STS® EDUCATION

PROTECTING YOUR SYSTEMS AND STUDENT DATA

K-12 Cybersecurity Solutions and Managed Services from STS EDUCATION

Whether you are looking for help assessing your technical, personnel, or policy systems for potential risks OR a partner to assist your district in identifying, preventing, detecting, responding to, or recovering from cyber threats, STS EDUCATION is here to help.

K-12 SCHOOLS FACE UNIQUE CYBERSECURITY CHALLENGES

Cyberattacks are a growing risk that can kill your productivity, hurt your reputation, and cost you money. But, for many school leaders, getting a handle on this ever-changing landscape is difficult and often very expensive.

While appointing someone to oversee cybersecurity for your school(s) makes sense, keeping students, staff, and families safe from potential threats extends beyond technology staff and solutions. Although the IT department is an essential ally, effective and sustainable risk mitigation would benefit greatly from:

1. A cybersecurity risk assessment framework developed specifically for schools by school technologists and experts from the fields of cybersecurity, law, and insurance to identify areas of highest risk
2. A cross-functional cybersecurity team—including the board, school leadership, legal and insurance representatives, privileged data users, and technology staff—to periodically review what additional work is needed to protect your school(s)
3. A holistic approach to K-12 cyber and data security risk management that spans personnel, policies and procedures, and technology

A recent report from the nonprofit K12 Security Information Exchange found that in 2020 [cybersecurity] incidents increased 18 percent over the previous year to reach a record high, equating to more than two cybersecurity incidents per day.

(Source: eSchool News, April 2021)

DEVELOPING YOUR CYBERSECURITY RISK MANAGEMENT ROADMAP

K-12 Cybersecurity Assessment

STS EDUCATION understands the complexities of managing cybersecurity risk in K-12 school environments. Accordingly, we utilize a risk assessment framework based on ATLIS cybersecurity recommendations when working with our school and district partners to assess, prevent, or mitigate cybersecurity risk.

Our assessment, delivered by school CTOs AND created by school technologists and experts from the fields of cybersecurity, law, and insurance, helps cybersecurity teams identify the highest risk areas and the actions they can take to get the best risk mitigation.

AT-A-GLANCE

Save Time

Our cybersecurity assessment, which typically takes less than four hours to complete, will point out areas of highest risk that are most easily attainable. Focus your energy on steps you can immediately take through internal changes.

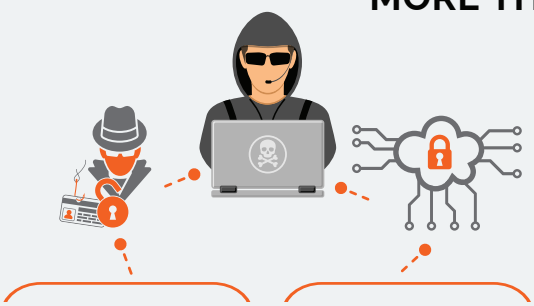
Save Money

A cybersecurity audit can easily cost more than $20,000. Leverage our low-cost assessment first to identify what you can do yourself and to inform future purchases.

Lower Risk

Our assessment identifies strategies based on ease of implementation and risk mitigation impact. Learn the steps that your cybersecurity team can take to achieve the greatest results quickly.

YOUR STUDENT RECORDS MAY BE WORTH MORE THAN YOU THINK



SOCIAL SECURITY NUMBERS

$10

ESTIMATED VALUE OF A SOCIAL SECURITY NUMBER ON THE BLACK MARKET

STUDENT DATA RECORDS

$250 AND $350

USDOE-ESTIMATED VALUE OF STUDENT RECORD ON THE BLACK MARKET

Hackers look at K-12 schools and districts and see easy access to data they can sell. Small districts with limited IT staff and technology resources are typically the easiest targets.

(Source: Education Week, March 20, 2019)

DEVELOPING YOUR CYBERSECURITY RISK MANAGEMENT ROADMAP

Comprehensive K-12 Cybersecurity Assessment

> *"A thorough audit conducted by an independent party can help schools learn new ways to address the constantly changing cyber threat landscape as well as identify serious concerns that schools can miss in their own review processes."*
>
> *- ATLIS Cybersecurity Recommendations (October 2020)*

HOW IT WORKS

Rapid Orientation

First, our experts guide you through assembling an action-oriented cybersecurity team of administrators, technology leaders, and privileged data users. We'll meet with your team to review the assessment steps and the purpose of the information being gathered-decreasing the time needed to complete the assessment and increasing the fidelity of the data submitted for analysis.

Cybersecurity Assessment

Then, your team works together to evaluate your personnel, policy, and technical systems for potential risk. Once the assessment is complete, our experts review and score your responses against our rubric in terms of both risk mitigation impact and relative ease of remediation

Personalized Cybersecurity Risk Management Roadmap

Next, our experts build your personalized cybersecurity action plan and create a performance dashboard for your school or district. Finally, we meet with your cybersecurity team to share key findings and begin the process of putting your school or district plan into action.

BENEFITS

Our quick, low-cost risk assessment process offers K-12 school leaders and cybersecurity teams:

- High impact, low-cost approach to developing your cybersecurity roadmap
- Shared understanding and stronger buy-in among district and school leadership regarding cybersecurity risk management
- Documentation of personnel, policy, and technology practices relative to cybersecurity best practices
- Summary of the most significant areas of cybersecurity risk
- Personalized, actionable recommendations for reducing cybersecurity risk across personnel, policy, and technical systems
- Performance dashboard for reviewing and documenting progress

"The final report delivery got school leadership on the same page with priorities and specific areas that needed focus. We've made more progress in the past month as a team than tech alone has made in a year and a half. It's incredibly cost-effective for small schools and delivers an understandable dashboard with actionable work plans to resolve deficient areas." — Brian Horton, Duke School (NC)

DEVELOPING YOUR CYBERSECURITY RISK MANAGEMENT ROADMAP

Other Cybersecurity Risk Assessments

> *"A thorough audit will likely include a penetration test to determine any unaddressed safety issues overlooked by the cyber safety and technology teams."*
>
> *- ATLIS Cybersecurity Recommendations (October 2020)*

WEB APPLICATION VULNERABILITY ASSESSMENT

This comprehensive test evaluates your web application source code against known exploitable vulnerabilities (e.g., a simulated hack of your website).

CYBERSECURITY / CRITICAL SECURITY CONTROLS ASSESSMENT

This assessment includes a questionnaire to identify the current state of the district's environment across critical security access controls. Additionally, we align district-specific results and recommendations to the Center for Internet Security's (CIS) best practices for the Top 20 Critical Security Controls.

FIREWALL RULES EVALUATION

Our certified security auditors review current firewall rules on Cisco, Meraki, Extreme Networks, Fortinet, Palo Alto Networks, Juniper Networks, WatchGuard, and Dell SonicWALL firewalls using various automated and manual tests.

INTERNAL & EXTERNAL VULNERABILITY ASSESSMENT

Service includes scanning for all known vulnerabilities, remediation recommendations of identified vulnerabilities, and a final report. There is **no attempt** to exploit or gain access to identified vulnerabilities. Vulnerability Scanning is recommended quarterly between PEN tests to identify any new vulnerabilities discovered after the Penetration Test.

EXTERNAL NETWORK PENETRATION TEST

An External Network PEN Test is a simulated hack of a client's external network, which K-12 districts should – at a minimum - perform annually. However, some compliance requirements may require testing more often.

INTERNAL NETWORK PENETRATION TEST

An Internal Network PEN Test* is a simulated attack to test the internal network for vulnerabilities of onsite guests. Additionally, districts perform an "Authenticated Test" to validate that employee access to critical systems is accurate and secure based on user-level rights and credentials.

**Does your district have numerous internal IPs? If so, STS strongly recommends completing an Internal Network Penetration Test on critical assets ONLY (i.e., servers, routers, firewalls) in conjunction with a Vulnerability Scan on the rest of the IPs. In addition, because workstations often represent an area of potential risk, it may be helpful to consider testing a representative sampling of workstations as well.*

IMPLEMENTING YOUR CYBERSECURITY RISK MANAGEMENT ROADMAP

Personnel and Policy Solutions

PERSONNEL SOLUTIONS

"The "human factor" in cybersecurity is the school's most vulnerable point of concern, whether through neglect or through the increasingly sophisticated evolution of social engineering techniques by cybercriminals." - ATLIS Cybersecurity Recommendations (October 2020)

Email Campaigns

We have several solutions that send email campaigns to your staff to see if they are vulnerable to phishing threats

End-User Awareness Training

Engaging training material from our partner, KnowBe4, to help your staff understand risks associated with emails and attacks. We can also provide end-user training for your team to educate them on recognizing and avoiding phishing email threats.

Social Engineering "People Hacking"

Social engineering or "people hacking" is currently the number one threat to schools and districts. This critical service includes developing and executing scripts for targeted phone and/or email campaigns designed to test whether employees will divulge sensitive security information related to passwords. No passwords, however, are collected. The final report will provide districts with actionable data to properly educate employees on their role in protecting the district's data. phishing email threats.

POLICY AND PROCEDURE SOLUTIONS

"Changes in legislation, the threat landscape, risk assessment, and even the school administration can affect the school's stance on cyber safety issues. Developing and revising policies and procedures as part of a process of vigilant review is required as new factors emerge." -ATLIS Cybersecurity Recommendations (October 2020)

Cybersecurity Policy Development

A wide variety of personnel and institutional policies have cybersecurity implications. Have a school cybersecurity expert help your cybersecurity team review policies for potential risks and recommend changes to mitigate your risks.

Cybersecurity Project Management

Once needs are identified, some schools and districts still feel ill-equipped to implement the risk management solutions. Contract with one of our school technology experts to manage the implementation of cybersecurity recommendations on behalf of the school or district as an "owner's rep."

24x7 Managed Network Security

Count on our multi-layer defense and detection strategy to detect, mitigate and respond to advanced threats.

- Advanced correlation
- Real-time alerts
- Malicious activity remediation
- Integrated incident management workflow
- Audit-ready compliance reports
- Compatible with over 1,000 network devices, operating systems, servers & other appliances
- Low monthly cost

IMPLEMENTING YOUR CYBERSECURITY RISK MANAGEMENT ROADMAP

Technical Solutions

Solutions	Description	NIST Cybersecurity Framework					Strategic Partners
		Identify	Protect	Detect	Respond	Recover	
EDR Solutions	Software that provides deep visibility into your endpoints, allowing for better protection and remediation of attacks as well as in-depth analysis of attacks in an easy-to-use interface.		✓	✓		✓	Sophos
MDR Solutions	Cybersecurity experts manage the above software to remediate all managed endpoints and provide deep reporting relating to any attacks.			✓	✓	✓	SentinelOne Sophos
Protection	These solutions can help protect all your sensitive data, both on-premise and in the cloud, with built-in ransomware protection. *Includes enhanced data protection and automation workflows to help identify, protect, and remediate from Ransomware attacks.		✓	✓		✓	Rubrik* DellEMC Veeam Commvault Datto/Backupify
SaaS	It gives you visibility across your entire Google and Microsoft cloud solutions, enabling you to automate protection responses and understand your total security posture.	✓	✓	✓			Managed Methods
Solutions	Layer 7 application firewalls with real-time threat protection for both your private and cloud data center needs.		✓	✓			Palo Alto Fortinet Checkpoint
MFA Solutions	Multi-Factor Authentication solutions to protect your systems to ensure your employees are logging in and not bad actors.		✓				Lastpass IDAuto
Patch Management Solutions	Solutions to help automate patching of operating systems and applications on all of your endpoints.		✓				Tanium SCCM JAMF Mosyle Microsoft Endpoint Protection
SPAM Filters	Email protection solutions to block malicious links and content from getting into your staff and teacher inboxes.		✓				Sophos Barracuda
Automated User Account Management	Implementing automated account lifecycle management is one of the best ways to ensure bad actors can't use old accounts to compromise your environments.		✓				IDAuto
Vulnerability Management	Gain visibility over all your assets and if they provide any security risks.		✓	✓			Tanium
Physical Security	Security doesn't apply to just the virtual world. Ensure you have the solutions in place that monitor and protect access to your environments.		✓	✓			Rhombus (C, ES) Entry Sign (VM) Genea (DAC) Halo (ES) Axis (C) Verkada (C, DAC, ES) HID (DAC) Milestone (C) Panasonic/Video Insight (C)

Protecting schools, students, and families from cyber threats is not solely a technology problem. Schools and districts should rely on a combination of training, technical solutions, policies, and procedures to proactively manage potential cybersecurity threats effectively.

READY TO LEARN MORE ABOUT CYBERSECURITY SOLUTIONS AND/OR MANAGED SECURITY SERVICES FROM STS?

LET'S TALK SECURITY!

David Hubbard
(805) 842-3637
david.hubbard@stseducation-us.com