SECURUS360

3 WAYS TO PROTECT YOUR K-12 SCHOOL DISTRICT FROM RANSOMWARE ATTACKS

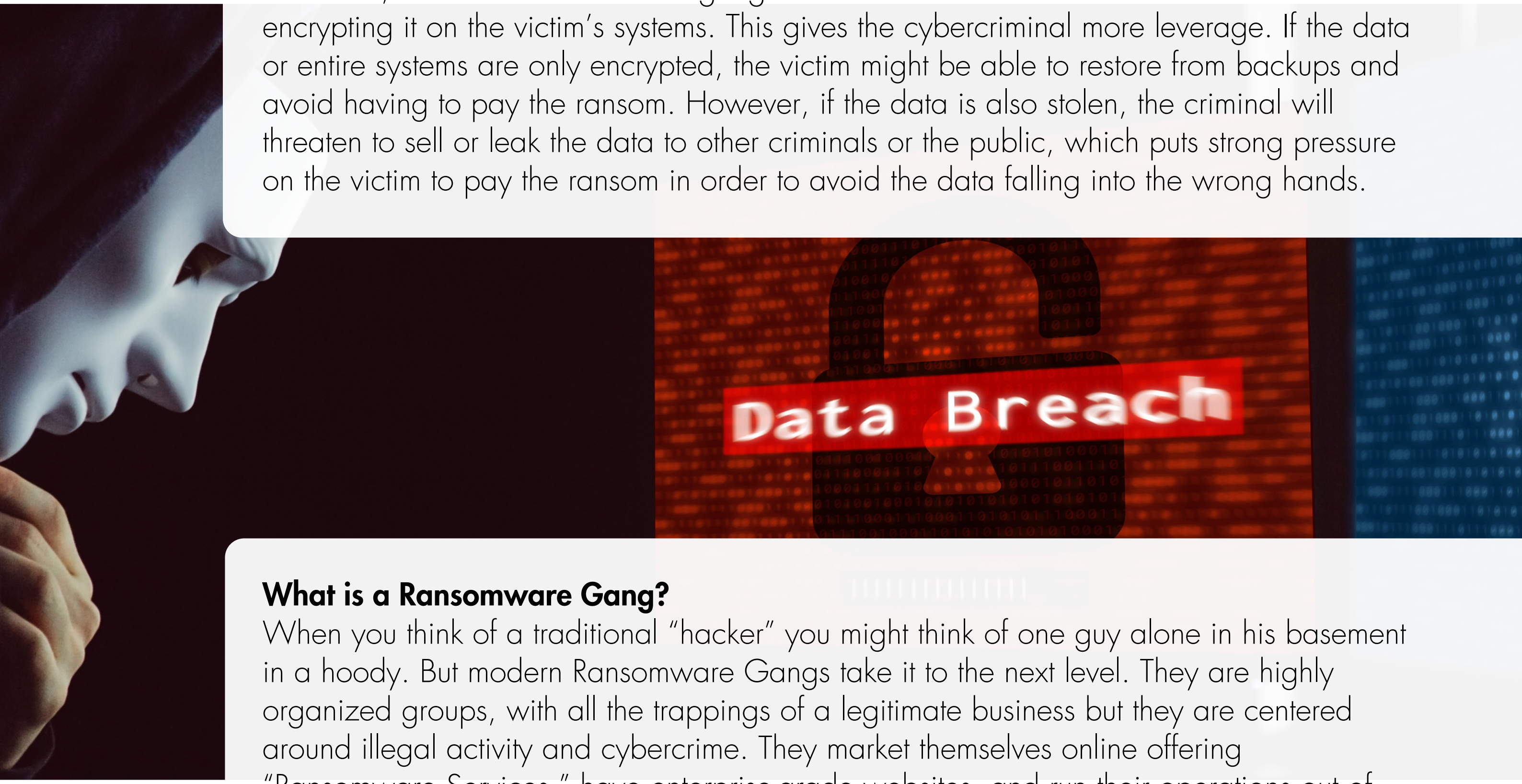
AN OLD ENEMY HAS EVOLVED INTO A MUCH MORE LETHAL THREAT TO K-12 SCHOOL DISTRICTS: THE RISE OF SOPHISTICATED, HIGHLY ORGANIZED RANSOMWARE GANGS

Since the beginning of 2023, attacks on educational institutions by Ransomware Gangs have increased by 84%, attacking not only large school districts but smaller districts in remote areas as well.

Ransomware Gangs find K-12 school districts to be particularly attractive targets not only because their networks are often wide open and vulnerable to attacks, but also because of the valuable data that schools are storing on their networks. Ransomware Gangs have evolved, becoming highly organized and sophisticated, and now have far more tactics at their disposal than ever before, enabling them to steal the valuable Personally Identifiable Information (PII) of your students and staff.

What is Ransomware?

Ransomware is a type of malicious software (malware) designed to breach your network then encrypt and extract sensitive data to hold it for ransom. While in the past, the data or entire systems would typically be encrypted in place and then simply be unencrypted after the ransom is paid, in recent years, most ransomware attacks use a method called "double extortion", where the ransomware gang exfiltrates and steals the data in addition to encrypting it on the victim's systems. This gives the cybercriminal more leverage. If the data or entire systems are only encrypted, the victim might be able to restore from backups and avoid having to pay the ransom. However, if the data is also stolen, the criminal will threaten to sell or leak the data to other criminals or the public, which puts strong pressure on the victim to pay the ransom in order to avoid the data falling into the wrong hands.



What is a Ransomware Gang?

When you think of a traditional "hacker" you might think of one guy alone in his basement in a hoody. But modern Ransomware Gangs take it to the next level. They are highly organized groups, with all the trappings of a legitimate business but they are centered around illegal activity and cybercrime. They market themselves online offering "Ransomware Services," have enterprise-grade websites, and run their operations out of traditional business offices.

Today, many Ransomware Gangs are using a "Ransomware-as-a-Service" (RaaS) model, where they make their ransomware code available to other cybercriminals for purchase or lease to use it to attack their victims. For example, LockBit, the largest RaaS Group, has collected more than $144m in ransom payment through hundreds of "affiliates". Ransomware Gangs are much more dangerous than a lone hacker trying to find a way into your network.

Their operations are sophisticated and coordinated. They even run "Bug Bounty"-like programs where they are paying other cybercriminals for information on new vulnerabilities they can exploit.

How can I identify a Ransomware Gang attack?

In the past, the number of attackers was much lower - they all developed and owned their own technology. Today, hundreds, if not thousands of "affiliates" are licensing RaaS technology from a relatively small number of providers, such as LockBit, Vice Society, AvosLocker, Medusa and others, to attack their victims. This is why the number of cyberattacks has increased so dramatically. This means that today, any school district is much more likely to be attacked than in the recent past, and the districts with less protection are the ones getting breached.

It might seem like these gangs only go after "the big ones" but this is a misconception. Every size of school district is vulnerable. Smaller districts are frequently targeted and usually do not have the resources and protection that larger districts have. Because of this, smaller districts may be more at risk than larger, more well-protected districts. Many districts are finding out the hard way that being smaller or lower profile than their neighboring districts, doesn't mean they won't be attacked.

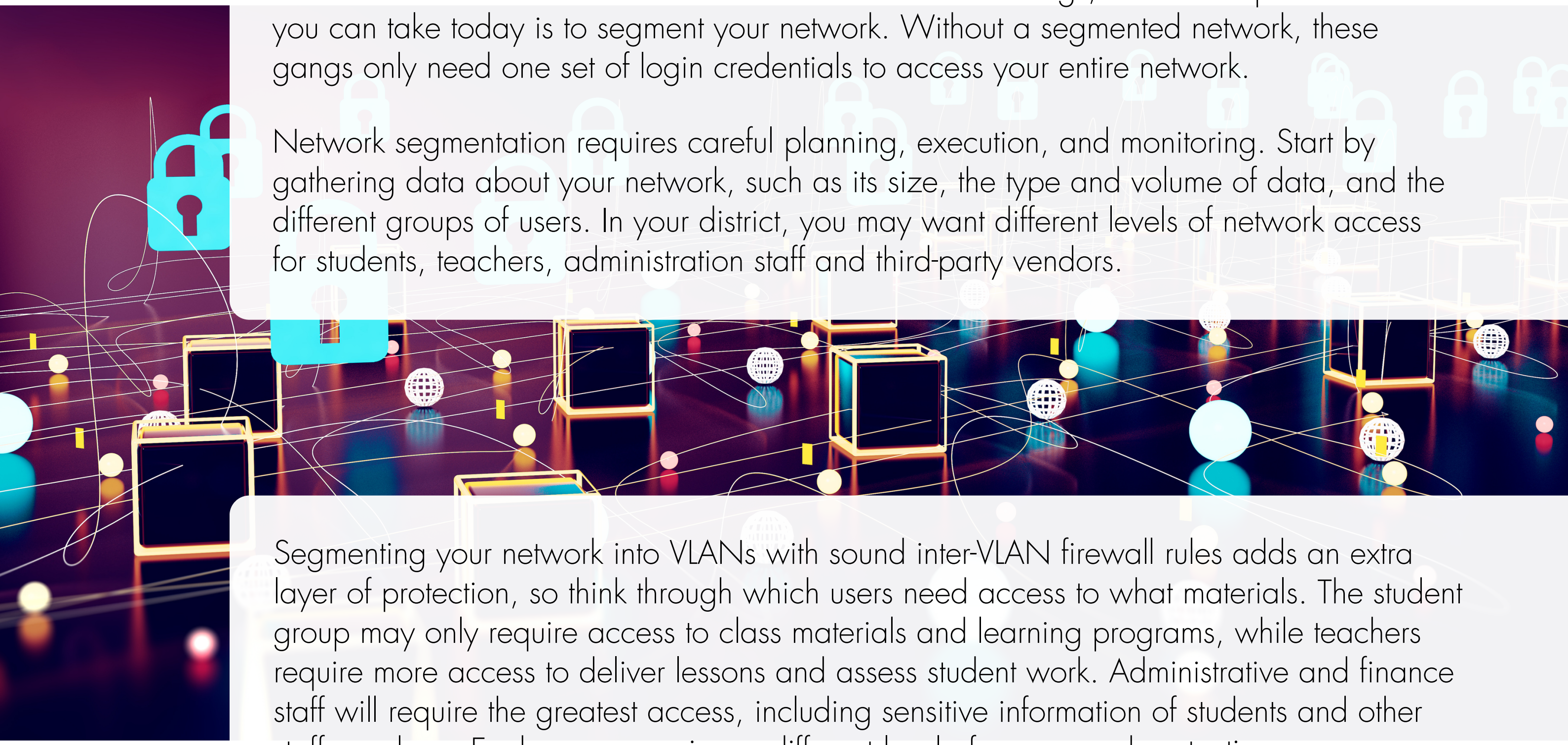
Given this unprecedented number of attacks against K-12 School Districts, it's more important than ever that you take action to protect your network. In this PDF, we'll cover 3 things you can do immediately to help protect your network and the sensitive data of your students and staff.

Actionable Tip 1: Segment your network now

Ransomware Gangs frequently target publicly available email addresses with social engineering attacks to gain access to your network, rather than attack a network with "brute force". The sad truth is, most K-12 staff, teacher and student emails are relatively easy to find via publicly available information. Once the hackers get ahold of a list of email addresses, they begin phishing attacks to lure users to take inadvertent actions or reveal their log-in information.

Because this is the most common tactic of Ransomware Gangs, the most important action you can take today is to segment your network. Without a segmented network, these gangs only need one set of login credentials to access your entire network.

Network segmentation requires careful planning, execution, and monitoring. Start by gathering data about your network, such as its size, the type and volume of data, and the different groups of users. In your district, you may want different levels of network access for students, teachers, administration staff and third-party vendors.



Segmenting your network into VLANs with sound inter-VLAN firewall rules adds an extra layer of protection, so think through which users need access to what materials. The student group may only require access to class materials and learning programs, while teachers require more access to deliver lessons and assess student work. Administrative and finance staff will require the greatest access, including sensitive information of students and other staff members. Each group requires a different level of access and protection.

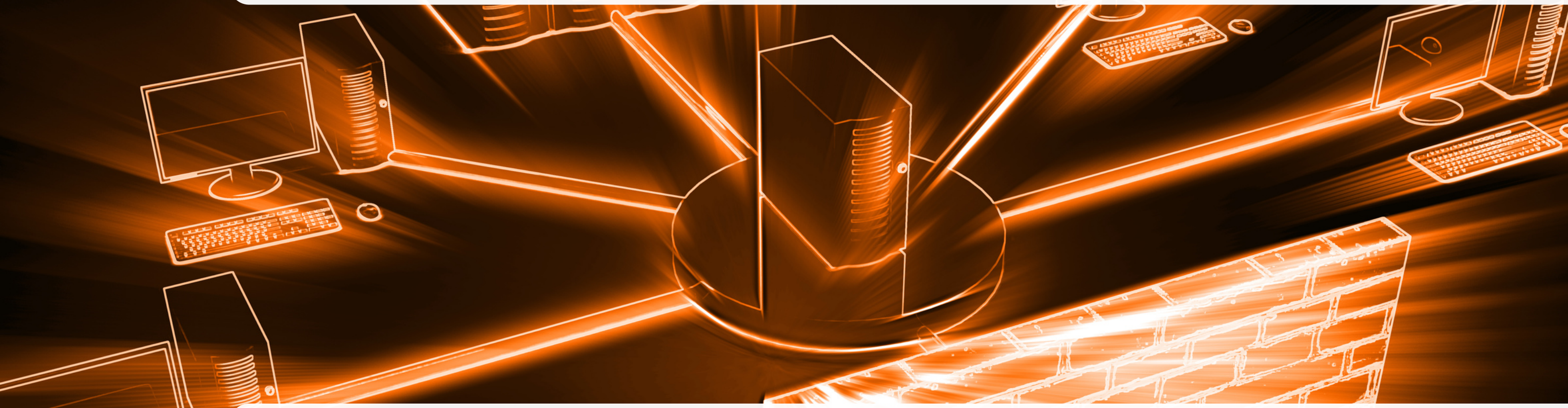
Once you have segmented each group into different layers of access, this will greatly reduce the risk of lateral movement between the groups. If your network is compromised from one segment, it will be difficult for Ransomware Gangs to gain access to a different segment of the network without overcoming additional security protocols. This will isolate a breach and minimize the scope of the attack.

An additional benefit of network segmentation is increased visibility into network activities, making monitoring easier. Each segment will have its own set of expected activities and anything suspicious can be easily identified, investigated, and quickly handled.

Actionable Tip 2: Conduct Security Awareness Training (SAT) for everyone in the school district

The easiest way for Ransomware Gangs to access your network is through user login credentials. These can be gained via credential phishing or man-in-the-middle (MITM) attacks, among other techniques. In many of these methods the user is often "the way in" for the bad guys, so your first line of defense is ensuring that every user in your district has completed Security Awareness Training (SAT).

This applies to all segments of your network - students, staff, administration, and third-party vendors. This includes anyone who has access to email and the internet and internal systems, including parents. If they can access your network with a password, that user is a possible entry point for Ransomware Gangs to strike.

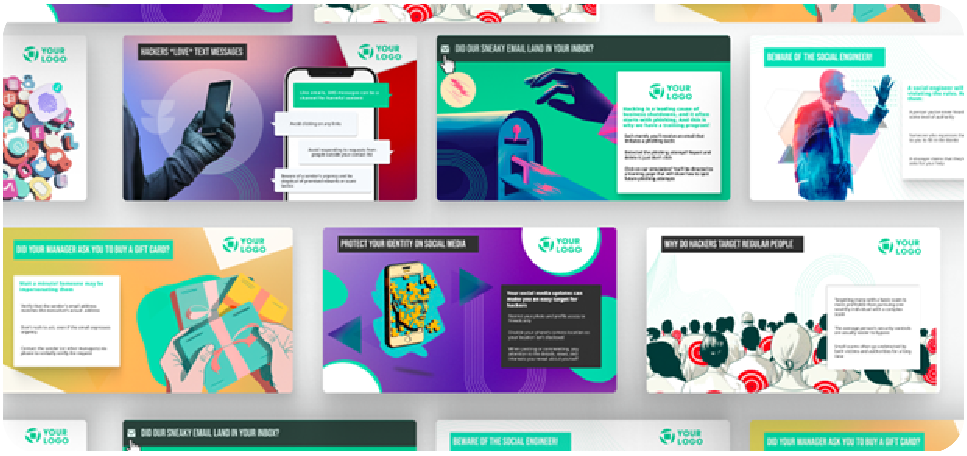


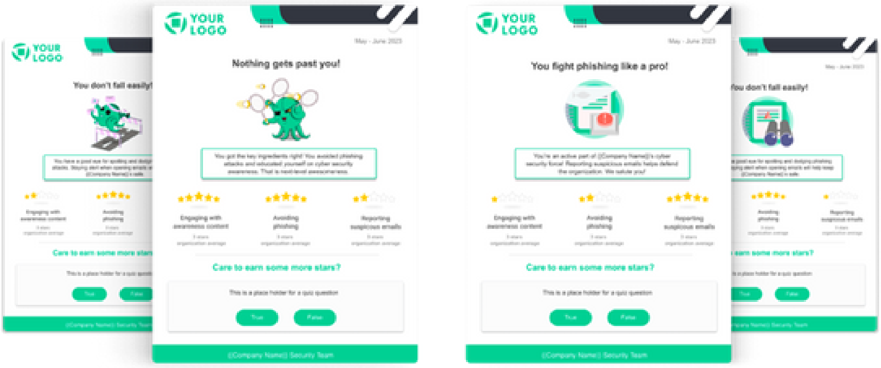
Ransomware Gangs love to exploit human error, and training can help reduce this risk. Modern SAT modules include a range of topics, from password best practices and phishing attack awareness, to email and web security, data privacy regulations, and response protocols for suspected incidents.

When your students, staff and administrators are informed and aware of different kinds of cyberattacks, they can be a powerful line of defense against ransomware attacks.

Security Awareness Training has evolved significantly and is no longer the often boring, irrelevant content that plagued everyone for the past 20 years. It has come a long way in the last few years, and now, SAT is focused on delivering relevant, interactive and engaging content that encourages everyone to play an active role in keeping the district, and sensitive data safe.

Securus360 is thrilled to partner with industry leader CybeReady to offer a best-in-class SAT program. With fun and interactive lessons, as well as games and high-production videos, these courses deliver the exact training needed to grow awareness across your entire district. Here are some examples of this type of high-quality training:


YOUR LOGO
HACKERS "LOVE" TEXT MESSAGES
DID OUR SNEAKY EMAIL LAND IN YOUR INBOX?
BEWARE OF THE SOCIAL ENGINEER!
DID YOUR MANAGER ASK YOU TO BUY A GIFT CARD?
PROTECT YOUR IDENTITY ON SOCIAL MEDIA
WHY DO HACKERS TARGET REGULAR PEOPLE


YOUR LOGO
May - June 2023
You don't fall easily!
Nothing gets past you!
You fight phishing like a pro!
Engaging with awareness content
Avoiding phishing
Reporting suspicious emails
Care to earn some more stars?
This is a place holder for a quiz question
True
False
{{Company Name}} Security Team

The cybersecurity landscape changes quickly, so training should be regularly updated and reinforced. This will create smart, aware users who take cybersecurity seriously. Everyone can take part in maintaining the security of the network.

"Little Miami School District Chief Technology Officer Stephen Collins speaks on how his districts cybersecurity posture has been strengthened by **Securus360** technology, and how much easier it is for he and his staff to manage any possible threats in their system"

Stephen Collins
CTO
Little Miami USD

Actionable Tip 3: Partner with a cybersecurity firm that offers a 24/7/365 Security Operations Center (SOC)

When you're up against a threat as sophisticated as a Ransomware Gang, there's only so much you can do onsite to ensure your network stays secure and protected. Even after you have segmented your network and provided SAT modules for all your users, the potential volume of these attacks is no match for any K-12 school district.

Remember, Ransomware Gangs operate by launching many sophisticated attacks simultaneously, helping to ensure that some of their targets are successfully breached. And they are focusing these attacks on night hours, and weekends and holidays—exactly when your staff is enjoying some well deserved time off. The best way to secure your network is to partner with a cybersecurity firm that offers 24/7/365 monitoring and a full-service Security Operations Center (SOC). This will ensure that when an attack happens, the response is quick and effective to minimize or eliminate damage altogether.

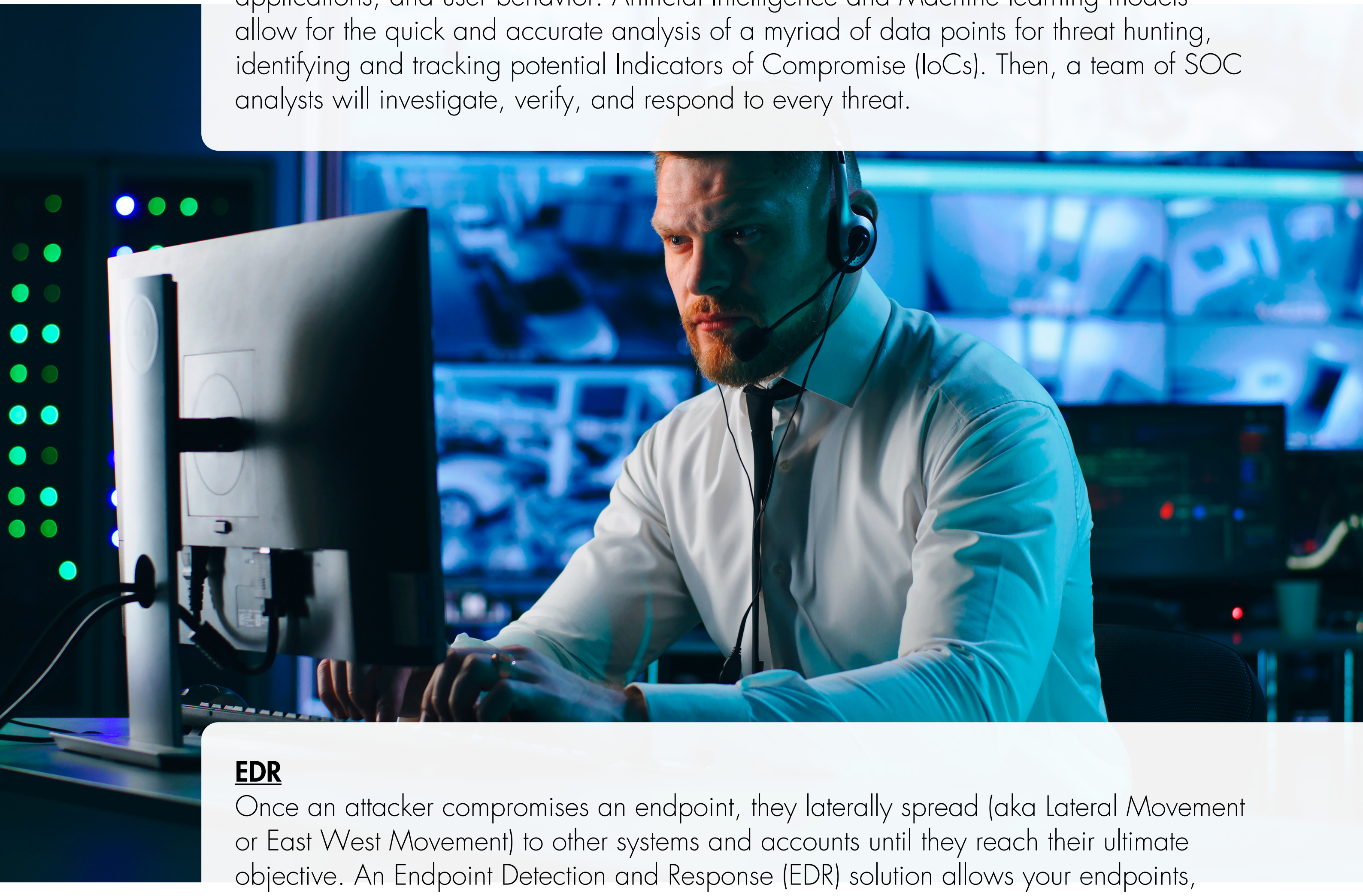
It's not a matter of "if" its only a matter of time to when your district will suffer a serious attack, but with a cyber security partner offering 24/7 protection and remediation services, you'll be ready.

Look for these types of services:

24/7/365 SOC
To ensure your network stays secure, 24/7/365 monitoring is essential. Let the experts look after your network by monitoring your entire IT environment. Vulnerability assessments and penetration testing are also essential to identify any gaps in your security before a Ransomware Gang does.

MXDR

A multi-vector Managed eXtended Detection and Response platform means that your K-12 school district is completely secured with a 360-degree defense around your entire technology infrastructure, monitoring endpoints, security devices, cloud environments, applications, and user behavior. Artificial Intelligence and Machine learning models allow for the quick and accurate analysis of a myriad of data points for threat hunting, identifying and tracking potential Indicators of Compromise (IoCs). Then, a team of SOC analysts will investigate, verify, and respond to every threat.



EDR

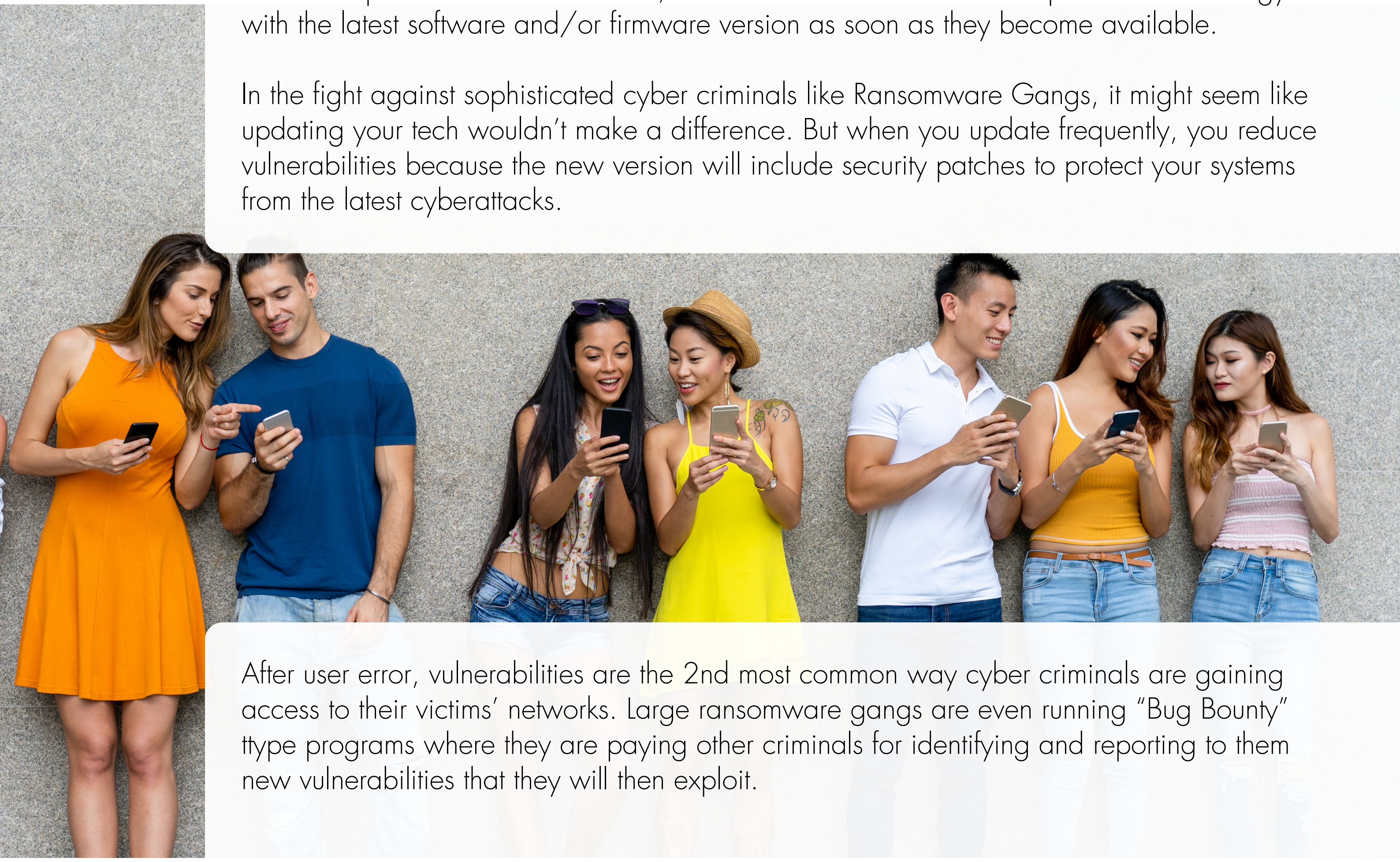
Once an attacker compromises an endpoint, they laterally spread (aka Lateral Movement or East West Movement) to other systems and accounts until they reach their ultimate objective. An Endpoint Detection and Response (EDR) solution allows your endpoints, including, workstations, tablets, and servers, to be isolated from the network instantly in the case of an attack, preventing the threat from spreading.

With a robust cybersecurity partner, you can sleep soundly knowing the sensitive data of your students and staff is safe.

BONUS Actionable Tip 4: Ensure all technology is regularly updated

Our final tip seems like a no-brainer, but it's essential. Make sure to update all technology with the latest software and/or firmware version as soon as they become available.

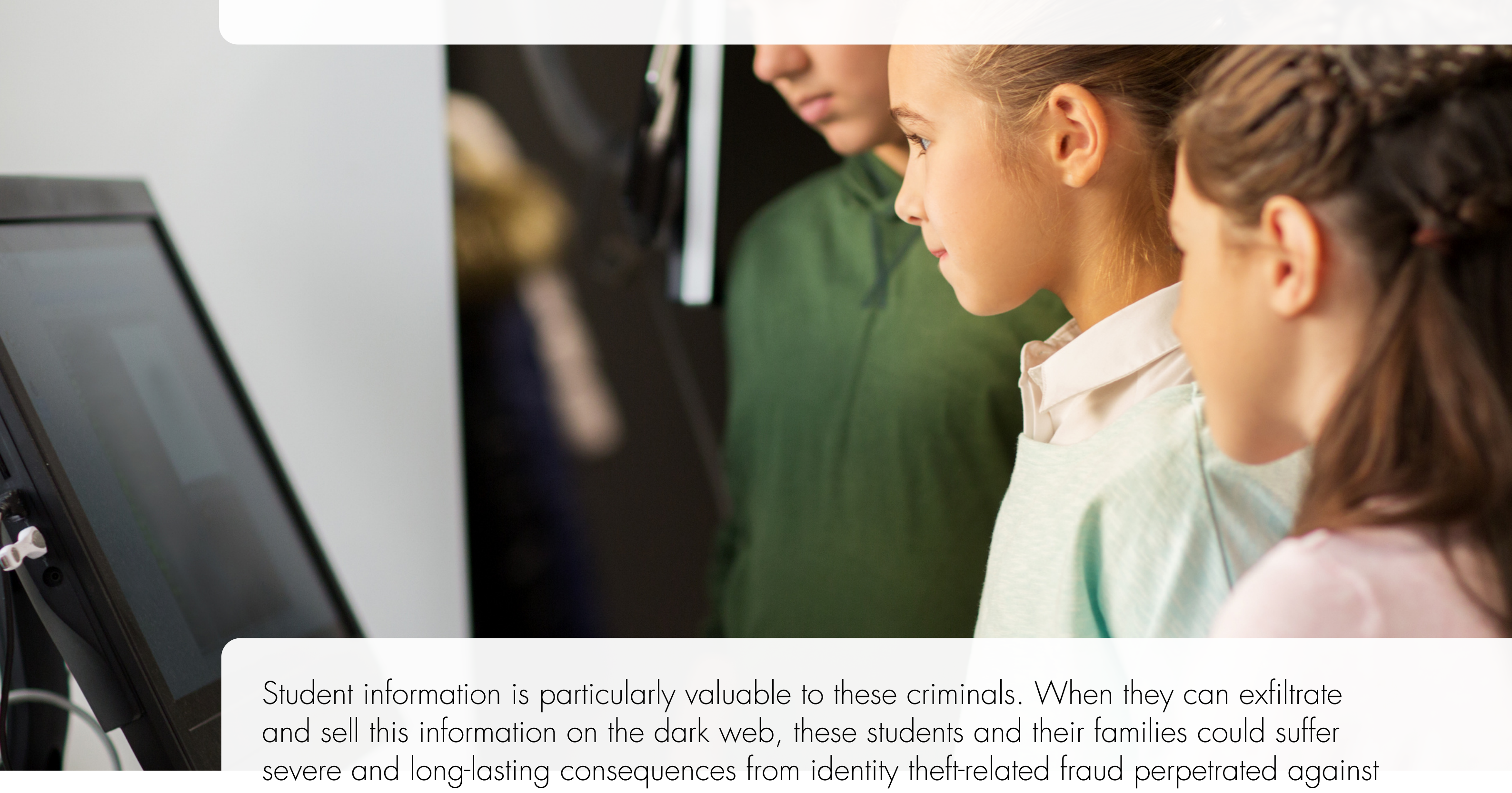
In the fight against sophisticated cyber criminals like Ransomware Gangs, it might seem like updating your tech wouldn't make a difference. But when you update frequently, you reduce vulnerabilities because the new version will include security patches to protect your systems from the latest cyberattacks.



After user error, vulnerabilities are the 2nd most common way cyber criminals are gaining access to their victims' networks. Large ransomware gangs are even running "Bug Bounty" ttype programs where they are paying other criminals for identifying and reporting to them new vulnerabilities that they will then exploit.

Conclusion

Over the last few years, the cybersecurity landscape has completely changed. Ransomware Gangs are launching far more and much more sophisticated cyberattacks than ever before. These gangs are targeting K-12 School Districts, not only because they know the education sector is more vulnerable (no matter the size or location of the district), but because of the value of the sensitive information of students and staff.



Student information is particularly valuable to these criminals. When they can exfiltrate and sell this information on the dark web, these students and their families could suffer severe and long-lasting consequences from identity theft-related fraud perpetrated against them.

But there is hope. By taking action to secure your network now, you can ensure your student and staff information stays protected. And with the right cybersecurity partner, that information will stay safe from Ransomware Gangs and cybercriminals everywhere.

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 artificial intelligence, 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