

the NetWork LeadingIT

Chicagoland Cybersecurity Support

September 2024



Understanding the Importance of Cyber Security Within Education

How Can AI Be Used as Your Next Line of Defense?

Out With the Old: Managing the Shift Away from Legacy Systems

Risks of Ignoring Hardware-Based Security for Your Business

LeadingIT Named to Inc 5000 List



GoLeadingIT.com



815-788-6041



@goleadingit



Understanding the Importance of Cyber Security Within Education

Imagine the following: you're a public school student. Every day you wake up, take the bus to school, go to classes, eat lunch in the cafeteria, attend an after-school club, and get picked up by one of your parents to head home. Sometimes, if your parents are sick, a different family member or a close family friend will get you.

Now, think about the information your school needs for you to carry out this typical day. Registering for classes means your school needs a copy of your medical records and birth certificate. You take the bus each morning, so they also have information regarding where you live. Since you buy lunch at school, some kind of financial information is attached to your name. Finally, the school knows who your parents are and who your secondary/emergency contacts are.

This only skims the surface of the information educational institutions need from students and their families. Therefore, it is reasonable to expect that tight systems are in place to keep it safe, especially from cybercriminals who can exploit some of the most vulnerable members of any given population.

The Vulnerability of Student Data in Schools

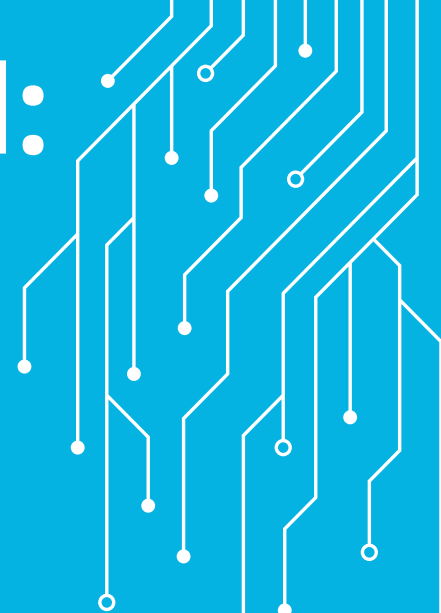
It will come as a shock to some, then, that there's a rising trend of hackers targeting the data of public schools.

When schools are locked out of their systems by cybercriminals, they lose access to bus route maps and schedules, what medications some students take during the day, and payroll systems for paying educators and administrators. As a result, schools

Continue reading on page 7

Pictured on the cover: (Left to Right) Stephen, Mark, Denise, Laura, Kyle, Jeremiah, Molly, Daniel, Mark and Heather.

Out With the Old: Managing the Shift Away from Legacy Systems



Change is scary. But when it comes to securing the longevity of your business's cybersecurity and general tech functions, it's necessary. This is especially the case if your company is running on legacy systems: software and hardware that is outdated but still in use.

Using legacy systems is risky business. Servers are put in a particularly vulnerable position to be hacked by cybercriminals when they operate on outdated tech. Healthcare institutions, for example, have seen increased rates of cyberattacks over the past few years, with one major cause being the use of software only compatible with older hardware models.

You may be considering moving away from legacy systems in you SMB. Fortunately, shifting away from outdated tech is easy when you understand the associated risks and how easy the transfer can really be.

Why Continue to Use a Legacy System?

Transferring data from an outdated drive to a modern server is a lengthy process that some businesses cannot afford to go through, especially if it disrupts regular operations. The learning curve of adapting to a modern system may also dissuade decision-makers from moving away from legacy systems, as that's an additional time cost they may not be willing to invest in.

Legacy systems can be outdated while remaining functional, and some want to stick with that familiarity. Decision makers may opt to stick with what's proven to work for them, despite the associated risk.

What Are the Risks of Using a Legacy System?

When Windows, Mac, and Linux roll out new versions of their operating systems, they begin phasing out support for previous versions until it reaches its "end-of-life". This means that, over time, users will be unable to install new updates unless they upgrade to the newest version. In some instances, investing in new hardware is necessary to do this.

Installing updates is one of the easiest things someone can do to keep their tech safe from malicious invaders. Updates come with patches that fix security flaws from previous versions, remedy annoying bugs, and keep things running smoothly and speedy.



Risks of Ignoring Hardware-Based Security for Your Business

By now, it's obvious that cyberattacks are becoming more complex, sophisticated, and dangerous for businesses across the globe. From Indian hackers targeting Canada's military to Chinese cyber-criminals targeting companies via altered hardware, cyber-attacks are costing entire economies millions of dollars. Unfortunately, despite the growing realization that cyberattacks are becoming more prominent, the World Economic Forum's 2020 Global Risk Report found that the rate of detection remains as low as 0.05%.

The truth is that, if you're solely using software-based IT solutions, you could be opening your company to a multitude of risks. Hardware-based security is an equally essential component for proactive protection and defense at every layer of your computing stack.

What is Hardware-Based Security?

Malicious actors are now targeting components and functionalities within systems that lie beneath the protective scope of software. Unlike software security, which protects software from being compromised, hardware-based security protects physical machines and peripheral hardware from attacks.

However, hardware-based security is not a replacement for software IT solutions. It should be used to enhance your overall security posture.

Hardware-Based Security Protects Against Physical Attacks

As stated above, one of the primary risks of ignoring hardware security is leaving your business vulnerable to physical attacks on your devices. When hardware security measures are absent, attackers can gain access to hardware components (e.g., hard drives, storage devices, etc.), steal data, or implant malicious software, all while bypassing existing software security.

Ensuring Data Integrity

Ignoring hardware security puts your data integrity at risk. Malware and software attacks can compromise your data, making it susceptible to unauthorized modification or theft. Hardware security, on the other hand, ensures the authenticity and integrity of your data through features like secure storage and hardware-backed authentication.

Strengthening User Authentication

Weak user authentication mechanisms are a common point of vulnerability in many businesses. Without hardware-based security, usernames and passwords may be susceptible to hacking. Incorporating hardware security features, such as biometric authentication or smart cards, provides an additional layer of protection and helps safeguard sensitive data and user identities.

Best Practices for Using Hardware-Based Security


1. Choose hardware with built-in security: Invest in devices equipped with hardware security features like TPM chips or hardware encryption capabilities.
2. Regularly update and patch: Keep your hardware security features up to date to address potential vulnerabilities.
3. Train employees: Educate your employees about the importance of hardware security and enforce best practices for device usage and data protection.

In a world where cyber threats are constantly evolving, ignoring hardware-based security can be a costly mistake for your business. Protecting against physical attacks, ensuring data integrity, and strengthening user authentication are just some of the critical reasons to invest in hardware security.

LeadingIT Named to Inc 5000 List



Inc. revealed in August that LeadingIT ranks No. 2546 on the 2024 Inc. 5000, its annual list of the fastest-growing private companies in America. The prestigious ranking provides a data-driven look at the most successful companies within the economy's most dynamic segment—its independent, entrepreneurial businesses. This is the 3rd time LeadingIT has been awarded a place on the prestigious list.



How Can AI Be Used as Your Next Line of Defense?

Artificial intelligence (AI) is going through a tech renaissance. From college students using ChatGPT for assistance on their assignments; to social media platforms using AI tools to analyze the effectiveness of ad campaigns, it seems like everyone is using this rapidly evolving resource for both the mundane and the extraordinary.

Perhaps you want to invest in a slice of the AI pie to bolster your SMB's cyber security monitoring. Before making any decisions, it's good to familiarize yourself with how businesses are already using AI, common concerns with AI to keep in mind, and what to consider when making your final decision.

How Can Businesses Use AI?

What is most confusing about AI is how it's an umbrella term that encompasses so many different tools and resources. It can refer to several things: from a robot that can hold a conversation, to a code capable of playing a game of chess, or even machine learning, which enables a computer to accurately carry out a task by learning from collected data and algorithms.

Machine learning is commonly used to bolster a business's cybersecurity. It can flag suspicious emails, detect the attempts of hackers trying to break through system weak points and evaluate huge amounts of company data to detect risky digital behavior.

AI can also be used to help with customer service. Implementing an AI chatbot on a company's website can be a useful tool for customers with a specific question or special accommodation needs. Even inventory management becomes easier with the help of AI, as it optimizes the time and resources needed to keep track of supply and demand.

Concerns Surrounding AI

As is the case with anything new and shiny, there is going to be some hesitancy from some parties to begin using it. Many concerns surrounding AI revolve around a lack of proper regulation. The regulation of AI takes on many different looks. It

may be a government body instating laws that limit potentially harmful uses of AI. For your business, it may be a member of your IT team monitoring AI cybersecurity tools to ensure they don't go rogue.

As innovative as AI enhancements are, a human's intentions with them could be innocent or malicious. Cybersecurity systems use AI to strengthen protective procedures, but hackers and other cybercriminals can also use it to break through these barriers more efficiently and with more damage.

Blackmailers also use deepfakes—AI-generated images and videos created through a machine learning tool known as deep learning—to create false and scathing interpretations of people. There are details to look out for when determining whether something is AI generated or not, such as an overabundance of teeth in a subject's smile or a suspiciously blurry background. AI can also be used to detect AI; Microsoft developed a tool to detect computer-generated inconsistencies deepfakes are often guilty of.

What to Consider Before Investing in AI

One thing about AI that decision-makers should keep in mind is that it is a tool, not a replacement. Remember what we said about regulation: AI tools are powerful, but so is the human touch, which can intervene if AI begins behaving in an unideal manner. Many concerns surrounding AI are mitigated with human intervention and intelligence.

When considering how to implement AI into your business, do not think of it as something that can cut costs on labor. Regard it as a tool that enhances productivity, giving employees resources for completing both small tasks and large projects.

AI serves cybersecurity as both a helpful ally and a new threat to servers holding private data globally. Consider discussing with your IT provider to understand how AI can help your business grow, assist them in protecting you, and what steps you can take to educate your business's team on detecting rogue or malicious AI behaviors.

■ *Out With the Old* continued from pg 3...

Additionally, cybersecurity tools used by IT support teams require businesses to keep up to date with tech that adheres to modern standards. If your cybersecurity team is unable to integrate 2FA, monitoring, or even a ticketing system, then your business is even more at risk of falling victim to a cyberattack.

How to Go About Transferring to a Modern System?

Before making any decisions around modernizing your systems, meet with your IT provider. They can consult you on the best course of action for your business.

In case anything goes wrong during the migration, you will want to ensure you have a backup of all your company's data. Ensuring the new systems you integrate will support the tools your business operates

with is also an essential step to take before updating. Consider doing gradual integration. Rather than upgrading all tech at once, only upgrade what needs immediate remediation, slowly ticking off the list of legacy systems that need to be replaced. This helps you avoid downtime due to updates in the office, gives your staff time to learn the new software, and allows your IT team to ensure all data properly transfers to the new system.

Updating your business's tech is daunting, yet possible. Having reliable IT support helps the process go smoothly. Finding a provider that will work with you and not try to push unnecessary upgrades on you, as well as one that will help your team adapt to new technology, will ease the pains that come with managing the shift away from legacy systems.

■ *Understanding the Importance of Cyber Security Within Education*

continued from pg 2...

are shut down for days as they scramble to regain control of their data.

But this is only the immediate damage. If hackers put a ransom on the data, then the information of students and their families can be sold on the dark web. Criminals may then buy the information of a child to commit identity theft, destroying their credit scores before they even have a credit card of their own.

The Role of Technology and Lack of Cybersecurity Resources

Why are these attacks on the rise? Students and staff alike are more attached to technology than ever. Big tech companies (think Google, Apple, Microsoft, etc.) invest millions of dollars into products targeted for school use, often providing schools with grants or giving it to them for free.

It's easy for students and staff alike to accidentally allow malware to breach these devices, especially if they lack the proper training on how to detect it. Suspicious links, phishing attempts, and poor password choice can victimize anyone, regardless of age or experience.

The risk remains present when personal devices are used for school-related purposes as well. Any device connected to the school's network—whether it be

managed by the district or holds log-in information for an associated account—is at risk of falling victim to ransomware attacks.

Then there's the age-old dilemma of staffing. Forbes reports that 66% of K-12 school districts do not have full-time cyber security resources or staff. Little to no cyber security support means no cyber security awareness training (for staff OR students) and no line of defense against hackers. As a result, districts end up losing an exorbitant amount of money on hiring a third-party IT support team to try and help them recover when a cyber attack does impact their schools.

The Importance of Proactive Cybersecurity Measures

While providing students with devices that promote the progression of their academic achievements is important, ensuring those devices won't victimize them in a data leak is even more important. Providing ample cyber security support to school districts is not only wise financial due to the proactive protection it provides, but also a matter of student, staff, and family safety. Cyber security in schools can educate students and staff on the actions they can take to keep themselves safe, protecting them from malicious intruders stalking the network.

LeadingIT Core Values Victor of the Month

Jeremiah Bird - Level 2 Technician



We are proud to celebrate Jeremiah as this month's Values Victor for embodying our core value of being Driven. At LeadingIT, being driven means committing to success in every facet of work and life, and understanding that hard work is the key to growth.

Jeremiah exemplifies this spirit through his relentless dedication and tireless effort, inspiring personal and collective growth. Congratulations, Jeremiah, for driving us forward and proving that our hard work truly makes a difference!

LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Have A Positive/Fun Mindset

*Continue reading on our blog
at goleadingit.com/blog*



Serving the Chicagoland area with
offices in Woodstock, Downtown Chicago,
and now in Manteno, IL.



\$1000

REFERRAL PROGRAM

WE LOVE REFERRALS!

Do you know an organization that needs fast + friendly IT and cybersecurity support?

If they sign up, you'll receive \$1000!

LEARN MORE



[GOLEADINGIT.COM/REFER](https://goleadingit.com/refer)

815-788-6041



WE ARE CELEBRATING!

Birthdays

Geovel Operana

September 9th

Matthew McMullan

September 24th

Anniversaries

Geovel Operana

9/1/2022