



NEOnet

Prompt. Courteous. Knowledgeable.

Support *you* deserve.



THE VALUE OF NEONET CYBERSECURITY

Why You Need To Protect Your
Private Student Data In Ohio

TABLE OF CONTENTS

2	Introduction
2	The Three Problems Making Schools And Students More Vulnerable To Cyberattacks
2-3	Outdated Infrastructure Without Backup Strategies
4	Failure To Adopt Modern Security Standards
5	Information Scattered Across Multiple Platforms And Systems
6	The Solution
6	Comprehensive Software And Services From NEOnet
6	NEOnet Tools – Modern, Elegant And Easy-To-Use
7	Conclusion



INTRODUCTION

In the world of information technology, the only thing that's constant is change. Every year, technology evolves – and if educational institutions don't change with the times, they are at serious risk for data breaches and loss of private student data.

The world of cyber security is also getting more complex. As schools begin to use more advanced IT programs, the risk of a data breach grows – and hackers are aware of the vulnerabilities that are common in the IT infrastructures of schools.

Recently, there have been many high profile data breaches at public schools around the US. In 2016, a data breach in Concord, New Hampshire, compromised the valuable personal information of employee Social Security numbers, employee names and other data – which could lead to the filing of false income tax statements.

In early 2017, a security researcher found that the Palo Alto Unified School District in California had a data breach that would allow access to the personal information, addresses and test scores of more than 24,000 students.

Without proper security consulting, application choice, and regular updates and maintenance of IT infrastructure, the risk of a serious breach of private student and employee data can increase dramatically.

In this whitepaper, NEOnet will take a look at the three most common issues that make Ohio schools vulnerable to hacks and data breaches – and how our National Institute of Standards and Technology (NIST)-compliant software can help provide valuable cyber insurance.

The Three Problems Making Schools And Students More Vulnerable To Cyberattacks

There are a plenty of vulnerabilities present in schools that can increase their risk of serious data breaches from hackers. From poor device management to misguided vendor contracts, there are a wide variety of security issues facing Ohio schools.

However, in this section, we'll focus on the three biggest problems that face Ohio schools today – and then we'll discuss how they can be addressed by NEOnet.

Outdated Infrastructure Without Backup Strategies

Schools in Ohio often fall behind when it comes to implementing modern tools, IT support and modern infrastructure that provides increased data security and backup strategies. Often, this is not because of ignorance on the part of school administrators – but because of school budgets that seem to constantly shrink year-by-year. IT simply isn't a huge priority for many schools, who would prefer to use funds elsewhere.

However, this is a mistake for two reasons. First, outdated infrastructure is inherently more vulnerable to hackers.

An outdated server that's running an unpatched operating system may have a huge variety of security vulnerabilities **that will never be fixed if it's no longer supported**. Hackers can take advantage of this legacy software, and easily steal student data, or even infect IT systems with ransomware like WannaCry or CryptoLocker. Because of this, upgrading IT systems should be a priority for school administrators and IT staff.

Second, failing to have a modern backup strategy can make things much more difficult if there is a high-profile data breach. An example of this would be a [2015 hack of the New Jersey Swedesboro-Woolwich School District](#). This ransomware attack caused the shutdown of systems across four elementary schools – and with no comprehensive backup plan in place, they were forced to completely rebuild their computer systems.

This rebuild caused a tremendous amount of data loss, and made all computer systems unusable throughout the school district for two entire weeks – a price that was nearly as steep as the \$128,000 that the hacker was attempting to squeeze out of school administrators.

Failure To Adopt Modern Security Standards

School districts have a tremendous amount of critical data about students and employees, including (but not limited to):

- Social Security numbers
- Employee identification numbers
- Addresses
- Student ID numbers
- Banking information (for payroll)
- Transcripts and grades

All of this data can be used for malicious purposes by hackers who seek to steal the identities of students and faculty alike. But despite the fact that schools have as much critical data as a retailer or a bank, **most schools have failed to adopt modern IT security standards and best practices**, including:

- Encryption
- Firewalls
- Device management standards
- Student/Teacher IT education
- Patching and maintenance of IT infrastructure

Due to budget issues, inattention and lack of proper infrastructure, schools are falling behind in security – at the same time, hackers begin to use more advanced, powerful tools to gain access to private student information.

Information Scattered Across Multiple Platforms And Systems

Most schools do not rely on any kind of unified online platform – instead using piecemeal applications to track and save data. This means that data is scattered across a variety of different systems and infrastructures – each of which may have serious security vulnerabilities.

And because school networks are often accessed by students, administration, teachers and even third-party vendors, it's difficult to protect the information contained in these systems, and create a comprehensive IT security strategy.

This risk makes it critical for schools to stop using diverse, individual applications – and instead turn to secured, encrypted, all-in-one solutions for administrators and staff.



THE SOLUTION

Comprehensive Software And Services From NEOnet

We've discussed – at length – the causes of poor data security at schools. But what's the solution? Cyber insurance? Updated IT systems? Security consultants?

If you're in Northeast Ohio, the answer is "all of the above." NEOnet offers comprehensive IT tools for schools all over Northeast Ohio – and we're experts in school IT solutions. We work with over 117 total educational entities in Ohio, and represent a total of over 136,000 students.

NEOnet Tools – Modern, Elegant And Easy-To-Use

We offer comprehensive IT tools and applications for educational institutions, including:

- **Virtual Servers** – Let us host all your servers with our state-of-the-art datacenters, storage and hardware. Our fully functional disaster recovery site not only provides us with a secure location to store backup data, it also generates an up-to-the-hour replication of all our hosted servers. Coupled with our approach to distributed administration, schools don't lose any local control and have the peace of mind that their data is backed up and readily available for a quick restore should any disasters strike.
- **Offsite Backups** – If you already have a significant investment in onsite storage and servers, let our offsite backup service store your data. This hosted and managed solution takes the burden off of school districts to provide backup software and offsite data protection. Our daily reports let you know the status of your backup jobs so you know your district's data is protected.
- **End-User Awareness Training** – New to the NEOnet service offering is the latest toolset in training and identifying high-risk end-users. NEOnet has teamed up with the Management Council of the Ohio Education Computer Network and KnowB4 to provide modern tools to not only train end users on internet safety, but also test the retention of that training against simulated attacks. The results of the testing will give schools the opportunity to focus on key individuals in an effort build a more resilient and secure organization.

With these tools, it's easier than ever for students, staff, and parents to access the data they need. Best of all, the powerful security precautions and modern technology used in these tools reduces your risk of a data breach.

Don't risk your school's network. NEOnet has the expertise, tools and experience required to secure your school – and protect valuable private student information.



CONCLUSION

In the modern world, cybersecurity cannot be overlooked anywhere – and this includes public and private schools in Ohio. Your IT infrastructure contains a huge amount of personal and private information that can be seriously damaging if it's released to the public – so it's critical that you have strong cyber security and cyber insurance to protect yourself in the case of an attack.

However, many schools lack this protection, and put themselves at risk. The best way to protect your school in Ohio is with the comprehensive IT consulting and the secure, all-in-one tools provided by NEOnet.

With over a hundred schools and educational institutions already using our services, we have a proven track record of success. We can help you protect valuable student information, streamline your administration's IT processes and update your outdated IT infrastructure, ensuring that your data is secure from malicious hackers.

So, don't wait. [Contact NEOnet today](#) to learn more about our services, products and background – and see why we're the number one choice for schools in Ohio.

Questions? Contact Executive Director Matt Gdovin at gdovin@NEOnet.org or call 330-926-3900, ext. 601100

