In September 2017, a small school district in Montana was targeted by threat actors with what seemed to be a typical ransomware attack. Initially, the story didn’t make national headlines, but it soon became apparent that this attack was far more disturbing than any ordinary ransomware attack.

The hacker group had acquired email addresses, phone numbers and home addresses of students, parents and leaders, and began sending personalized messages with disturbing threats of violence if their demands weren’t met.

Understandably, the threats terrified school and community leaders, and fear soon spread to neighboring towns. Within days, over 30 schools and a local community college were closed, affecting more than 15,000 students.

While most cybersecurity and law enforcement experts agreed that the actual risk of violence was extremely low, there still existed another very real threat: that the hackers would release highly sensitive data they claimed they had taken from counseling and school health records—information that could be used to potentially embarrass or bully vulnerable students.

**A general strategy for reducing your attack surface**

Clearly, school district and site leaders have a weighty responsibility to protect the data they hold. But the increasing size and complexity of the K-12 technology landscape makes this challenging. Whether large or small, school districts have thousands of people using an incredibly wide range of devices—all of which have to be managed and secured.

Each of these connections becomes a potential vector for attackers looking to breach your school district, and as the attack surface grows, so does the importance—and challenge—of managing risk.

The better you are at developing an organizational understanding of cybersecurity risk to systems, people, assets, data and capabilities, the more prepared you can be to manage those risks.

Dr. William Kennedy, a cybersecurity expert at Verizon, advises school systems to adopt a holistic approach to improve their risk posture and specifically recommends four key strategies for improving cybersecurity strength and lowering risks.

---

**In 2019, 9 out of 10 breaches against educational institutions were motivated by money.**

**Ransomware is everywhere.**

Ransomware now accounts for 27% of malware incidents, and 18% of organizations blocked at least one piece of ransomware. No organization can afford to ignore it.
1. Implement a comprehensive risk mitigation strategy.

Prevention of a ransomware attack is never an easy undertaking. However, utilizing established cybersecurity best practices and being prepared for an attack could result in reduced damage and a quicker return to normal operations.

- Our Verizon experts can help start the risk mitigation process by sharing a thorough understanding of the historical and current cybersecurity threat environment that has or is being utilized to conduct ransomware attacks.
- We utilize cybersecurity threat intelligence sources to prioritize the threats to your specific environment and help you determine the funding of areas of critical vulnerabilities.
- We can help discover and document all devices, both desktop and various mobile devices, that are being used within your educational environment.
- We can also help discover and document all educational system users, including all of your stakeholders and clients (students and parents), as well as their network access methodology.
- We can help you effectively coordinate and utilize available federal, state and professional cybersecurity resources.

2. Create an effective cybersecurity program.

Our experts can help you plan the initial steps toward implementing an effective cybersecurity program, including developing a detailed understanding of your environment and documenting an approach or policy to address risk mitigation. These steps typically include the following:

- Building an effective cyber hygiene training program. A critical point of failure is not training staff members and clients on cybersecurity practices, particularly the importance of not opening attachments or links from unknown sources.
- Implementing segmentation of your network, as all staff and clients do not require the same level of data access.
- Ensuring that data is backed up on a daily basis to a security office site location. This action will be critical in a recovery operation.
- Ensuring that software is patched and kept up to date.

3. Monitor and protect your IT environment.

The recommended approach to an effective cybersecurity program is rather straightforward: Understand your weaknesses (vulnerabilities), strengths and threats within the educational landscape, and have a program in place to balance the costs and necessary level of cybersecurity based upon an intelligence-driven methodology. Our experts can help you:

- Conduct reoccurring cybersecurity assessment and penetration testing to identify and classify vulnerabilities.
- Maintain an active list of all authorized devices accessing the network and track any known device vulnerabilities.
4. Prepare for responding to the worst-case scenario.
The proper time to prepare for an attack is well before it occurs. Our experts can help you create a structured response plan that includes a communication strategy for informing staff and clients of any system lockdown or the introduction of a virus. A solid response plan should also define how to:

- Determine if you will budget to pay the ransom or budget for the prevention of the ransomware attack
- Develop a plan to recover the systems and data by using retrieved backup data storage to rebuild a clean system restoration

Cybersecurity risk assessment: Discover your weaknesses before a threat actor does!
Integrating the right end-to-end security program is a complex proposition, especially for school districts that lack sufficient IT and cybersecurity funding. Public-sector security experts warn that cybercriminals commonly troll for vulnerabilities that signal easy targets, which is why more districts are finding themselves in hacker crosshairs.
Recognizing this risk, we recommend that school districts engage with a reputable security vendor to conduct a cybersecurity risk assessment, which can provide a detailed, custom evaluation to help you strengthen your cybersecurity posture.

What is a cybersecurity risk assessment?
A cybersecurity risk assessment is a detailed analysis of your current IT environment that provides specific suggestions on how you can improve your district’s security goals, policies and processes.

A thorough assessment should produce an accurate snapshot of your IT environment, pinpoint areas that need improvement, answer any questions you might have about security issues and provide expert guidance on actions you can take to improve your security posture.

At its broadest level, a cybersecurity risk assessment can guide decision-making around a number of security initiatives and is ideally suited for:

- Protecting a network from emerging threats and known dangers on the internet, including, but not limited to, ransomware
- Training staff how to avoid enabling cybercrime, whether accidental or otherwise
- Teaching people using the network how to deter automated systems that troll for vulnerabilities

Ransomware is evolving quickly.
While early versions simply locked the files on your devices, new variants can lock the files you have stored on online services like Google Drive™ and Office 365®.
How does a cybersecurity risk assessment work?

In a cybersecurity risk assessment, experts work directly with IT leaders to 1) assess systems, 2) identify vulnerabilities and 3) create a plan for strengthening the organization’s cybersecurity program.

Using remote and onsite assessments, security experts comb through systems and networks to find weaknesses. The assessment method should be objective, evidence based and collaborative, which enables cybersecurity specialists to assess risks pertaining to:

• Intellectual property and reputation
• Web applications
• Email filters
• Phishing
• Wireless systems
• Premises and office facilities

Keep in mind that a proper assessment will employ security controls rooted in industry-standard frameworks and often integrate findings from respected cybersecurity reports such as the Verizon Data Breach Investigations Report (DBIR).

What formal guidance should a cybersecurity risk assessment provide?

After an assessment has been conducted, the insights gained should produce a number of valuable deliverables that outline detailed guidance on how to build a stronger security footing. These should include:

• Written reports that include test outcomes that are tailored to technical, managerial and executive-level users
• Assessment scores that measure how prepared you are to fend off an intrusion
• Risk-reducing recommendations for strengthening your security posture, prioritized by risk level
• Industry benchmarks to gauge how your security preparedness compares to peers across your industry

Breach discovery can take months.

Over a quarter of breaches were discovered months or more after the initial compromise.5
Additional things every district should consider

Verizon’s 2019 DBIR provided specific cybersecurity guidance for education leaders. This guidance is still relevant today.

Keep your lockers clean.

In education, poor security hygiene and a lack of attention to detail contribute to many of the breaches that occur. You can reduce human error by conducting regular cyber-hygiene training for IT staff as well as users. Gamification exercises can test how adept users are at detecting and responding to basic cyberthreats. In addition, you should establish a baseline level of security around internet-facing assets like web servers and employ two-factor authentication on those servers at a minimum.

The more visible you are, the more risk there is.

School districts that have cooperative program relationships with local higher education institutions or private businesses might be at a higher risk of cyber espionage than those that don’t. Understand what data you have or have access to, and keep in mind that you have personally identifiable information on students and faculty at the very least.

Small districts are not invisible.

No matter how low you try flying under the radar, there will always be cyberthreats that you need to be aware of. Phishing and general email security, ransomware and denial of service are all potential issues that should be threat-modeled and addressed.

Keep up your cybersecurity “continuing education.”

You should continue to engage with cybersecurity professionals to keep up to date with the latest threats and best practices. These experts are in the trenches every day and can provide up-to-the-minute guidance on current and emerging threats.

In 2019, more than half of organizations surveyed were less confident about the security of their mobile devices than that of their other systems.

Forty-eight percent of organizations do not have an efficient incident response plan in place.

What’s next:

Talk with a consultant to find out how a cybersecurity risk assessment can help you
Your ounce of prevention
What you know today can make all the difference tomorrow, which is why Verizon offers a range of cybersecurity thought leadership resources to provide the insights and knowledge you need to make smart decisions.

Data Breach Investigations Report
For over a decade, the Data Breach Investigations Report has analyzed hundreds of thousands of real-world incidents and data breaches to help security professionals better understand what they’re up against. Each scenario is drawn from a real-world investigation and is told from a different point of view, covering critical decision points, actions taken and crucial lessons learned.

Download the DBIR

Incident Preparedness and Response Report
This report is a new data-driven, scenario-based approach focusing on incident preparedness and response. It draws on three years of Verizon’s Incident Response Plan assessments and breach simulation exercises and provides valuable lessons learned to optimize your incident response plan. The report also provides firsthand insight into the six phases of incident response, as well as five “breach scenario” simulation kits that can help you apply learnings.

Download the report

Data Breach Digest
The Data Breach Digest scenarios break down some of the most interesting cybercrime cases from the Verizon Threat Research Advisory Center (VTRAC) Investigative Response Team's case files. It puts cybercrime in context, outlining the specifics of data breaches and cybersecurity incidents. It walks the reader through the situation leading to the incident, the investigative response approach and findings, and the lessons learned. These best practices can be applied by IT leaders to their cybersecurity and incident response posture to better prevent, better detect, better respond to and better recover from a data breach or cybersecurity incident.

Download the Data Breach Digest

Mobile Security Index
This comprehensive report takes a deep dive into the state of mobile security, looking at different types of threats and offering tips to protect your environment. Using the Mobile Security Index, organizations can protect against mobile security threats by establishing a “security-first” focus, developing and enforcing policies, and encrypting data over unsecured networks.

Download the Mobile Security Index

57%
Fifty-seven percent of database breaches involved insider threats within an organization.
**Payment Security Report**

Verizon's annual Payment Security Report on payment card security and compliance with the Payment Card Industry Data Security Standard (PCI DSS) looks at the details of payment security and PCI DSS compliance. The report has become vital reading for those responsible for data security or compliance with security standards such as the EU’s General Data Protection Regulation (GDPR), HIPAA or the Federal Information Security Management Act (FISMA).

Download the report 

**Insider Threat Report**

Insider threat activities are an exceptional challenge. Insiders enjoy trust, privilege and access. Add a detrimental motivation and potential disaster ensues. This presentation pivots off the Verizon Insider Threat Report with data breach data, scenarios and experience-driven insights into detecting and investigating insider threats.

Download the report 

**Monthly Intelligence Briefing**

This monthly briefing, hosted by the Verizon Threat Research Advisory Center, brings together our leading threat researchers and breach investigators to examine important security topics and review the current cybersecurity threat landscape. Content includes a featured topic (and guest speaker) along with current threat intelligence that covers attacks, advanced threat actor activities, threat indicators, malware trends and significant vulnerabilities.

Download the briefing 

For a deeper dive into all things cybersecurity, be sure to check out these additional resources:

- Verizon Threat Research Advisory Center
- Verizon Governance, Risk and Compliance
- Verizon Cyber Risk Programs

---


Network details & coverage maps at vzw.com. © 2020 Verizon. ART869052