THE VALUE OF NEONET CYBERSECURITY

What You Can Do To Protect Yourself from Cyber-Attacks

NEOnet
Prompt. Courteous. Knowledgeable.
Support *you* deserve.

TABLE OF CONTENTS

"Skilled hackers do not discriminate, and every organization needs to recognize the massive threat that they present."

INTRODUCTION

In the realm of information technology, the only thing that is constant is change. Every year, technology shifts and evolves – and if businesses and educational institutions don't adjust to these changes, they will be at serious risk for data breaches and loss of private, personal data.

Just as the world of technology grows more complex, so does the complexity of cyber security. As organizations begin to implement more advanced information technology programs, the risk for data breaches grows – and hackers are aware of the many vulnerabilities that are common in the IT infrastructure of schools.

Cybercriminals continue to make headlines and show no sign of stopping. They target not just individual servers, but the servers of hospitals, academic institutions, blue-chip companies and so on.

In early 2017, Russian hackers used a phishing scam to gain access to sensitive data from the Morton School District in Tazewell County, Illinois. The hackers sent an email claiming to be from the district's superintendent, requesting information for W2 forms and receiving the social security numbers of over 400 employees. Because the district acted quickly, the hackers were unable to retrieve birth dates or addresses, limiting what they could do with the information.

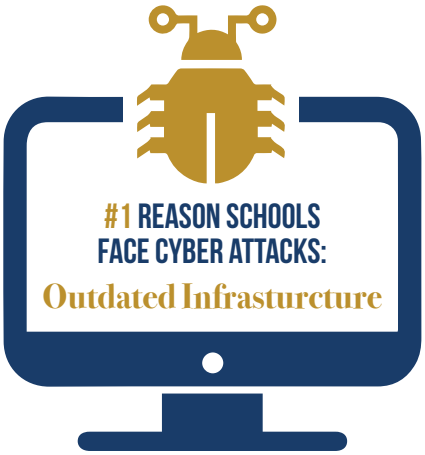
The fact that Russian hackers successfully stole social security numbers from an Illinois school district is unsettling, prompting concerns for other at-risk schools. Without proper security consulting, application choice and regular updates and maintenance of IT infrastructure, the risk of a serious breach of private student and employee data can increase dramatically for schools.

HOW DISTRICTS MAY BE PUTTING THEMSELVES AT RISK FOR CYBER-ATTACKS

Many school districts face a variety of vulnerabilities that directly attract hackers – and schools can put themselves at serious risk without even knowing it. In general, IT is not a huge priority for many schools that prefer to apply funding to other projects. Plus, school networks are shared amongst a variety of users, including students, administration, teachers and even third-party vendors. Not all users recognize that their data is susceptible to breaches – especially when they trust the school's IT capabilities.

If schools are not properly backing up their data nor keeping current on antivirus (AV) and operating system (OS) patches, hackers can invade without much difficulty. Running old OS's that are no longer supported can present an easy opportunity for data breaches. Also, schools should make sure that certain privileges are not being elevated to standard users.

If any of these areas are not being properly managed, cyber-attacks will more easily ensue, as private data will be overly, and unsafely, available. Outdated infrastructure is ultimately the number one reason that schools are attacked.



WHAT CAN DISTRICTS DO TO PROTECT THEMSELVES?

Having identified the core risk factors for a data breach, school districts can implement strategies to better protect themselves. To increase protection immediately, school districts can be better prepared for data breaches by taking the following actions:

- Choose a person and/or identify a team of individuals who will respond to attacks.
- Correct the most vulnerable IT features that attract hackers.
- Know where the most important assets are and who has access to the school's most sensitive data.
- Know what devices contain sensitive data (personally identifiable information).
- Obtain cyber liability insurance to minimize risk.

RESPONSE CHECKLIST

1. Pinpoint affected users/systems
2. If necessary, alert victims
3. Contact liability insurance

HOW SHOULD DISTRICTS RESPOND TO AN ATTACK?

The Morton School District is a great model for how schools should respond to system breaches. As soon as an attack occurs, schools need to first pinpoint the affected users and systems. Once the victims are identified, the school can then determine what potential data has been lost or exposed. If there has been data exposure that affects end users, the users must be notified.

After taking into consideration the consequences of the breach, schools should contact a liability insurance company to report the incident. By contacting an authority, a school can stop the hackers from gaining more traction – as shown in the case of Morton School District. From there, the path to mitigation, which will depend on the attack suffered, can be outlined – resulting in data restoration or end user notification and credit monitoring.

WHEN FACING A BREACH, NEONET IS HERE TO HELP

NEOnet can reduce the risk of hacking to a minimum by offering valuable cyber-security support. Schools can be assured that their data is backed up and can be restored in the event of a ransomware attack with the help of NEOnet's server hosting or offsite backups.

NEOnet is proud to offer a cost-effective alternative to locally-hosted hardware through the use of industry-leading SmartStack technology powered by Cisco UCS servers and Nimble SSD storage. With a locally-hosted look and feel, schools can maintain full administrative control over their virtual environment while leveraging an off-site data center in a privately-hosted cloud.

HOW CAN DISTRICTS REDUCE LIABILITY AND VULNERABILITY?

The best security in the world won't stop a user from willingly giving someone their password. School districts can reduce cyber liability and vulnerability by providing end user awareness training. NEOnet offers training through its KnowBe4 service, the world's largest security awareness training and simulated phishing platform to protect its customers. KnowBe4 trains users and continues to test them. By providing proper end user training, districts essentially increase protection through the creation of a human firewall.

School districts can also reduce cyber liability by obtaining cyber liability insurance. NEOnet can help districts obtain cyber liability insurance to protect against breaches of personally identifiable information (PII). Cyber liability insurance provides peace of mind by reducing school district's liability risk and protecting sensitive student data information.

If you would like to continue this discussion further, contract Executive Director Matthew Gdovin at *gdovin@NEOnet.org* or call *330-926-2900, ext. 601100.*