SPELL JIF CYBER SECURITY

BLUE TEAM GLOBAL WHITE PAPER SUMMARY
SEPTEMBER 2017

The attached white paper is the result of member school districts of the School Pool for Excess Liability Limits Joint Insurance Fund (SPELL JIF) choosing to invest in a serious audit of two member school districts with the express purpose of identifying a cyber risk management road map for school districts. The intent is to help school districts reduce the chance they are impacted by a cyber event and be far better prepared to manage one, if it should occur. It is a guide for school districts who are developing a management perspective and methodology for identifying cyber risk across operational and instructional purpose.

For more information, contact Craig Wilkie
Deputy Executive Director: SPELL, ACCASBO, BCIP and GCSSD JIFs
6000 Sagemore Drive, Suite 6203 Marlton, NJ 08053-3900
P: 856.446.9128 E: craig_wilkie@ajg.com

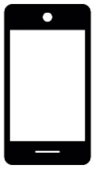
BLUETEAMGLOBAL

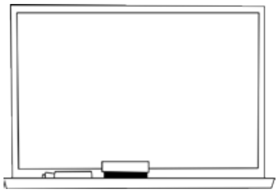
Cybersecurity for Primary and Secondary Schools

Threat Landscape

Since January 1, 2016, there have been over 200 separate cybersecurity-related incidents resulting in the disclosure of personal information, the loss of taxpayer dollars, and/or the loss of instructional time at K-12 public schools and districts.[1]

In 2016, 8% of all cyberattacks are targeted at the education sector.[2] Educational institutions are attractive environments for malicious actors because their networks are open by nature, accessible to staff, teachers, and students, often through multiple buildings and locations. IT dollars are directed at the education mission and often overlook security investment or rely on vendors to secure their products. Because students (and sometimes faculty) typically use their own computers, schools also often have loose device management policies that allows independent devices to access network resources.





What is at Risk?

At risk are student, faculty, and administrative information, the school's reputation, taxpayer money, and IT assets and services. Schools host a wide variety of non-public data, including personally identifiable information (PII), personal health information (PHI), financial data, personnel assessments, and testing data. Whether this information is stored locally or in the cloud, this information is at risk from attack by criminals and current or former students or employees.

These malicious actors can get to proprietary systems in a variety of ways, including theft or unauthorized access of physical devices, remote attacks on IT systems, attacks on vendor-managed systems, or the use of a witting or unwitting employee or student.

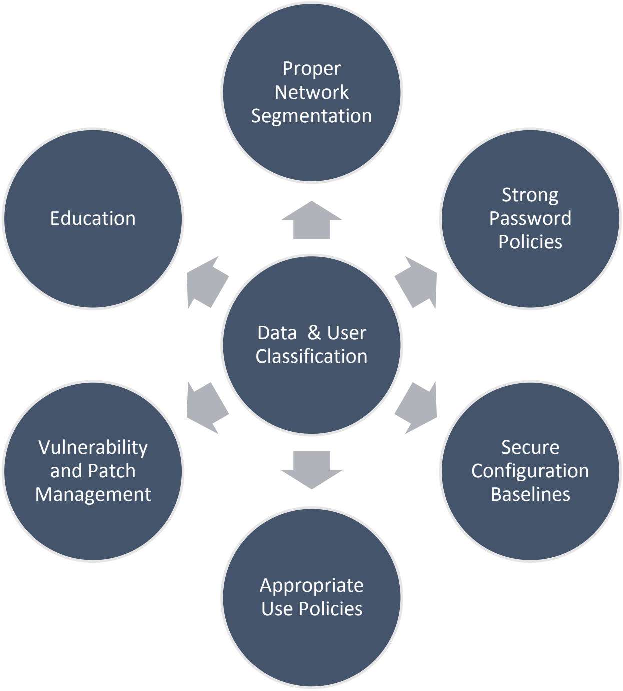
If such an attack should occur, the school might experience financial loss from the theft of information or financial/banking information, fines, costs from incident cleanup, or damage to other vendors that the school relies on.

[1] EdTechStrategies K-12 Cyber Incident Map, https://www.edtechstrategies.com/k-12-cyber-incident-map/
[2] Mandiant MTrends Report 2016, https://www2.fireeye.com/M-Trends-2016.html

How to Approach the Threat

To approach cybersecurity threats, an organization needs to know what they are protecting and who their users are. From there, the organization can take a risk-based approach to prioritize initiatives so that resources can be devoted to the proper areas based on carefully considered impact analysis.

Highlighted below are several key elements of a cybersecurity program that provide quick improvements in security and help to inform the rest of the security program as it develops. These foundational elements of a cybersecurity program are designed to address the greatest risks with the highest impact on improving security.


Proper Network Segmentation
Strong Password Policies
Secure Configuration Baselines
Appropriate Use Policies
Vulnerability and Patch Management
Education
Data & User Classification

The threats that pose the highest threat to K-12 schools are phishing, malware infection, and hacking, either by insiders or external malicious actors.

91% of all cyberattacks start with a phishing attack.[3] Any attempt to access, change, or exfiltrate information starts with gaining access to the network. One of the easiest ways to do so is via a phishing or Spearphishing campaign, where an attacker will target legitimate users. Sometimes the attacker will try to get users to provide credentials directly; other times, they will try to get the user to click on a link or access a webpage that downloads software to give the attacker access. Educating users on what a phishing attempt looks like is critical to preventing this kind of attack.

99.9% of exploited vulnerabilities compromised more than a year after the vulnerability became publicly known.[4] All software has vulnerabilities – as much as developers would like to create bug-free software, there are always weaknesses that aren’t found during the initial testing. As further testing is done and vulnerabilities reported, the system provider releases patches to improve usability and performance and plug security holes. Not keeping up to date with patching leaves a system wide open to all levels of attacker, not just the highly trained.

[3] PhishMe 2016 Enterprise Phishing Susceptibility and Resiliency Report, https://phishme.com/2016-enterprise-phishing-susceptibility-report

[4] Verizon 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

95% of all incidents involve harvesting credentials.[5] Attackers can harvest credentials using phishing campaigns, but they can also do so by gathering credentials saved on network devices. It is essential to have strong passwords and effective security baselines to ensure that passwords aren't kept in clear text and are complicated enough not to be easy to crack. When feasible, two-factor or multi-factor authentication can also be used to thwart attackers using stolen credentials. Attackers would have to provide a second authenticating factor in order to access the system.

Segmenting the network can help reduce the impact of a compromised system. A segmented network with established granular security zones can prevent an attacker from traversing a network and potentially accessing sensitive or critical resources. While an effective action, segmenting a network will involve a significant level of effort due to the complexity of ensuring network communications work as expected. With different security zones, network flow will have to be filtered between the zones increasing the complexity of the network design and management.

Secure configuration baselines ensure systems are hardened appropriately, making them less susceptible to compromise. Security configurations should be based on the specific technology being used and current industry best practices regarding devices of that type. Implementing such controls should have no budgetary affect since most if not all security baselines are available free of charge by organizations such as the Center for Internet Security[6]. The bulk of the effort would be determining the appropriate configuration for the systems operating environment. The baselines typically have very restrictive settings and care should be taken to ensure critical or essential services are not negatively affected.

Appropriate use policies help minimize risky user behaviors. Users are the weakest link in an organization's security chain. By clicking on a single link, a user can aid an attacker in by-passing all the expensive and hi-tech security controls an organization has implemented to protect itself. An appropriate or acceptable use policy identifies what behavior is appropriate when using company resources and assets. This helps minimize behavior that can lead to a compromised system and unauthorized access to the organization's network. Implementing such a policy should have minimal to no budgetary affect. The main cost typically associated with any legal fees that may be incurred for having the policy reviewed by counsel, which is recommended to help ensure proper language and maximum enforceability.

* * *

Securing your organization should be a risk-based, holistic, layered approach. Any implemented controls should take into account your organization's business goals and operating environment. For school districts, this represents unique and complex challenge. The open and collaborative environment which require minimal restrictions must be balanced with security controls that impose restrictions. The management of large numbers of loosely controlled mobile devices with increased external exposure to attackers, must be balanced with disruptions resulting from applying configuration changes and/or remediation actions necessary to secure them. Reviewing each challenge separately and applying a layered security approach the district will be able to properly secure its resources to an acceptable level of risk.

[5] Ibid.
[6] Center for Internet Security Benchmarks, https://www.cisecurity.org/cis-benchmarks/

Appendix A: Using the CIS Critical Controls for Assessing and Building an Effective Cyber Security Program for your School District.

The Center for Internet Security's (CIS) Critical Security Controls is a set of prioritized, well vetted security actions that an organization can take to help assess and improve their security posture. The controls, shown in Table 1, focus on prevention, detection, and corrective actions that help create a holistic and balanced approach to securing your organization.

The first 5 controls consist of what the CIS refers to as "Foundational Cyber Hygiene". These are actions that should be considered first when attempting to establish a strong foundational cyber security posture. In addition to listing the Critical Controls, figure 5, identifies the level of effort and potential budgetary impact of implementing the control.

Table 1: Critical Security Controls

	Critical Security Control (Industry Standards)	**Cost**	
		Level of Effort	Budget
CSC 1	Inventory of Authorized and Unauthorized Devices	Medium	Low
CSC 2	Inventory of Authorized and Unauthorized Software	Low	Low
CSC 3	Secure Configurations for software and hardware	Medium	Low
CSC 4	Continuous Vulnerability Assessments and Remediation	Medium	Medium
CSC 5	Controlled use of administrative privileges	Low	Low
CSC 6	Maintenance monitoring and analysis of audit logs	High	High
CSC 7	Email and Web browser Protections	High	High
CSC 8	Malware Defenses	Medium	Medium
CSC 9	Limitation and Control of Network Ports	Low	Low
CSC 10	Data Recovery Capability	High	High
CSC 11	Secure Configuration of Network Devices	Medium	Low
CSC 12	Boundary Defense	Medium	Medium
CSC 13	Data Protection	Medium	Medium
CSC 14	Controlled access based on need to know	Low	Low
CSC 15	Wireless Access Control	Medium	Medium
CSC 16	Account Monitoring and Control	Medium	Medium
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps	Medium	Medium
CSC 18	Application Software Security	Medium	High
CSC 19	Incident Response and Management	High	High
CSC 20	Penetration Tests and Red Team Exercises	Low	High

The first step in implementing the Critical Security Controls (CSC) should be to identify the school district's critical assets and resources and the risks associated with them. These actions are beyond the scope of this paper. We will assume that this process has already been completed by the district and will instead concentrate on mitigating common relevant threats to school districts.

According to current trends and reporting the most common threats facing the Education industry, in particular K-12, are Spearphishing, ransomware, malware (other than ransomware), loss or theft of equipment, and disgruntled student or staff. Table 2 shows a list these threats along with the actions that can help mitigate them. Also shown in the table, is the cost of the action in terms of level of effort and budget. The level of effort is a measure of the complexity and time resources that may be expended in implementing and maintaining the specified control. The budget cost is a measure of the potential financial cost of implementing the control. Finally, the figure provides a mapping to the relevant critical control.

A school district can use the table to identify and prioritize the appropriate controls for their unique operating environments. The controls highlighted in the last column identify if a control is a foundational cyber hygiene control. Notice, that with the exceptions of Spearphishing, implementing the foundational cyber hygiene controls assists in mitigating all of the identified threats to some degree.

Table 2: K-12 threats and mitigations

Threats	**Mitigations**	**Cost**		**CSC Control Mapping**
		Level of Effort	Budget	
Spearphishing	Awareness Training	Medium	Medium	CSC12
	Email Filtering/Monitoring	High	High	CSC7
	Web Filtering/Monitoring	High	High	CSC7
Ransomware	Endpoint Protection	Medium	Medium	CSC8
	Web Filtering/Monitoring	High	High	CSC7
	Email Filtering/Monitoring	High	High	CSC7
	Software Baseline	Low	Low	CSC2
	Security Configuration Baseline	Medium	Low	CSC3/CSC11
	Patching	Medium	Medium	CSC4/CSC18
Malware	Endpoint Protection	Medium	Medium	CSC8
	Web Filtering/Monitoring	High	High	CSC7
	Email Filtering/Monitoring	High	High	CSC7
	Software Baseline	Low	Low	CSC2
	Security Configuration Baseline	Medium	Low	CSC3/CSC11
	Patching	Medium	Medium	CSC4/CSC18
Theft/Loss of Equipment	Full Disk Encryption	Medium	Medium	CSC3
	Remote Wiping	Medium	High	CSC3
	Geo-fencing/location	Medium	Medium	CSC3
Insider (disgruntled student or employee)	Monitoring User Activity	High	High	CSC16
	Password policy	Low	Low	CSC3/CSC11
	Account management	Medium	Low	CSC5/
	Privilege access management	Medium	Low	CSC5/CSC15