DYOPATH eBook

Superintendent Cybersecurity Framework

DYOPATH

Table of Contents

solutions@dyopath.com
1.866.609.PATH

DYOPATH

Superintendent Cybersecurity Crisis

The Framework to Cybersecurity for School Districts

Cybersecurity in Schools

As education-based technology evolves and school districts across the nation are implementing online learning and virtual classes, their chances of falling victim to cyberattacks are exceedingly high. Superintendents need to be aware of this matter and take the extra steps to ensure privacy of digital information to protect their school districts.

The Cybersecurity and Infrastructure Security Agency (CISA) defines cyber security as "The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

The Risks Schools are Facing

In April of 2020, the FBI warned the public that cyber attackers will be taking advantage of the recent switch to virtual learning platforms. Cyber crooks often choose to attack school districts because of their large database of Personally Identifiable Information (PII). PII included names, addresses, social security numbers, health records and employee forms.

Hundreds of school districts across the country are experiencing cyberattacks and data theft. There have been over 220 school system attacks in 2020 alone, with the most recent reports showing cases where student information is being sold to pedophiles.

How are these school districts and individuals making themselves vulnerable to cyberattacks? Ethical hacking assessment results show that 90% of people are clicking on staged emails, 80% of those are opening attachments or clicking on links, leaving 40% of those who are sending in personal data.

Without proper cybersecurity, any person associated with a school district is susceptible to a cyberattack, including parents, students, employees, emergency contacts, people on the school board, etc.

> "After a school district in Texas had to shut down on their first day of virtual learning, and postpone their start date by several weeks after a malicious cyber-attack, we know without a doubt that cyber security is more prominent than ever."
>
> - Leonard Merrell, Ed. D.

solutions@dyopath.com
1.866.609.PATH

DYOPATH

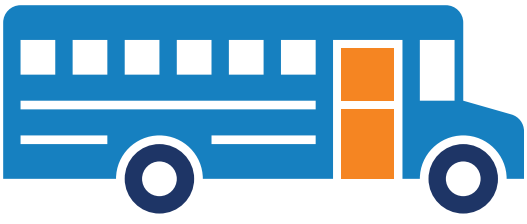
Is Your District Compliant?

Texas lawmakers recently passed House Bill 3834, requiring district employees and board members to participate in an annual cybersecurity training program, certified by the Texas Department of Information Resources. This program was developed to increase the school district's ability to protect their data and prepare for unexpected cyberattacks. The training was to be completed by June 14, 2020, just in time to be fully prepared for the start of the new school year.

Texas lawmakers have also recently passed Senate Bill 820 that requires school districts to create a cybersecurity policy, have the superintendent designate a cyber security coordinator, and report all cyberattacks or suspicious activity to not only the Texas Education Agency, but also the district families.

Illinois lawmakers have recently passed House Bill 4443, which requires local governments with a population of 35,000+ to designate someone as the primary point of contact for cybersecurity issues. This position will act as a cybersecurity liaison to assist school districts with cybersecurity and threats. Similar to the House Bill 3834 in Texas, the Illinois House Bill 4443 also requires district employees to complete cybersecurity training.

Most other state legislatures are passing similar legislation to that of Illinois and Texas to advance policy proposals addressing improving cybersecurity for school districts. As threats continue to evolve and expand and as the pace of new technologies increase, legislatures throughout the country are making cybersecurity measures a top priority.



Accountability Begins with Understanding

As a superintendent, you are accountable to your community. This involves, but surely is not limited to, understanding the cybersecurity risk that is present in your school district. To be certain that you've done your diligence, make sure that your school district can answer these top ten questions:

1. **If a cybersecurity attack were to happen today, do you have a plan in place?** You need to have a plan of action set in place to ensure the safety of your school district and community if an attack happens.

2. **Do you feel that you have reasonable measures in place to protect students and the continuum of learning in the event of an attack?** Most superintendents would agree that their first priority is the safety of their students. Their second priority would be to ensure that their students are learning. Make sure that your cybersecurity measures do not keep you from achieving those priorities.

3. **Are you regularly monitoring your data?** Motoring your data means being aware of what data is being stored where, and what data is being transmitted when. Be aware that any digital data can at any point and already may have been confiscated. It is wise to have a master list of the data being transmitted in your district on a daily basis.

4. **What is the risk level of your district to a cyberattack?** While cyberattacks can happen in any school district, you should be aware if yours has been prone to them in the past or if nearby districts are.

5. **Who has access to what information?** Keep track of who has access to specific data, records, and PII in your system. It will be easier to monitor and locate in time of a crisis.

6. **Is your district currently in compliance with federal and local legalities?** Educate yourself on any laws that may dictate how you manage this data. This is legal information that goes beyond an IT worker's duties.

solutions@dyopath.com
1.866.609.PATH

7. **Do you have a good understanding of your role in the event of a cybersecurity attack?** As a superintendent, you are in charge of making decisions and ensuring that everyone is doing their job. However, you need to be prepared for your role and responsibility if a cyberattack were to occur.

8. **Do you have a designated person to be the primary point of contact during a cybersecurity attack?** Not only is it the smart thing to do, but it is now the law to have an employee who works as a liaison for those experiencing cyberattacks and cyber threats.

9. **Do you have backup data? Where is it?** If you do not have backup of all your data, someone is not doing their job right. Backup data provides relief if data is stolen or if the attacker wants ransom money to return it.

10. **Do you have a budget of what your IT department can spend to compensate for a cyberattack?** If an attack happens, is your district financially prepared to handle it? A budget for this issue can be discussed with your board members.

Developing a Framework for Your District's Cybersecurity Program

School districts across our nation implement a variety of protocols to keep schools prepared for the potential of catastrophic events, such as active school shooter readiness programs, fire drills, and the life safety test. These protocols help to ensure the safety of their faculty and students on a daily basis, but also to be prepared when disaster strikes. Similarly, superintendents in today's time need to implement protocols to safeguard against cyberattacks, such as penetration assessments, phishing prevention, and cyber assessments.

Before an Attack

As the superintendent, you need to develop a proper security policy. It is important to keep track of who has access to what data, where and how your data is stored, and how it is transmitted. Invest in the right technology and insurance plans to prevent cyberattacks. Hiring a reputable IT Managed Service Provider like DYOPATH is key to protecting your school district.

Ensure that all of your school district employees are obeying the law and properly completing their cybersecurity training by the proper date. Make sure each employee has the correct phone number for the primary point of contact related to cyberattacks.

You need to have an incident response plan set in place before an attack happens. When your school district is in the midst of a cyberattack, it is too late to figure out who is responsible for handling the technical work, how much money can be allocated, and how to communicate this crisis. Develop your incident response plan in hopes that you do not need it, but to be over prepared if you do.

During an Attack

If you discover that your school system is under a cyberattack or threat, it is time to bring that incident plan of action to life. Start by notifying your stakeholders; these are the people that are involved with responding to the attack. If it is not too late, stop the attack and remove the source of the attacker. Do not pay a ransom for getting your data back until you understand future options. Then, secure your backup data and identify which of your assets may have been impacted.

After the Attack

After the attack, you need to collect all evidence for civil, criminal, or regulatory proceedings. This evidence is necessary for legal reasons and insurance claims. You should also consider hiring a professional public relations specialist to train you how to properly inform the public, and how to handle the reputable damage. The PR specialist will also guide you on informing those who could have had personal information compromised.

solutions@dyopath.com
1.866.609.PATH

DYOPATH

About DYOPATH

DYOPATH is a professional IT Managed Service Provider with the purpose of helping our clients fight the increasing number of cyber threats and the growth in more complex IT environments. Not only is DYOPATH committed to delivering the highest quality software, but our services provide a program that is willing to grow, evolve, and adapt to new technology. DYOPATH offers security program development, awareness training, assessments, monitoring, event management, and so much more. We work with small to large school districts to deliver thought leadership to communities through innovative turn-key educational solutions.

Contact DYOPATH Today for Your Education Services Questions

1.866.609.PATH

Texas Office:
13430 Northwest Fwy,
Suite 1000
Houston, TX, 77040

Illinois Office:
905 Parkview Blvd
Lombard, IL 60148

solutions@dyopath.com

www.DYOPATH.com
solutions@dyopath.com
1.866.609.PATH