SECURUS 360

WHEN IT COMES TO CYBER CRIME – BAD ACTORS NEVER SLEEP!

3 ACTIONABLE STEPS ANY K-12 SCHOOL DISTRICT CAN TAKE RIGHT NOW TO PROTECT THEIR STUDENT DATA AND ENTIRE TECHNOLOGY INFRASTRUCTURE

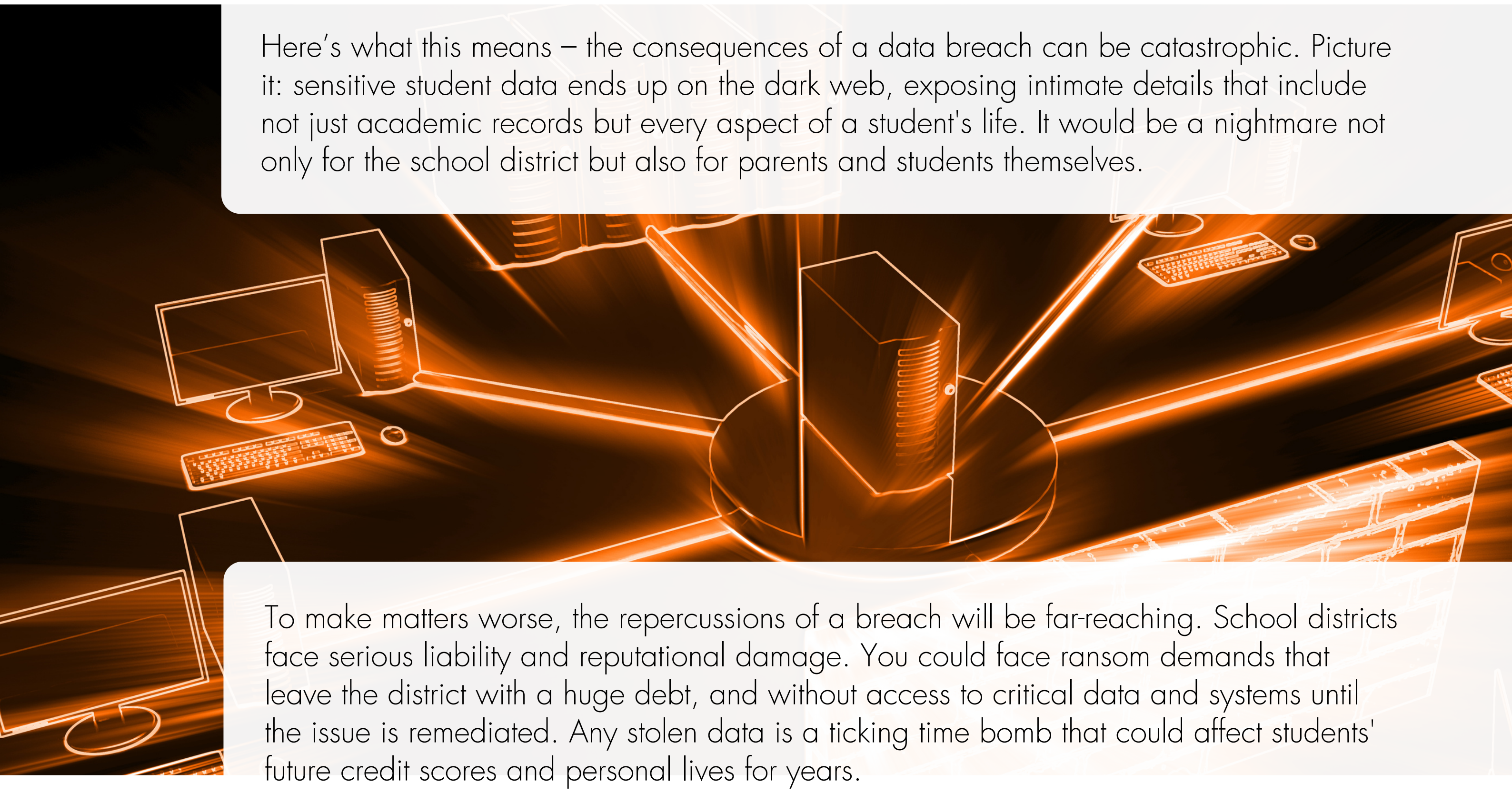
www.securus360.com | contact@securus360.com | (949) 266-6900

It won't be a surprise to hear that protecting student data is now more important than ever. Over the past several years, new technology has revolutionized the classroom, and it's a necessity in every aspect of running and maintaining a thriving school district.

With this digital revolution comes increased cybersecurity vulnerability, where highly valuable student and staff Personally Identifiable Information (PII) is more at risk than ever before. School districts are now faced with an unprecedented, and exponentially increased, burden to protect the mountains of sensitive data on their networks.

The reality is, there is more personal information in school districts' networks than simply names and SSNs. Highly personal student details are at risk, such as demographic information, economic backgrounds, grades, psychographics, medical conditions, and even records of personal traumatic experiences. Everything that happens inside and outside of the school appears in these files.

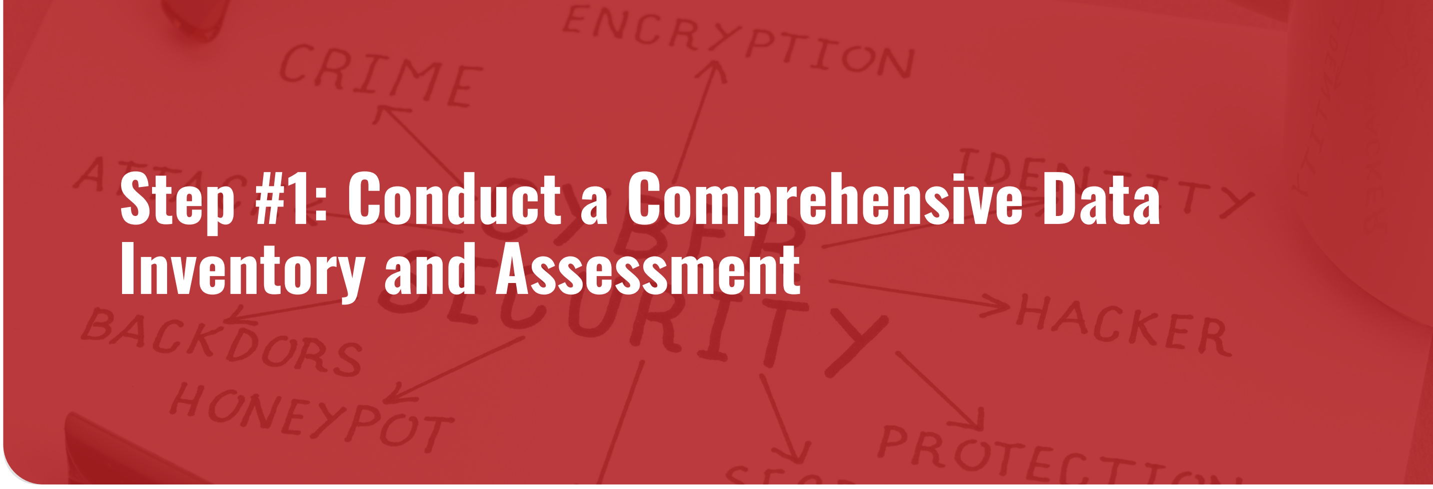
Here's what this means – the consequences of a data breach can be catastrophic. Picture it: sensitive student data ends up on the dark web, exposing intimate details that include not just academic records but every aspect of a student's life. It would be a nightmare not only for the school district but also for parents and students themselves.



To make matters worse, the repercussions of a breach will be far-reaching. School districts face serious liability and reputational damage. You could face ransom demands that leave the district with a huge debt, and without access to critical data and systems until the issue is remediated. Any stolen data is a ticking time bomb that could affect students' future credit scores and personal lives for years.

In this ever-evolving environment, the role of a K-12 IT department is more important than ever. You're not only IT professionals; you are actively protecting the future of your students.

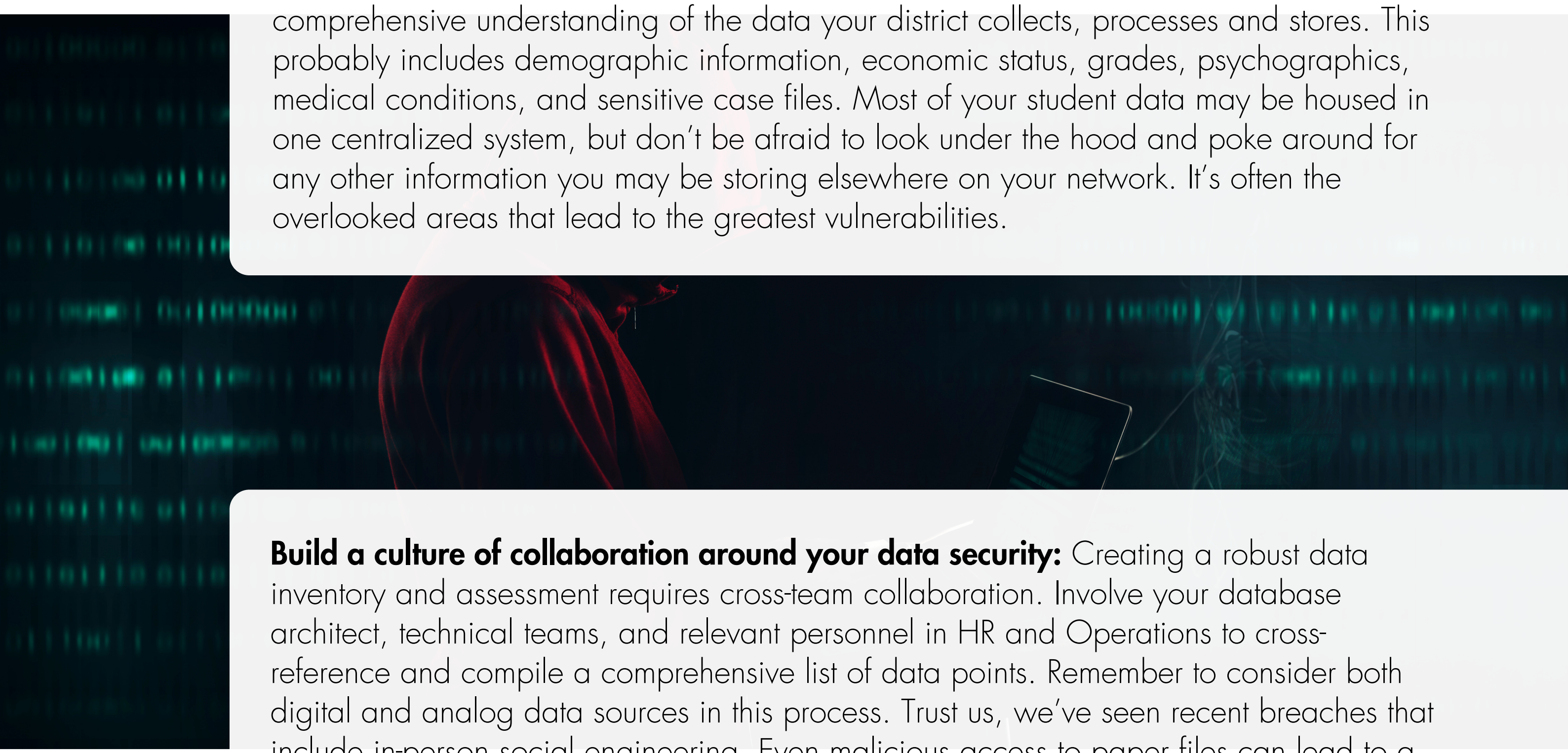
Luckily, you don't have to do it alone. This guide has been designed to help you by providing a comprehensive roadmap, equipping you with actionable tips, strategies and tools you can utilize today to navigate the complex landscape of protecting your network and student data.



Step #1: Conduct a Comprehensive Data Inventory and Assessment

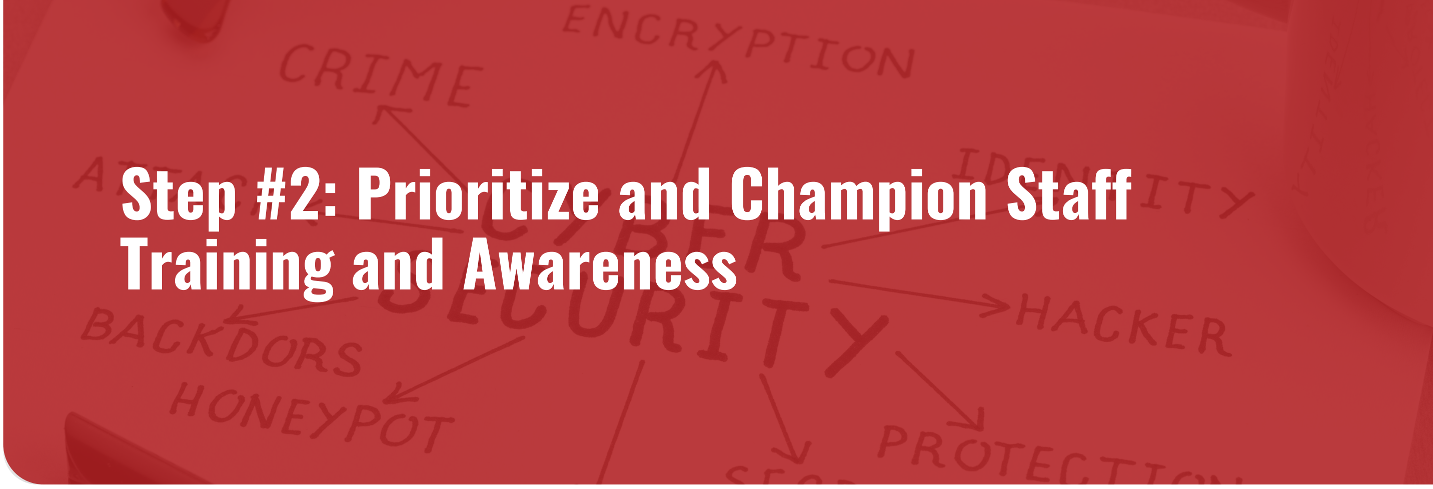
You can't map out a strategy for protecting your data until you understand exactly what data you must protect. Once you have a full understanding and inventory of your data, you can make informed decisions, identify vulnerabilities, and develop a targeted cybersecurity strategy to safeguard sensitive student information. Here's how to get started in running an inventory and assessment of your data:

Understand your data: The first step in safeguarding student data is gaining a comprehensive understanding of the data your district collects, processes and stores. This probably includes demographic information, economic status, grades, psychographics, medical conditions, and sensitive case files. Most of your student data may be housed in one centralized system, but don't be afraid to look under the hood and poke around for any other information you may be storing elsewhere on your network. It's often the overlooked areas that lead to the greatest vulnerabilities.



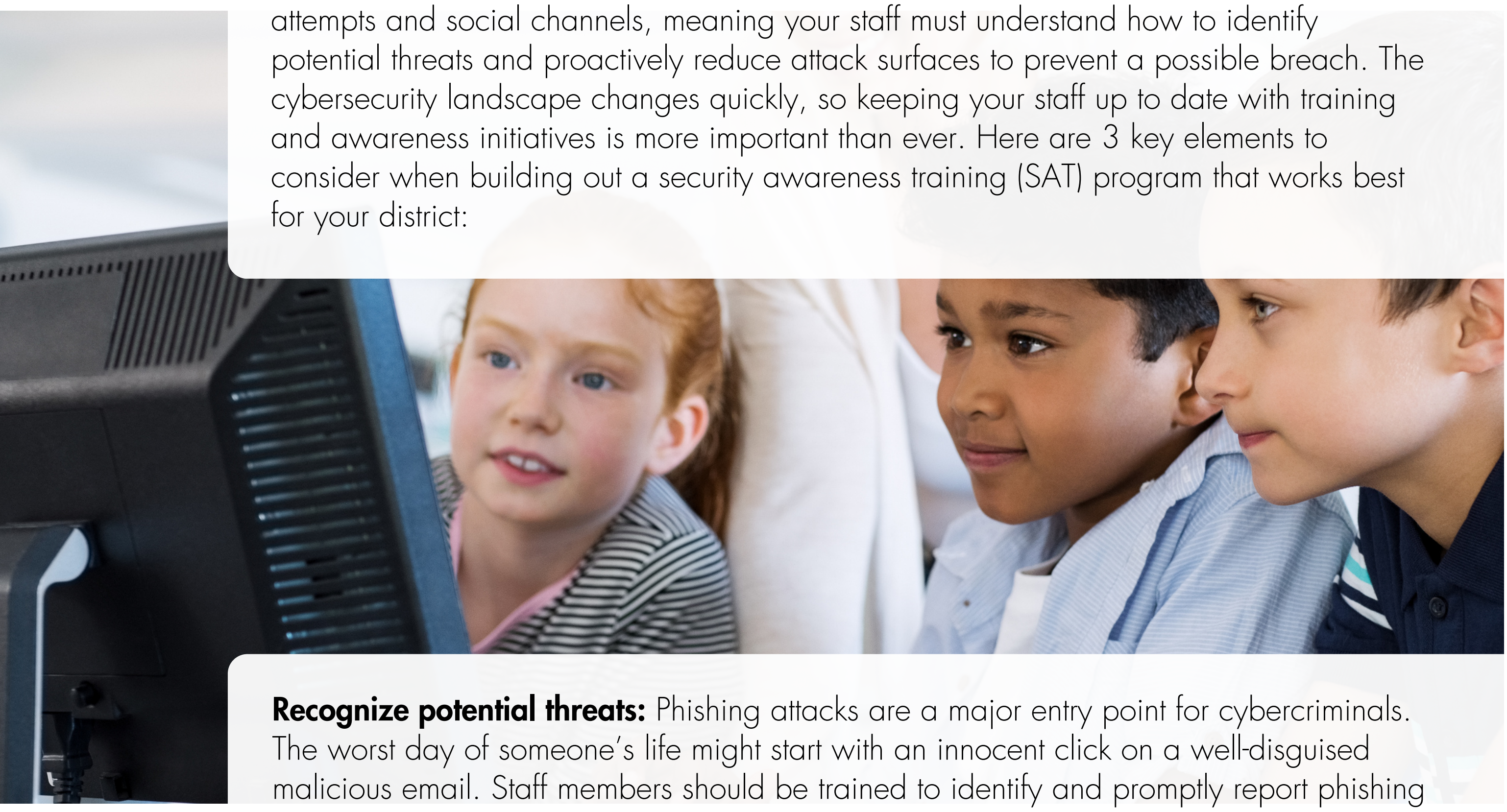
Build a culture of collaboration around your data security: Creating a robust data inventory and assessment requires cross-team collaboration. Involve your database architect, technical teams, and relevant personnel in HR and Operations to cross-reference and compile a comprehensive list of data points. Remember to consider both digital and analog data sources in this process. Trust us, we've seen recent breaches that include in-person social engineering. Even malicious access to paper files can lead to a full-on network breach.

Prioritize data security: Once you've identified the data you have stored within your network, you must prioritize its security. Not all data is equal, and some might need more (or less) protection. Ensure that everything is covered to prevent it from falling into the wrong hands. Read on for the best ways to prioritize data security!



Step #2: Prioritize and Champion Staff Training and Awareness

Your staff is your first line of defense. Many hacking attempts come through phishing attempts and social channels, meaning your staff must understand how to identify potential threats and proactively reduce attack surfaces to prevent a possible breach. The cybersecurity landscape changes quickly, so keeping your staff up to date with training and awareness initiatives is more important than ever. Here are 3 key elements to consider when building out a security awareness training (SAT) program that works best for your district:



Recognize potential threats: Phishing attacks are a major entry point for cybercriminals. The worst day of someone's life might start with an innocent click on a well-disguised malicious email. Staff members should be trained to identify and promptly report phishing attempts, whether through emails, phone calls or text messages. Understanding and recognizing the techniques often used in social engineering attacks can mean the difference between a failed phishing attempt and a multi-million dollar ransom demand.

"We don't have the manpower and the large budgets that the private industry might have. **Securus**360 has been a great partner, supporting our organization and my team by monitoring our entire network and critical endpoint devices for us 24/7."

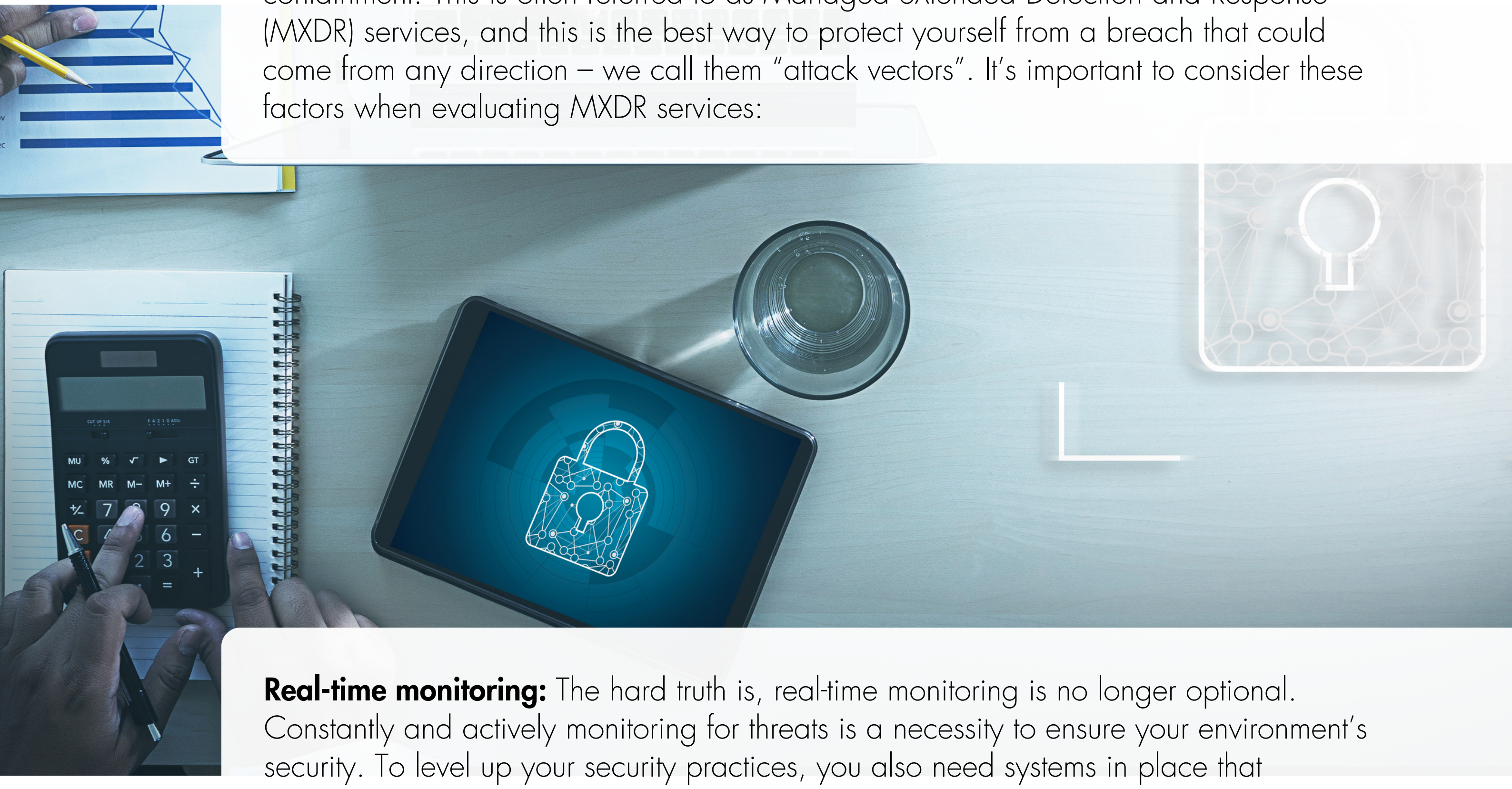
Gil Mara
Chief Ed Tech & Info Services Officer
Torrance USD

Consider a professional, third-party training program: Most cybersecurity companies now offer security awareness training services for organizations that want to train their employees to become more proactive in their fight against cybercrime. The best place to start is to evaluate the unique needs of your staff and look for a program that best fits those needs. Will your staff respond better to live classroom style training? Or modular online training they can conduct on their own time? Look, we've all been faced with requisite training programs that feel more like a burden than professional development. Working with a third-party vendor may help increase your completion rates and engagement through tried and tested methods. Whatever your training needs are, there's a program out there.

Encourage and champion strong participation: Creating a culture of cybersecurity awareness within your district is just as important as standardized training. It's important for senior management to lead by example and emphasize the value of security training. Regularly assess and encourage staff participation in programs to make it more engaging. Offer rewards or recognition when staff goes above and beyond with security protocols. Often, the best motivator is to paint a picture of what the successful – and unsuccessful – ending of a cybersecurity incident story might be. Anyone working at a school district has their students' best interest in mind, so connect the training effort to the protection of your students and you'll be likely to see a more motivated approach to training.

Step #3: Deploy a Comprehensive Approach to Cybersecurity

We said it before, and we'll say it again: bad actors never sleep. The cybersecurity landscape is constantly evolving, which means that your cybersecurity plan must be agile and ready to evolve as well. The single most important priority in developing a comprehensive cybersecurity plan is to ensure that you're set up with 24/7/365 monitoring of your infrastructure, which includes active threat hunting, threat detection and containment. This is often referred to as Managed eXtended Detection and Response (MXDR) services, and this is the best way to protect yourself from a breach that could come from any direction – we call them "attack vectors". It's important to consider these factors when evaluating MXDR services:



Real-time monitoring: The hard truth is, real-time monitoring is no longer optional. Constantly and actively monitoring for threats is a necessity to ensure your environment's security. To level up your security practices, you also need systems in place that proactively hunt for threats, identify them, and contain them efficiently. The best defense is a strong, proactive offense, and investing in comprehensive MXDR services. This is the best way to protect your school district.

Overcoming resource constraints: We recognize that budget and resource constraints can be a challenge for K-12 school districts. The reality is, hiring full-time employees to give you 24/7/365 monitoring and response is so expensive, it's off the table for most districts. Outsourcing these types of cybersecurity tasks can be a more cost-effective solution to augment your team, instead of taking on additional internal headcount and purchasing the necessary technology.

Choosing the right services: When evaluating MXDR services, it's important to carefully consider all the options. There are hundreds of cybersecurity companies out there who offer similar services. How do you know which one to pick? Look for companies and services that align with your district's specific needs and budget. You might find that a smaller cybersecurity company may be able to deliver the same robust services as any "big dog," but offer more hands-on support and consistent, proactive communication. Looking for companies that have experience working with and understanding the unique needs of K-12 school districts means both you and your cybersecurity provider will be on the same page when issues arise. It's never an imposition to request a detailed Service Level Agreement (SLA), and assess the scalability of each service to ensure you have full visibility into what it looks like to work with a vendor.

An investment in protecting your network is an investment in protecting your students.

A data breach can be catastrophic for any organization. But a data breach of a K-12 school district leads to damage at an entirely different level. To avoid sensitive data being stolen, leaked, and used for nefarious activities, you must have comprehensive, robust security practices in place across your entire district.

Protecting sensitive student data is about more than just ensuring files are kept safe. It's about equipping your staff with the resources they need to understand, identify, and mitigate issues from happening.

That might feel like a lot of pressure – but you're not alone. There are solutions and resources available, no matter the size or needs of your district. Start by implementing the steps laid out in this guide, and you'll be well on your way to boosting your cybersecurity posture and protecting your students.

A strong cybersecurity practice is not just an investment in data security; it's an investment in the future of the education and the well-being of the students you serve.

24/7 Protection: A Phone Call Away

School districts are prime targets for cyberattacks. In fact, the Education space is now the #1 most attacked industry in the United States. To make matters worse, K-12 IT teams often don't have the bandwidth and resources to mitigate fast-evolving, global threats.

We understand how much pressure you're under to defend your school district against constantly changing cyberattacks. Bad actors never sleep.But fortunately – neither do we (and neither does our AI-based MXDR platform!).

With **Securus360**, you'll be confident your network is protected from even the most sophisticated attack, and your IT team and district leaders will have the peace of mind they deserve, thanks to our exclusive concentration on K-12 cybersecurity, including:

- **Securus360** Products and services are optimized for school districts: We're singularly focused on cybersecurity for K-12 schools, so we know and can stop the specific threats targeting your district
- Razor-sharp focus on innovation: Our commitment to continuous improvement means you'll be ready for any evolving threats – even those that are highly sophisticated and have never been seen before
- Purpose-built hybrid intelligence: We combine machine learning and human expertise to make sure nothing falls through the cracks
- Full transparency: Our straightforward processes and proactive communication ensure you've got strategic support every step of the way

Let the experts at **Securus360** protect your student and staff identities and sensitive data so you can focus on what truly matters: your students.

Schedule a demo with **Securus360** today to see how we can alleviate security stress and build deeper resilience into your network.

No child's personal information should ever be at risk. And now, you don't have to shoulder that burden alone. Let **Securus360** help. Schedule a demo today.

Book A Demo

SECURUS 360