

Information Security Services K-12 School Districts

Technology is critical to the classroom. Digital learning programs such as blended learning, online portals, and BYOD are just a few examples of the role technology plays in schools. While technology has a positive impact and is transforming how students learn, your networks, servers and websites are storing more critical information than ever. And it's not just the personally identifiable information (PII) residing your network, but also the PII recorded on physical documents.

Many years ago, state and local institutions were not high on threat actors list of targets. Now, threat actors from all over the world consider state and local institutions as ideal targets.

School districts host a wide range of high-value digital information on their networks, such as student PII, bus routes, after school programs, and payment card information for example. Schools can also be a tunnel to hackers' intended target such as government agencies, services contractors and vendors. Threat actors know school district IT departments typically lack the resources, budget, time and expertise to defend their networks from cyber attacks and data breaches.

Cyber Attacks Can Result in:

- Breaches and infections
- Non-compliance fees and penalties
- Disruption of the learning experience and school operations
- Loss of community trust
- Lost time and expense
- Legal liability
- Financial consequences

"Parents entrust schools to create and maintain a safe environment for their children. This extends beyond the physical security of the buildings and includes student data as well."

—Brian Spittle, Director of Technologies
Fort Mill School District, South Carolina

[Read the full Fort Mill School District Case Study >](#)

K-12 Schools Cyber Concerns

- **Attacks and Data Breaches**
Cyber incidents can be costly in terms of time, money and reputation.
- **Data Privacy**
Safeguarding the privacy, security and confidentiality of student, employee and community data.
- **More Attack Vectors**
Defending networks from even more threat vectors such as social media, BYOD, e-learning systems and student hackers.
- **Balancing Network Defense and Accessibility**
Providing students, parents and staff access to portals and other online tools without compromising network security.
- **Compliance**
Achieving and maintaining the unique K-12 compliance requirements, such as CIPA and FERPA.
- **Lack of Security Awareness**
Phishing attacks have increased but only 50 percent of educational institutions have an employee educational and training program.¹

School districts need to have a strong and robust security program in place to provide exceptional services and resources to the students and community. SecureWorks is a security partner who can extend your security capabilities, allowing you to focus on enhancing the students' educational experience.

An Extension of Your Security Capabilities

An effective information security program involves protecting your organization from emerging threats while embracing new technologies and managing daily operations, and ensuring compliance with countless rules and regulations. Combine this with the challenges of finding and retaining experienced security staff and identifying the best way to allocate your budget and resources, and it becomes quite clear that IT security groups are too often stretched thin.

"To protect the data privacy of students, teachers and staff, we're confident we're doing all we can do and improving on that daily, with SecureWorks on call if needed."

— Brian Spittle, Director of Technologies
Fort Mill School District, South Carolina

Organizations choose to partner with SecureWorks because we understand these challenges. We have created a diverse portfolio of information security solutions that empower security teams to focus resources where they make the most sense. Our security experts serve as an extension of your team, filling in the gaps to strengthen your organization's security and compliance postures, and reduce your risk.

SecureWorks Solutions

Security Solutions

SecureWorks offers a wide range of managed IT security solutions for enterprise clients. The strength of our security solutions lies in our proprietary management technology, SecureWorks Counter Threat Platform, our certified security analysts and elite threat intelligence to help protect clients from attacks 24x7.

Our security analysts serve as an extension of your team to monitor for and detect threats across your environment.

Security and Risk Consulting

Our Security and Risk Consulting team provides strategic advice and analysis to help you enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency.

Our highly skilled security consultants can help you test and improve your security defenses, streamline security processes, and design and develop new security programs.

Intelligence

The SecureWorks Counter Threat Unit research team collects relevant information wherever it can be found, and then analyzes and synthesizes it into meaningful guidance on which you can act.

Our intelligence can help you identify actors who may be specifically targeting your organization or its executives, and provides the insights to help you defend and even preempt the attacker.

Incident Response and Management

Our incident management practice provides rapid containment and eradication of threats, minimizing the duration and impact of a security breach to your organization.

Leveraging our cyber threat intelligence and global visibility, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents.

SecureWorks has been awarded *SC Magazine's* 2015 Best Managed Security Services Provider



For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com

1. Price Waterhouse Coopers Global State of Information Security Survey, 2016
2. [Complete Fort Mill School District Case Study](#)