SECURUS360

RANSOMWARE-AS-A-SERVICE IS CHANGING THE CYBERSECURITY GAME (AND NOT FOR THE BETTER)

3 ACTIONS K-12 SCHOOL DISTRICTS NEED TO TAKE TO PROTECT THEMSELVES NOW

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

This is bad news for school districts. IT teams are already strapped for resources, and staff and budgets are being cut. With this lack of resources, vulnerabilities in their networks increase. Basic cybersecurity practices such as antivirus software, DNS filtering, and firewalls are not enough to stop today's sophisticated ransomware attacks. RaaS Groups aren't just targeting the big school districts in big cities. They're going after small and medium-sized school districts, too. When those smaller school districts are breached, the results can be catastrophic for students, staff, and the community.

Here's the good news: there are a few things you can do today to begin to shore up the cybersecurity protection in your network.

In this discussion, we'll cover 3 advanced processes you can begin today that will lead to a safer, more secure network for your school district.

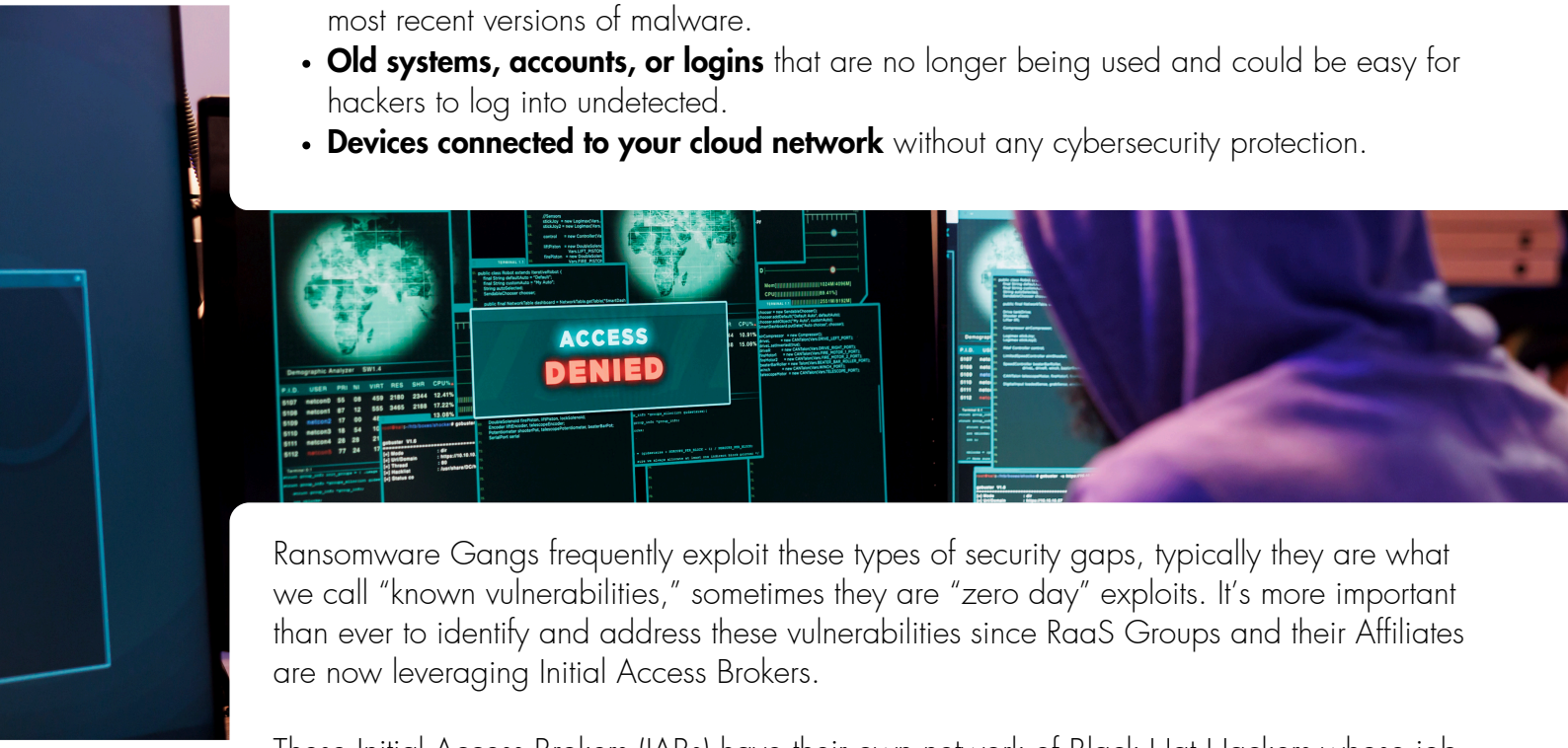
Actionable Tip 1: Identify, Prioritize and Address Critical Vulnerabilities

It is impossible to protect your network until you know where it is most vulnerable.

The first step to address critical vulnerabilities is to identify them with a vulnerability scan. Using scanning software, you can identify gaps in your security posture.

Gaps could include:

- **Out-of-date software or firmware**, missing critical updates that protect against the most recent versions of malware.
- **Old systems, accounts, or logins** that are no longer being used and could be easy for hackers to log into undetected.
- **Devices connected to your cloud network** without any cybersecurity protection.



Ransomware Gangs frequently exploit these types of security gaps, typically they are what we call "known vulnerabilities," sometimes they are "zero day" exploits. It's more important than ever to identify and address these vulnerabilities since RaaS Groups and their Affiliates are now leveraging Initial Access Brokers.

These Initial Access Brokers (IABs) have their own network of Black Hat Hackers whose job it is to gain access to a victim organization but without exploiting that access themselves. Instead, they sell that access via the IAB to an Affiliate or the RaaS Operator. They gain access by stealing credentials via social engineering attacks or hunting for vulnerabilities. Rarely is access gained by way of brute force anymore. IABs and RaaS Operators are even offering Bug Bounty Programs that pay these "pentesters" (network penetration testers) for uncovering new vulnerabilities.

Once cyber criminals gain access to your network, they can move laterally within it. From there, they might gain access to your records and databases and the most sensitive information about students and staff.

Actionable Tip 2: Increase Security Awareness Training Across Your School District

The easiest and fastest way for Ransomware Gangs to access your network is through compromised user login credentials.

Your students or staff might unknowingly let bad actors into your network.

Phishing emails and texts are the most common. But cybercriminals have become more creative than ever, even using phishing techniques over voice calls or snail mail. Examples are: spoofed emails offering gift cards, or the "IT guy" calling a user, pretending they have to "update their system, but just need the user's password real quick to install the latest software."

It's essential to increase Security Awareness Training (SAT) efforts to combat phishing. This applies to all users in your network (students, staff, administration, and third-party vendors and partners), and even parents who have access to their student's login credentials. If they can access devices on your network with a password, that user is a possible entry point for cybercriminals.

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

When your students, staff and administrators are equipped with the necessary knowledge and basic skills around cybersecurity, they can be a powerful line of defense against Ransomware Gangs. SAT is focused on delivering relevant information that encourages everyone to play an active role in keeping the school district and sensitive data safe.

Securus360 has partnered with market leader **CybeReady** to offer best-in-class Security Awareness Training created specifically for K-12 School Districts. The program provides interactive, engaging, and highly effective training modules for your entire school district.

Actionable Tip 3: Implement Network Segmentation

Ransomware Gangs frequently target publicly available email addresses to gain access to your network. Many K-12 student, teacher, and staff emails are readily available via public information. Once the hackers have this information, they initiate phishing attacks to lure and trick users into taking inadvertent, detrimental actions or revealing their login information.

It only takes one click on a bad link for a Ransomware Group to gain access and wreak havoc on your network. Because of this, the most important action you can take today is to segment your network. Without a segmented network, bad actors can move laterally within your network with just one login.

Segmenting your network adds an extra layer of protection, so think through which users need access to what materials or systems. 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 school district, you may want different levels of network access for students, teachers, administration staff, and third-party vendors. For example, students do not need access to platforms for teachers, or accounting or HR systems that hold records and other sensitive data. Each group requires a different level of access and protection.

Focus on protecting your most critical assets to minimize damage if defenses fail. 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 damage 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.

Ransomware Gangs have completely changed the face of cybersecurity.

Just a few years ago, most cyber security attacks came from a single hacker going after high-profile targets. Hacking was more challenging, so bad actors concentrated their efforts on those victims that would promise a larger payout.

Now they're going after everyone.

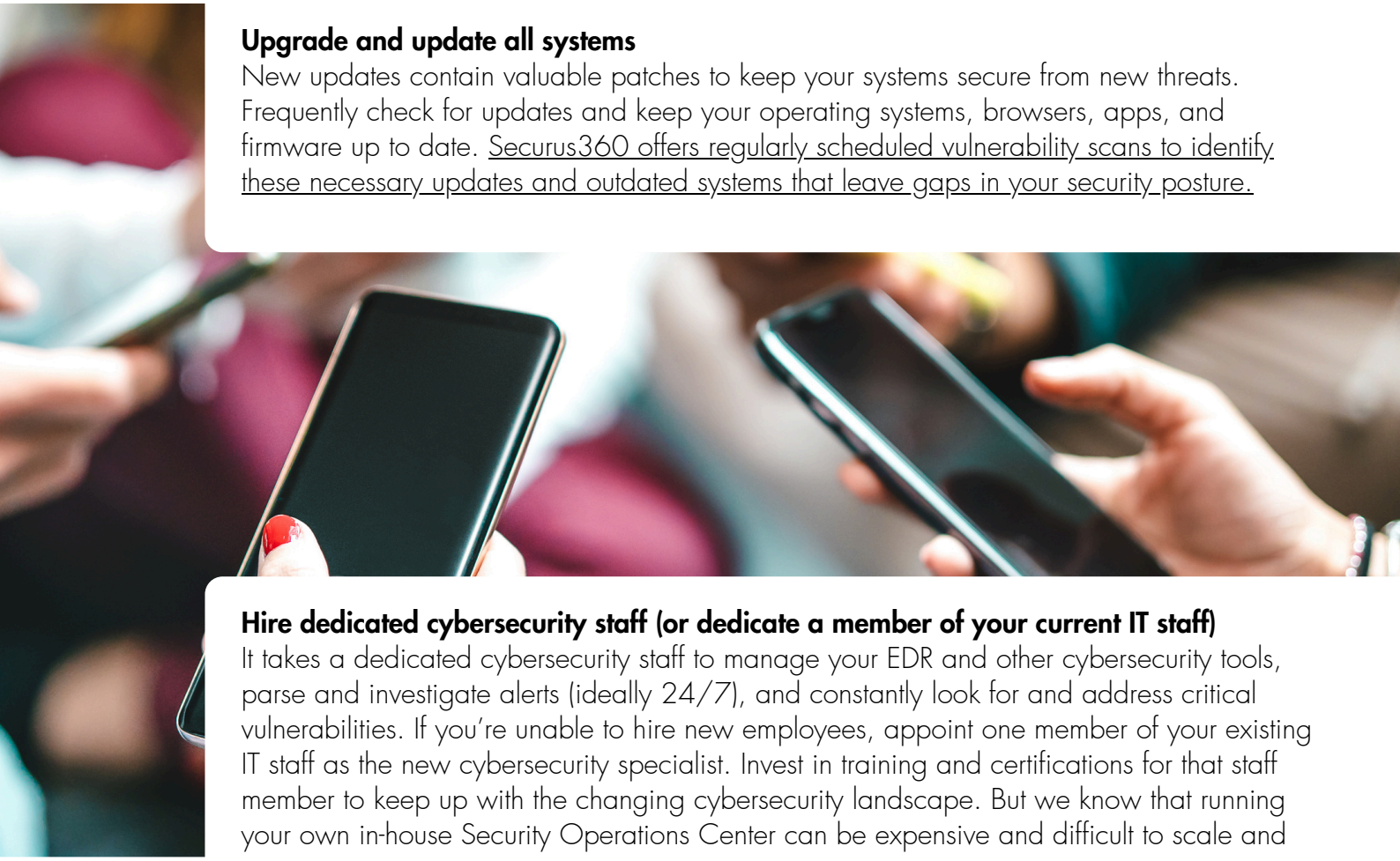
Today's Ransomware Gangs are highly sophisticated operations, and they are more commercialized than ever. Ransomware-as-a-Service (RaaS) Groups operate like legitimate businesses, posting job ads and working out of offices in commercial real estate. They have full teams of employees, including Marketing, Development, Recruiting, and even a "Victim Support" team, which handles the negotiations.

Ransomware-as-a-Service Groups can attack a large number of victims by working with affiliates, basically independent RaaS contractors. Some RaaS Groups have 100+ affiliates that each pay a license fee of around 30% of their ransom revenue to use the platform, software, and the name brand. You've probably heard of some of these Ransomware brands: LockBit, Medusa, Vice Society, and AvosLocker.

By using affiliates, a RaaS Group can now hit a lot more targets than before. They no longer have to concentrate on victims that will guarantee a large payout. They can now go for quantity over quality and play the numbers game, hitting as many targets as possible. The most vulnerable targets are the ones that end up getting breached.

BONUS Actionable Tip 4: Improve Cybersecurity Protection

For those who have completed the first three steps, there are some advanced actions you can take today to improve your cybersecurity protection against a ransomware attack.



Upgrade and update all systems
New updates contain valuable patches to keep your systems secure from new threats. Frequently check for updates and keep your operating systems, browsers, apps, and firmware up to date. Securus360 offers regularly scheduled vulnerability scans to identify these necessary updates and outdated systems that leave gaps in your security posture.

Hire dedicated cybersecurity staff (or dedicate a member of your current IT staff)
It takes a dedicated cybersecurity staff to manage your EDR and other cybersecurity tools, parse and investigate alerts (ideally 24/7), and constantly look for and address critical vulnerabilities. If you're unable to hire new employees, appoint one member of your existing IT staff as the new cybersecurity specialist. Invest in training and certifications for that staff member to keep up with the changing cybersecurity landscape. But we know that running your own in-house Security Operations Center can be expensive and difficult to scale and maintain.

Partner with an MXDR provider like Securus360
A Managed eXtended Detection and Response (MXDR) solution provides fully managed services for monitoring, detecting, and responding to even the most advanced threats. It provides visibility and protection across your entire network, including endpoints, servers, cloud, SaaS applications, and user behavior. A true MXDR platform uses multi-vector monitoring to secure your entire school district. With AI-powered monitoring and threat hunting, you can sleep soundly knowing you have maximum protection. SOC analysts will investigate and verify threats 24/7, and contain attacks before they can do damage.

Conclusion

Ransomware-as-a-Service has changed the face of cybersecurity. School Districts can no longer fly under the radar because they are smaller or not located in big cities. The new RaaS Groups are now hitting as many targets as possible, and those without a solid cybersecurity defense are at the highest risk of being breached.

K-12 school districts must upgrade their security practices to keep the sensitive data of their students and staff secure. There are many steps you can take on your own, but partnering with an MXDR provider will ensure your network and your students stay safe.

For more information about the evolution of Ransomware-as-a-Service and how to keep your school district secure, we have provided this informational webinar – https://www.youtube.com/watch?v=EVE7j-aWAB8

24/7 Protection: A Phone Call Away

We understand how much pressure you're under to defend your school district against constantly evolving threats. Bad actors never sleep. But fortunately – neither do we (and neither does our AI).

With **Securus360**, you'll be confident your network is protected, and your IT team and school district leaders will have peace of mind, thanks to our:

- **Products and services optimized for school districts:** We're singularly focused on cybersecurity for K-12 schools, so we know the specific threats targeting your school 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 receive hands-on 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.

Book A Demo

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.