily exceed $150,000/year. Medium and large school systems anticipate spending between $25,000 and $100,000 per year for MDM management.

Utilization of a mobile device management tool serves a dual purpose of supporting cybersecurity objectives and directly supporting classroom activities through central management of the mobile devices in the classroom.

Non-Technical Cybersecurity Successes in School Systems: End User Training & Phishing Campaigns

While the CoSN Cybersecurity Costing Survey didn't expressly ask questions about end user cybersecurity and awareness training, almost every school system interviewed identified this as an important way to reduce cybersecurity risk. Phishing remains a common attack vector, and 32% of data breaches involve phishing attacks.[4] All the IT leaders interviewed have either implemented an active end-user phishing awareness training campaign, including simulated phishing attacks, or they plan on implementing this kind of program in the upcoming school year.

School systems interviewed identified staff training as one of their biggest cybersecurity challenges. Technology leaders struggle to find time and opportunities to provide school system employees with cybersecurity awareness training. Often, they must compete with a roster of other mandatory trainings during in-service days, or cybersecurity training may be relegated to optional status. Many are finding that online cybersecurity awareness training combined with simulated phishing attacks is a time and cost-effective method of improving a school system's cybersecurity posture. One school system that has been tracking the success this program has reduced employee response rates to simulated phishing attacks from 40% to 7% over the last three years. They note that 7% is consistent with the rate of staff turnover.

While the funding of end user training is not recommended as an addition to qualified expenses under E-Rate, school systems could make more funds available for cybersecurity awareness training if high cost technologies such as next generation firewalls, IDS/IPS, web content filtering, etc. and services such as managed security services and security operations center services were discounted as E-Rate Category 2 services.

4 Verizon 2019 Data Breach Investigations Report (https://enterprise.verizon.com/resources/reports/dbir/)

OPPORTUNITIES FOR IMPROVEMENT IN CYBERSECURITY TECHNOLOGY IMPLEMENTATION

School systems are behind in implementing modern security systems in use by other industries to manage cybersecurity risks due in large part to the cost of those implementations. With combined annual costs for firewalls and web content filtering running between $50,000 and $300,000, depending on the size of the school district, opportunities to implement additional technical controls have been limited.

CoSN has identified the following opportunities to expand E-Rate eligible services to offset the high-risk cybersecurity threats and high-cost of mitigating them.

- Opportunity 1: Enhance network monitoring and response capabilities to improve cybersecurity
- Opportunity 2: Enhance user access security and end point device security

These opportunities are described below.

Opportunity 1: Enhance network monitoring and response capabilities to improve cybersecurity

Districts could enhance protection of their networks and Internet access by leveraging additional network security tools in wide use in other industries including: intrusion detection/intrusion prevention systems (IDS/IPS), distributed denial of service (DDoS) mitigation, data loss prevention (DLP), encrypted traffic inspection, and security information and event management (SIEM). Expansion of E-Rate funding to cover cybersecurity technologies and services for protecting networks would make these technologies more accessible to districts.

DDoS Response and Mitigation

DDoS response and mitigation services are generally procured from, and provided by, the Internet Service Provider and are designed detect traffic that indicates a DDoS attack, and respond and manage the malicious traffic to prevent the attack from disabling the network. DDoS attacks impact school systems in disproportionally high numbers and account for over half of all cybersecurity incidents in education.[5]

In education, pain from frequent DDoS attacks interrupts learning, prevents VoIP communication (which can impact 911) and disrupts many of the operational systems that make schools safe, productive learning environments.

While the Cybersecurity Costing Survey did not specifically collect data on the implementation rates of DDoS mitigation, the post-survey interviews identified that DDoS attacks continue to be a significant issue for most of the school systems interviewed and they were struggling to find options to finance DDoS mitigation services from their ISP. The one district that had managed to implement DDoS mitigation services with their ISP reported that DDoS attacks dropped off significantly once attackers realized they were no longer successful.

Data Loss Prevention (DLP)

Data loss prevention (DLP) systems monitor outbound traffic including file transfers, email, etc. for potential data breaches and unauthorized data transmissions and prevents them by monitoring, detecting and blocking sensitive data. DLP systems can often be enabled as an add-on service on next generation firewalls.

Despite the obvious advantages of having DLP systems to monitor outbound traffic and examine traffic for protected data such as social security numbers or credit card information, only 49% of school systems surveyed have a DLP solution in place. 51.5% cite lack of staffing to implement and/or manage and 39% cite lack of funds to purchase and/or maintain as significant barriers to utilizing data loss prevention systems in their school systems.

5 Verizon 2019 Data Breach Investigations Report (https://enterprise.verizon.com/resources/reports/dbir/)

Encrypted Traffic Inspection

Encrypted traffic inspection functionality allows firewalls to inspect encrypted traffic entering or leaving the organization's network for possible threats to network performance, availability and/or security. Increasingly, web sites and Internet traffic is encrypted. While encrypting traffic between an organization's systems for security is good, allowing unchecked access to encrypted websites can leave an organization vulnerable to cyberattacks executed through encrypted web sites. Encrypted web traffic can transport malicious network traffic into the network because it bypasses traditional packet inspection on firewalls.

44.5% of survey respondents report they have implemented encrypted traffic inspection to examine traffic coming into the network. Of those who report they haven't implemented encrypted traffic inspection on their networks, 69% cite lack of funding, lack of staffing, or both as the reason.

Implementation and management of encrypted traffic inspection will increase in importance for defending networks from cybersecurity attacks as the volume of encrypted Internet traffic continues to grow.

IDS/IPS

Intrusion detection systems (IDS) monitor network activity to identify and provide alerts of anomalous behavior. Intrusion prevention systems (IPS) take this one step further; in addition to identifying anomalous behavior, they can be configured to block potentially dangerous activity as it occurs.

Both IDS and IPS systems are extremely useful security tools, but neither are widely deployed in school systems. While correctly configured IPS would improve response time to suspected network intrusions, only 72% of survey participants have implemented IDS or IPS (breakdown by type, IDS or IPS, is not available). School systems identify staffing support for management of IDS/IPS as an ongoing challenge. IT leaders interviewed would like to further leverage automation opportunities and the active response and blocking capabilities of IPS to protect their networks, but struggle to fund IPS equipment, licensing, and configuration expenses.

Security information and event management (SIEM) systems

Security information and event management (SIEM) systems offer a platform for managing security incidents by providing real-time analysis of logs and security alerts generated by applications and network hardware. SIEM services and capability can be implemented in a variety of ways, through software, a network appliance or managed services. A well implemented SIEM can provide a comprehensive view of the organization's cybersecurity, but requires a sizeable investment in both equipment and staffing to implement and monitor effectively. Only 28% of respondents report implementing a SIEM solution. 46% of respondents cite cost and 41% cite staffing as significant barriers to implementation.

Vendors interviewed for the Cybersecurity Costing Survey expressed concern that some school systems purchase and implement SIEM solutions without the requisite staffing and training to fully utilize and support these systems. The presence of an underutilized SIEM system can pose a potential legal liability for school systems because the presence of a system implies it will be used and monitored to identify, prevent and respond to cybersecurity threats. A cost-effective alternative to an in-house managed SIEM would be the leveraging of managed security services and/or the participation of school systems in public agency Security Operation Centers (SOC). SOCs are centralized organizations that oversee cybersecurity for multiple units or organizations. There is a growing movement toward states and universities developing SOCs to provide cybersecurity services, including monitoring and response, to public agencies and organizations including school systems. As these SOCs come online, there are growing opportunities for school systems to leverage the economies of scale available to a central SOC and utilize SIEM services through a security operations center.

Opportunity 2: Enhance user access security and end point device security

Data storage, data utilization and data access controls are additional areas where school systems can continue to enhance the protections of the data stored on their networks. Data encryption, multi factor authentication (MFA), and identity and access management (IAM) are all tools that can improve the cybersecurity stance of school systems. However, because most school system cybersecurity funds are concentrated on web content filtering and firewalls, funding can be a challenge.

Data Encryption

Data encryption is often considered the gold standard of data protection because it transforms data and makes it incomprehensible to anyone who lacks the key to decode

it. Most state and federal data protection legislation recognizes encrypted data that has been lost or stolen from a server or mobile device without the related key as protected and not subject to data breach notifications. Data breaches remain one of the top five cybersecurity threats for schools and data encryption is one of the best ways to protect data from exposure.

Encryption at rest is the encryption of data where it is stored, for example on servers, storage area networks (SAN), desktops and laptops. While school systems report diligently encrypting data in transit on the network, data is less likely to be encrypted at rest on school system servers. Only 35% of school systems responding to the survey report they have implemented encryption at rest for data stored on their network. 78% of respondents cited lack of staffing, lack of funds, or a combination of both for the lack of data encryption at rest.

Like encryption at rest, encryption of mobile devices remains low within school systems responding to the survey. While mobile devices can represent a significant threat to data security when utilized by administrative and teaching staff with access to student data and personally identifiable information, the majority of mobile devices in most school systems are student devices. Staff support and funding to encrypt mobile devices are also cited as a barrier by 51% of respondents.

An additional barrier to consistent implementation of data encryption is that the survey reveals 24.5% of respondents do not consider data encryption to be a priority. This does not mean data encryption is considered unimportant; rather, it is competing for limited funding and staffing resources.

Multi Factor Authentication

Multi factor authentication (MFA) is a security system that requires use of more than just a username and password to gain access to a system. Generally, MFA systems require that the user have something, often a security token, to verify identity before gaining access to the system. MFA implementations have proven successful at curtailing the exploitation of credentials stolen through phishing attacks and social engineering by requiring more than just a username and password to access critical systems housing sensitive data such as student information, financial records, social security numbers, bank accounts, etc.

MFA is not widely adopted in school systems at this time. Only 27.5% of respondents have implemented MFA in any capacity. As with other technical security controls, lack of staffing (40%) and lack of funding (30%) were identified as barriers to adoption. While extensive adoption of MFA in school systems may not be feasible in the near future, the interviews with technology leaders revealed that many utilize small scale implementations of MFA for key personnel such as business managers and technology staff. These targeted implementations reduce costs and protect the accounts of staff with the highest levels of protected data access including Personally Identifiable Information (PII) and financial data.

Identity and Access Management

Identity and access management (IAM) covers a broad category of solutions to manage end user identity and approved access to systems. These solutions can include features such as support for single sign on (SSO), support for role-based access management to data and systems, and automation of user onboarding and offboarding. Larger and more complex environments rely heavily on IAM solutions to efficiently manage user access to systems. In small organizations, the cost and complexity of an IAM solution can outweigh the benefits, and many small organizations opt to manage user's identity and access through a manual process.

Survey respondents were consistent with this pattern of IAM adoption based on school system size. While 100% of the largest school systems (>50,000 students) surveyed report utilizing an IAM solution, this number dropped to 66% in large school systems (10,000-49,999 students), 45-50% in small and medium school systems (1,000-2,500 and 2,501-9,999 students, respectively), and 37.5% in the smallest school systems (< 1,000 students).

While more medium and large school systems could benefit from utilizing an IAM solution to efficiently manage and streamline user access controls, survey participants again report this is an area where funding and staffing are a challenge.

CONCLUSION: AN OPPORTUNITY FOR THE E-RATE PROGRAM

An E-Rate program that does not address the lack of adequate funding for school cybersecurity equipment, services and personnel to protect networks is putting schools and their communities at risk.

The E-Rate program has an opportunity to enhance the cybersecurity stance of the networks and Internet access that the program currently funds by expanding the funded list of services and equipment to include web content filtering and modern network security monitoring and capability as identified in this document's executive summary. By making these changes to the E-Rate program, the FCC would remove the burden of the unfunded web content filtering mandate and allow school systems to modernize network security monitoring/response services and equipment. This would help mitigate the ongoing and rapidly increasing threats to educational services, business continuity, and confidential student and employee data.

CoSN respectfully requests security products and services that school systems need including: advanced threat protection (ATP), anti-virus/anti-malware filtering, data loss prevention(DLP), DDoS mitigation, intrusion detection/prevention systems (IDS/IPS), SSL encryption, encrypted traffic inspection, security information and event management (SIEM), spam filtering, and managed security services be made eligible, and that web content filtering be reviewed as an item eligible for Category 2 funding.

Today's education communities have become enticing targets for cybercriminals because of the vast amounts of private data they manage and, often, their underdeveloped cybersecurity postures. According to research, a minor's identity is 50 times more likely to be compromised than an adult's because of his or her "clear" identity and credit history.

The "it won't happen to us" mentality--pervasive in education, particularly in smaller, rural communities--is quickly becoming a dangerous and costly liability. It's critical for all school districts, regardless of size or geography, to acknowledge that they are targets and formulate a comprehensive defense and mitigation strategy.

That's why ENA has developed a holistic approach that goes beyond network protection to enhance overall security. Our robust portfolio of solutions includes cloud computing, backup, and storage; content filtering; DDoS mitigation; hosted firewall; unified threat management; security assessment services; and CatchOn, a data analytics tool that enables districts to identify applications that may be vulnerable to violations of student data privacy policies.

Beyond that, our connectivity, communication, cloud, security, and software services include built-in security features and tools designed to combat today's evolving and ever-growing cybersecurity threats and attacks. Additionally, our experienced and knowledgeable engineers are always proactively monitoring the network security landscape in order to build enterprise-grade solutions that meet our customers' specific needs.

To learn more about our comprehensive technology solutions, visit www.ena.com, or contact info@ena.com to schedule a time to speak with our security experts about your specific security challenges and objectives.

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

For organizations of all types, having secure networks requires extending visibility beyond traditional perimeter defense. With more devices and the transition to the cloud, they attract more threat vectors driving organizations to react and deploy different security solutions for each different security problem. But for many organizations, cybersecurity protection ends up being suboptimal due to a wide array of security tools that aren't well integrated, that add operational complexity to already strained or short staff cybersecurity teams, that lead to potential blind spots and vulnerabilities. Juniper Networks believes in a security approach that is end to end, integrated between vendors across all areas of the network, with visibility from top to bottom. With Juniper Connected Security, we extend security to all connection points across the network to safeguard users, application and infrastructure against advanced threats. We do so through a robust open framework that provides seamless integration with security and network solutions from Juniper, Juniper's technology alliance partners and other vendors.

To learn more about Juniper Connected Security, visit
http://www.juniper.net/juniper-connected-security .