The K-12 Cybersecurity Crisis

New And Critical Protections Every K-12 School Must Have in Place NOW to Protect Their Students Data & Privacy

Notice: This publication is intended to provide accurate and authoritative information in regard to the subject matter covered. However, no warranties are made. It is provided with the understanding that the author and the publisher are NOT engaged in rendering legal, accounting or related professional services or advice and that this publication contains opinions of its author. This publication is NOT intended as a substitute for specific legal or accounting advice for any particular institution or individual. The publisher accepts NO responsibility or liability for any individual's decisions or actions made as a result of information or opinion contained herein.

The growth and sophistication of cybercriminals, ransomware and hacker attacks has reached epic levels. School leaders can no longer ignore it or foolishly think, "That won't happen to us."

Your school– large OR small – will be targeted and will be compromised UNLESS you take action on the information revealed in this important new executive report.

Provided By: IKON BUSINESS GROUP
Author: KEN NERO, CEO
ken@ikonbusinessgroup.com
(212) 334-6481
www.ikonbusinessgroup.com

About The IKON Business Group

IKON Business Group (IBG) is a 20-year-old premium IT consulting company focused on providing K-12 schools with customized technology solutions and personalized support. Through our charitable organization, IKON Cares, we are committed to providing students in disadvantaged neighborhoods with early exposure and access to technology.

IKON is pleased to announce the creation of the IKON EduTech Group

As an IT provider for K-12 schools, we recognize that K-12 schools have unique technology needs. Schools need to determine the best software to work with their curriculum stack and how to train staff to take advantage of all the tools available to educate students in the most efficient manner. In addition, hardware has to be integrated to allow for a seamless experience.

The IKON EduTech team will help you find and support solutions in the following areas:

- Instructional technology
- Administrative systems
- Student data and systems
- Classroom design and AV
- School safety
- Professional development training
- School technology planning and budgeting

The IKON EduTech team aims to improve student outcomes, enhance individualized education, and reduce the teaching burden. We have specialized staff that can work with your school to support and implement the best solution for your organization.

When Your School Falls Victim to a Cyber-Attack By No Fault of Your Own, Will They Call You Incompetent… or Just Irresponsible?

It's EXTREMELY unfair, isn't it? Victims of all other crimes – burglary, mugging, carjacking, theft – get sympathy from others. They are called "victims" and support comes flooding in, as it should.

But if your school is the victim of a cybercrime attack where sensitive student information is compromised, you will NOT get such sympathy. You will be instantly labeled as "incompetent" or "irresponsible." **You may be investigated and families and community members will question you about what you did to prevent this from happening** – and if the answer is not adequate, you can be found liable, facing serious fines and lawsuits EVEN IF you trusted an outsourced IT support company to protect you. Claiming ignorance is not an acceptable defense, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders.

But it doesn't end there…

According to New York State Education Law 2-D, failure to comply with Education Law 2-D can lead to several consequences for schools. Here are some of the potential repercussions:

1. **Legal Penalties**: Schools that fail to comply with Education Law 2-D may face legal consequences, including fines and penalties. These penalties can vary depending on the severity of the violation and can result in financial burdens for the institution.
2. **Loss of Trust and Reputation**: Non-compliance with student data privacy regulations can lead to a loss of trust among students, parents, and the community. This can damage the school's reputation and affect its ability to attract students and maintain positive relationships with stakeholders.
3. **Data Breaches and Security Risks**: Non-compliance increases the risk of data breaches and unauthorized access to student data. This can expose sensitive information, such as personally identifiable information (PII), leading to potential harm to students and legal liabilities for the school.
4. **Negative Publicity and Media Attention**: Instances of non-compliance with student data privacy regulations can attract negative publicity and media attention. This negative coverage can further damage the school's reputation and erode public trust.
5. **Loss of Funding or Grants**: Non-compliant schools may face repercussions when it comes to funding or grant opportunities. Funding agencies and organizations often prioritize institutions that demonstrate a commitment to data privacy and compliance.
6. **Investigations and Audits**: Schools that fail to comply with Education Law 2-D may be subject to investigations and audits by regulatory bodies. These investigations can be time-consuming, costly, and disruptive to the school's normal operations.

It is crucial for schools to prioritize compliance with Education Law 2-D to avoid these potential consequences and protect the privacy and security of student data. Implementing robust data privacy practices and staying informed about the requirements of the law can help schools mitigate risks and ensure a safe and trustworthy educational environment.

<u>Please do NOT underestimate</u> the importance and likelihood of these threats. It is NOT safe to assume your IT company (or internal staff) is doing everything they should be doing to protect you; in fact, there is a high probability they are NOT, which we can demonstrate with your permission.

But first, please allow me to introduce myself and give you a little background on why I created this report.

Why We Are So PASSIONATE About Informing and Protecting <u>YOU</u>

My name is Ken Nero, CEO of IKON Business Group. We specialize in being the outsourced IT department for K-12 school of all sizes.

Over the last few years, my team and I have seen a significant increase in calls from school leaders desperate for help after a ransomware attack, data breach event or other cybercrime incident.

When they call, they're <u>desperate</u>, scrambling for anyone who can help them put the pieces back together again. Often their school technology infrastructure is completely on lockdown. ALL their data has been corrupted or held for ransom, preventing them from fulfilling obligations they have to their clients. **YEARS of work and critical data – *all gone*.**

They're also scared and *intensely* angry. They feel violated and helpless. Embarrassed. How can information be taken from them WITHOUT their permission or knowledge? Why didn't their IT company or IT team prevent this from happening? *How are they going to tell their students and families that they've exposed them to cybercriminals*? They're in complete disbelief that they actually fell victim – after all, they "didn't think we had anything a cybercriminal would want!"

What makes this <u>unforgivable</u> is that ALL of the schools coming to us for help after a serious attack had an IT company they trusted with the responsibility of protecting them but realized all too late the company wasn't doing the job it was PAID to do.

To make matters worse, so many so-called "IT experts" out there aren't doing the job they were hired to do – and that truly angers me. As a school leader, you're FORCED to trust that your IT company or team is doing the right things to protect your organization – and when they fail to do their job, this expensive, devastating, education-disrupting disaster lands squarely on YOUR desk to deal with.

That's why we've started a "one-company revolution" to educate and help as MANY k-12 schools as we can so they never have to deal with the stress, anxiety and loss caused by a cyber-attack, and help you understand just how serious this is so you can be brilliantly prepared instead of caught completely off guard.

Yes, It CAN Happen To YOU
And The Damages Are VERY Real

You might already know about the escalating threats, from ransomware to hackers, but it's very possible you are underestimating the risk to you. It's also possible you're NOT fully protected and are operating under a false sense of security, ill-advised and underserved by your IT team.

In fact, if your current IT teamhas not talked to you about the protections outlined in this report, or about putting a cyber "disaster recovery" plan in place, you are at risk and you are not being advised properly.

This is not a topic to be casual about. Should a breach occur, your school's reputation, your student and staff information, and your neck will be on the line, which is why you must get involved and make sure your school is prepared and adequately protected, not just pass this off to someone else.

QUESTION: When was the last time your current IT company had THIS conversation with you? What HAVE they told you about these new threats? If they have been silent, then I would urge you to read this report in full and act on the information urgently.

"Not Me… Not My People… We're Just a School,"

You Say?

Don't think you're in danger because you're "just a school" and not a big company like Experian, J.P. Morgan or Target? That you have "good" people and protections in place? That it won't happen to you?

That's EXACTLY what cybercriminals are counting on you to believe. It makes you easy prey because you put ZERO protections in place, or grossly inadequate ones.

Right now, there are over 980 million malware programs out there and growing (source: AV-Test Institute). Eighty percent of school IT professionals reported that their schools were hit by ransomware in the last year, according to a global survey conducted by cybersecurity company Sophos. That's up from 56 percent from the 2022 survey; you just don't hear about it because the news wants to report on BIG breaches OR it's kept quiet by the school for fear of attracting bad PR, lawsuits and data-breach fines, and out of sheer embarrassment.

Is your school "too insignificant" to be significantly damaged by a ransomware attack that locks all of your files for several days or more?

Are you "too insignificant" to deal with a hacker using your school's server as **ground zero** to infect all of your student, vendors, employees and contacts with malware? According to Osterman Research, the AVERAGE ransomware demand is now $84,000 (source: MSSP Alert). It's also estimated that schools lost over $100,000 per ransomware incident and over 25 hours of downtime. Think about how much $100,000 could mean to your school's annual budget. It may not be the end of the world, but are you okay to shrug this off? To take the chance?

How Bad Can It Be?
My Insurance Will Cover Me, Won't It?

Insurance companies are in the business to make money NOT pay out policy claims.

A few years ago, cyber insurance carriers were keeping 70% of premiums as profit and only paying out 30% in claims. Fast forward to today and those figures are turned upside-down, causing carriers to make drastic changes in how cyber liability insurance is acquired and coverages paid.

For starters, getting even get a basic cyber liability or crime policy today may require you to prove you have certain security measures in place, such as multi-factor authentication, password management, endpoint protection and tested and proved data backup solutions.

Insurance carriers want to see phishing training and cyber security awareness training in place, and some will want to see a WISP and/or a Business Continuity Plan from your organization. Depending on the carrier, your specific situation and the coverage you're seeking, the list can be longer.

But the biggest area of RISK that is likely being overlooked in your school is the actual enforcement of critical security protocols required for insurance coverage and compliance with data protection laws. Insurance carriers can (and will) deny payment of your claim if you failed to actually implement the security measures required to secure coverage. When a breach happens, they will investigate how it happened and whether or not you were negligent before paying out.

You cannot say, "I thought my IT team was doing this!" as a defense. Your IT company will argue they were not involved in the procurement of the policy and did not warranty your security (none will; check out your contract with them). They might show evidence of you refusing to purchase advanced security services from them to further distance them from any responsibility. And if you haven't been documenting the steps you've taken to secure your network and prove that you were not “willfully negligent,” **this gigantic expensive nightmare will land squarely on your shoulders to pay**.

It’s NOT Just Cybercriminals Who Are The Problem

Most school leaders erroneously think cybercrime is limited to hackers based in China or Russia, but the evidence is overwhelming that disgruntled and/or careless employees, both of your school and your vendors, can cause significant losses due to their knowledge of your organization and access to your data and systems. What damage can they do?

- **They leave with YOUR school’s files, student data and confidential information stored on personal devices**, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example), that your IT department doesn’t know about or forgets to change the password to.

- **They accidentally (or intentionally) DELETE everything.** If you don’t have that data backed up, you lose it ALL. Imagine all of the time wasted on recovering the data, not to mention the aggravation and distraction of dealing with it all.

You May Want to Believe You're "Safe"
But Are You Sure?

It's very possible that you are being ill-advised by your current IT company. What have they recently told you about the rising tsunami of cybercrime? Have they recently met with you to discuss new protocols, new protections and new systems you need in place TODAY to stop the NEW threats that have developed over the last few months?

If not, there could be several reasons for this. First, and most common, they might not know HOW to advise you, or even that they should. Many IT companies know how to keep a computer network running **but are completely out of their league when it comes to dealing with the advanced cybersecurity threats we are seeing recently**.

Second, they may be "too busy" themselves to truly be proactive with your account – or maybe they don't want to admit the service package they sold you has become OUTDATED and inadequate compared to far superior solutions available today. At industry events, I'm shocked to hear other IT companies say, "We don't want to incur that expense," when talking about new and critical cybersecurity tools available. Their cheapness CAN be your demise.

And finally, NOBODY (particularly IT folks) likes to admit they are out of their depth. They feel compelled to exaggerate their ability to avoid being fired. To be fair, they might actually have you covered and be on top of it all. So how do you know?

Is Your Current IT Team Doing Their Job?
Take This Quiz toFind Out

If your current IT company does not score a "Yes" on every point, they are NOT adequately protecting you. Don't let them "convince" you otherwise and DO NOT give them a free pass on any one of these critical points.

Further, it's important that you get verification on the items listed. Simply asking, "Do you have insurance to cover US if you make a mistake?" is good, but getting a copy of the policy or other verification is critical. When push comes to shove, they can deny they told you.

☐ **Have they met with you recently – in the last 3 months – to specifically review and discuss what they are doing NOW to protect you?** Have they told you about new and inexpensive tools such as 2FA or advanced endpoint security to protect you from attacks that antivirus is unable to detect and prevent? If you are outsourcing your IT support, they should, at a MINIMUM, provide you with a quarterly review and report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

☐ **Do they proactively monitor, patch and update your computer network's critical security settings daily? Weekly? At all? Are they reviewing your firewall's event logs for suspicious activity?** How do you know for sure? Are they providing ANY kind of verification to you or your team?

☐ **Have they EVER urged you to talk to your insurance company** to make sure you have the right kind of insurance to protect against fraud? Cyber-liability? MORE IMPORTANT: Have they reviewed your insurance policy with your agent to ensure they were implementing the cyber protections required under that policy to avoid having a claim denied, coverage not paid?

☐ **Do THEY have adequate insurance to cover YOU if they make a mistake and your network is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages?

☐ **Have you been fully and frankly briefed on what to do IF you get compromised?** Have they provided you with a response plan? If not, WHY?

☐ Have they told you if they are outsourcing your support to a 3rd-party organization? **DO YOU KNOW WHO HAS ACCESS TO YOUR PERSONAL COMPUTER AND NETWORK?** If they are outsourcing, have they shown you what security controls they have in place to ensure a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?

☐ **Have they kept their technicians trained on new cybersecurity threats and technologies, rather than just winging it?** Do they have at least ONE person on staff with CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) certification? Do they have anyone on staff experienced in conducting security risk assessments?

☐ **Do they have a ransomware-proof backup system in place?** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. ASK THEM TO VERIFY THIS. You might *think* you have it because that's what your IT vendor is telling you.

☐ **Have they put in place a WRITTEN mobile and remote device security policy, and distributed it to you and your employees?** Is the data encrypted on these devices? Do you have a remote "kill" switch that would wipe the data from a lost or stolen device, and is that data backed up so you CAN wipe the device and not lose files?

☐ **Do they have controls in place to force your employees to use strong passwords?** Do they require a monthly password update for all employees? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?

□ **Have they talked to you about replacing your old antivirus with advanced endpoint security?** There has been considerable talk in the IT industry that antivirus is dead, unable to prevent the sophisticated attacks we're seeing today.

□ **Have they discussed and/or implemented "multifactor authentication" for access to highly sensitive data?** Do you even know what that is? If not, you don't have it.

□ **Have they recommended or conducted a comprehensive risk assessment every single year?** Many insurance policies require it to cover you in the event of a breach. If you handle "sensitive data" such as medical records, credit card and financial information, social security numbers, etc., you may be required by law to do this.

□ **Have they implemented web-filtering technology to prevent your students and staff from going to infected websites, or websites you DON'T want them accessing at school?** Porn and adult content is still the #1 thing searched for online. This can potentially expose you to sexual harassment and child pornography lawsuits.

□ **Have they given you and your staff ANY kind of cybersecurity awareness training?** Have they offered to help you create an AUP (acceptable use policy)? Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the #1 way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously.

□ **Have they properly configured your e-mail system to prevent the sending/receiving of confidential or protected data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data, like social security numbers, from being sent or received.

□ **Do they allow your employees to connect remotely using GoToMyPC, LogMeIn or TeamViewer?** If they do, this is a sure sign to be concerned! Remote access should strictly be via a secure VPN (virtual private network).

□ **Do they offer, or have they at least talked to you about, dark web/deep web ID monitoring?** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once detected, it notifies you immediately so you can change your password and be on high alert.

A Preemptive Independent Risk Assessment:
The ONLY Way You Can Really Be Sure

A security assessment is exactly what it sounds like – it's a process to review, evaluate and "stress test" your school's network to uncover loopholes and vulnerabilities BEFORE a cyber-event happens.

Just like a cancer screening, a good assessment can catch problems while they're small, which means they will be a LOT less expensive to fix, less disruptive to your organization AND give you a better chance of surviving a cyber-attack.

An assessment should always be done by a qualified 3rd party, NOT your current IT team or company; fresh eyes see things hidden, even in plain sight, from those looking at it daily.

You want a qualified "Sherlock Holmes" investing on YOUR behalf who is not trying to cover up inadequacies or make excuses, bringing to you a confidential report you can use before others find dirty laundry and air it in harmful ways.

Our Free Cybersecurity Risk Assessment Will Give You the Answers You Want and the Certainty You Need

For a limited time, we are offering to give away a Free Cybersecurity Risk Assessment to a select group of K-12 schools. This is entirely free and without obligation. EVERYTHING WE FIND AND DISCUSS WILL BE STRICTLY CONFIDENTIAL.

This assessment will provide verification from a **qualified 3rd party** on whether or not your current IT team is doing everything they should to keep your computer network not only up and running, but SAFE from cybercrime.

Here's How It Works: At no cost or obligation, one of my lead consultants and I will come to your office and conduct a non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols. Your current IT team DOES NOT NEED TO KNOW we are conducting this assessment. Your time investment is minimal: one hour for the initial meeting and one hour in the second meeting to go over our Report of Findings.

When this Risk Assessment is complete, you will know:

- **If your login credentials are being sold on the dark web.** We will run a scan on your network, right in front of you, in the privacy of your office if you prefer (results will NOT be e-mailed or otherwise shared with anyone but you). It's RARE that we don't find compromised credentials – and I can guarantee what we find will shock and alarm you.

- IF your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees.

- IF your **current backup would allow you to be back up and running again fast** if ransomware locked all your files. *In 99% of the computer networks we've reviewed over the years, the owners were shocked to learn the backup they had would NOT survive a ransomware attack*.

- IF employees truly know how to spot a phishing e-mail. We will actually put them to the test. *We've never seen a company pass 100%.* Not once.

- If your IT systems, backups and website in sync with compliance requirements for HIPAA, E-Rate, NYS Ed-Law 2-D, and other mandates.

If we DO find problems…overlooked security loopholes, inadequate backups, credentials that have been compromised, out-of-date firewall and antivirus software and (often) active malware…on one or more of the PCs in your school, we will propose an Action Plan to remediate the situation that you can have us implement for you if you choose.

Again, I want to stress that EVERYTHING WE DISCUSS AND DISCOVER WILL BE STRICTLY CONFIDENTIAL.

Why Free?

Frankly, we want the opportunity to be your IT company. We know we are the most competent, responsive and trusted IT services provider to K-12 Schools.

However, I also realize **there's a good chance you've been burned, disappointed and frustrated by the complete lack of service and the questionable advice** you've gotten from other IT companies in the past. In fact, you might be so fed up and disgusted with being "sold" and underserved that you don't trust anyone. *I don't blame you*.

That's why this assessment is completely and entirely free. Let us earn your trust by demonstrating our expertise. While we would love the opportunity to be your IT company, we will come in with no expectations and only look to provide you with fact-based information so you can make a quality, informed decision – and we'll ONLY discuss the option of becoming your IT company if the information we share makes sense and you want to move forward. No hard sell. No gimmicks and no tricks.

Please…Do NOT Just Shrug This Off

(What to Do Now)

I know you are *extremely busy* and there is enormous temptation to discard this, shrug it off, worry about it "later" or dismiss it altogether. That is, undoubtedly, the easy choice…but the easy choice is rarely the RIGHT choice. **This I can guarantee:** At some point, you WILL HAVE TO DEAL WITH A CYBERSECURITY EVENT.

Hopefully you'll be brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do NOTHING, I can practically guarantee this will be a far more costly, disruptive and devastating attack that will happen to your school.

You’ve spent a lifetime working hard to get where you are today. Don’t let some lowlife thief operating outside the law get away with taking that from you. And certainly don’t “hope” your IT guy has you covered.

Get the facts and be certain you are protected.

Contact us and schedule your Free, CONFIDENTIAL Cybersecurity Risk Assessment today: https://www.ikonbusinessgroup.com/cyberreport/. Feel free to also reach out to me direct at the phone number or e-mail address below.

Dedicated to serving you,

Ken Nero
CEO, IKON Business Group
Web: www.ikonbusinessgroup.com
E-mail: ken@ikonbusinessgroup.com
Direct: (212) 334-6481

P.S. – When I talked to other IT professionals like myself and the organizations who have been hacked or compromised, almost all of them told me they thought their IT team “had things covered.”

I’m also very connected with other IT firms across the country to “talk shop” and can tell you most IT teams have never had to deal with the enormity and severity of attacks happening in the last few months. That’s why it’s VERY likely your IT team does NOT have you “covered” and you need a preemptive, independent risk assessment like the one I’m offering in this letter.

As a CEO, I understand that you have to delegate and trust, at some level, that your employees and vendors are doing the right thing – but it never hurts to validate that they are. Remember, it’s YOUR school’s information, reputation, and money that’s on the line. THEIR mistake is YOUR nightmare.

Here Are Just a Few K-12 Schools We’ve Helped:

The Bronx Better Learning Charter School Works with IKON to Navigate E-Rate Application Process and Implement Critical Technology Initiatives

"Apart from making me look good, IKON is very knowledgeable. They are a very important part of our team. I'm not sure where I'd be without them, and I really don't want to find out. IKON is like Tylenol--they offer pain relief!"

- Kevin Williams, Technology Director

The Renaissance Charter Schools Tap IKON to Provide Added Security and Peace of Mind Across Locations

"What set IKON apart from other IT providers was their commitment to onsite support. If our Internet goes down, we can't function. Other companies said they'd try to be there by the end of the day, whereas IKON guaranteed us that they'd have someone in the building within 4 hours or less."

- Dan Fanelli, Assistant Director and Assistant Principal

IKON Helps Ascend Public Charter Schools Navigate Remote Learning and Staffing Challenges with After-Hours Support

"The skillset that IKON brings and their laser-focus on K-12 schools were key differentiators. It's important for us to work with vendors who are invested in our community. Working with a managed services provider who specializes in the education space has been invaluable."

- Emeka Ibekweh, Managing Director of Technology