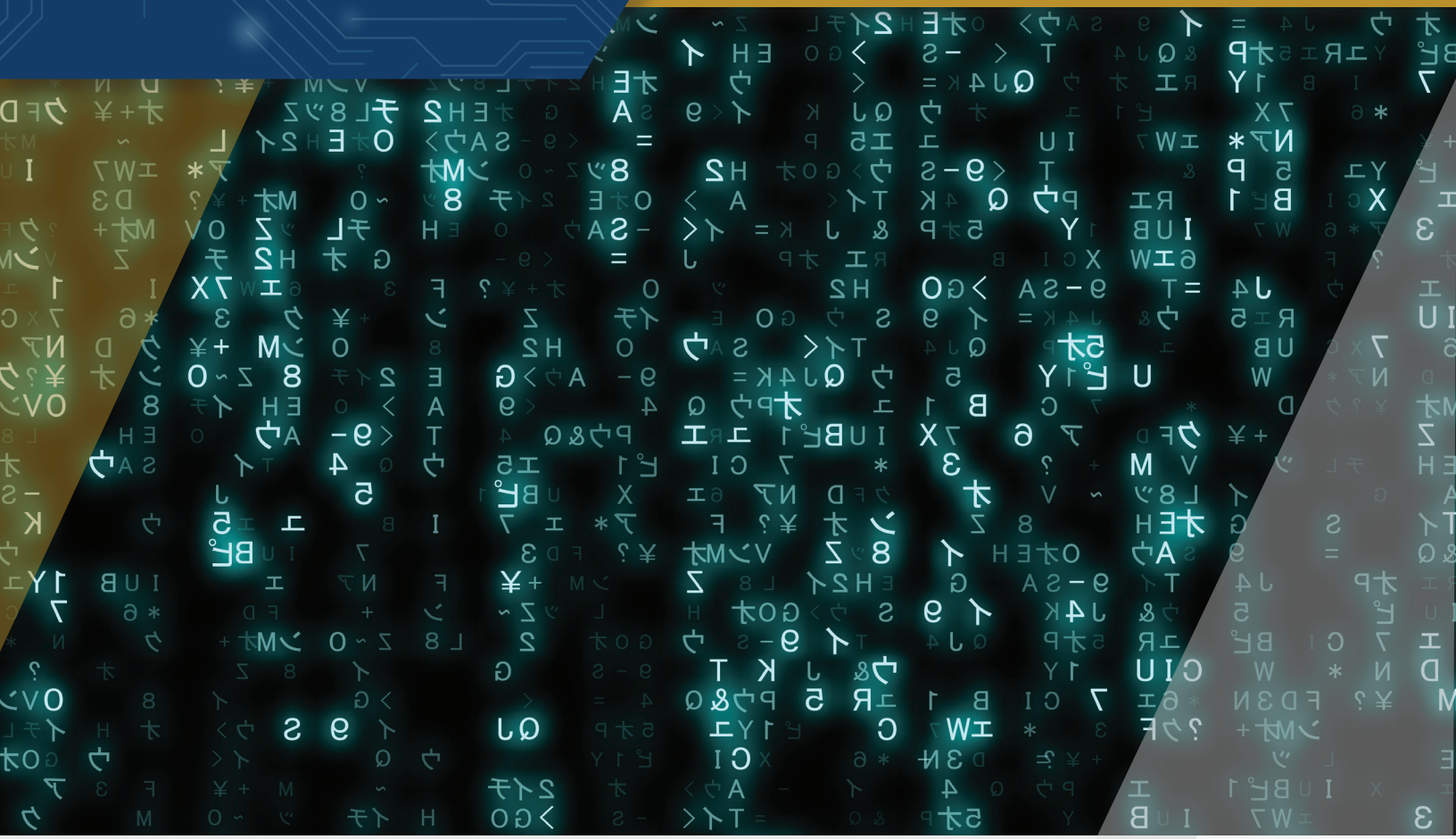


WHAT DOES A DATA BREACH LOOK LIKE?

NEOnet

Prompt. Courteous. Knowledgeable.

Support *you* deserve.

WHAT DOES A DATA BREACH LOOK LIKE?

A data breach can be defined as the intentional or unintentional release of private or confidential information into an untrusted environment. So, what does this mean for K-12 entities similar to those supported by NEOnet? It can mean any number of things, including negative media coverage, missed payrolls or even loss of district funds.

If you are a school district administrator, it is important to constantly ask yourself and know the answers to the following questions:

- How do we know if we are vulnerable?
- What are our vulnerabilities?
- How do we protect our district, employees and students?
- What can we do when security is so complex and expensive?

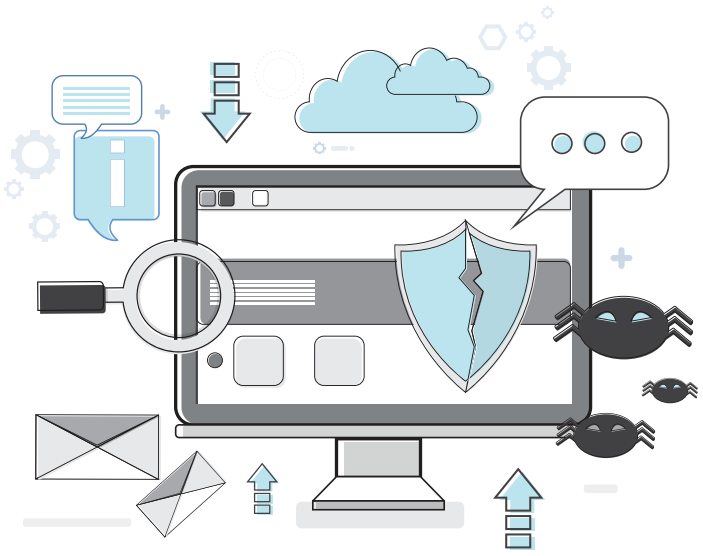
Simply put, every K-12 institution is vulnerable to a data breach and the less time a school district takes in understanding that risk, the sooner they may seek out the holistic approach necessary for reducing the likelihood of having a breach and the associated impact it could have. NEOnet can assist in the journey to a better understanding and of where a district stands in their vulnerability, beginning with the consideration of the following four factors: awareness, threats, methods and prevention.

Awareness

It is very important for a district to understand where they are in their security journey. Part of that journey revolves around understanding where sensitive data is stored and how it is accessed. In short, in order to highlight what your vulnerabilities are, you need to know what can be breached and whose responsibility it is to respond if an incident were to occur. Here are some questions to consider:

1. Do we know who should respond to a security incident?
2. Where does sensitive data live?
3. What technology assets do we have that access sensitive data?
4. What is our policy for accessing that sensitive data?
5. Can a staff member download that data and work on it from home?

While this is not an exhaustive list, it is simply meant to spark additional questions in regard to what data you have and what your rules are for accessing that data. Policy on data security is one of the most important components to limiting the attack avenues available to unwanted visitors.



Threats

Once you understand where your data is and how it is being accessed on a daily basis, the next step is understanding where threats may come from. While this can vary from organization to organization, K-12 entities share some common threat vectors.

- ***Insider Threats*** – Insider threats, both malicious and non-malicious, come from students or staff allowed on your network. For example, a staff member could unknowingly provide an unauthorized entity their username and password. A student could also maliciously attack a system with the intent to gain or restrict access.

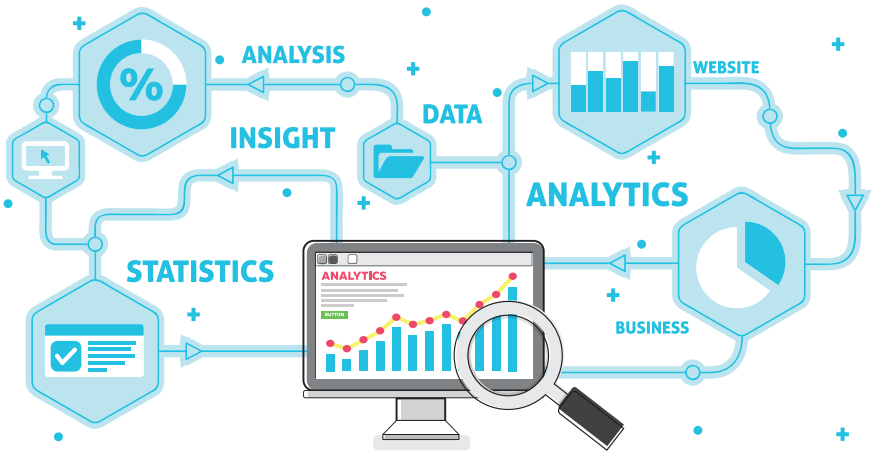
- ***External Threats*** – Malicious threat actors are by far the most common. This includes outside entities who try to trick users into providing information by pretending to be something they are not. There are also external suppliers who should be identified as threats. These external entities, who may provide services to the schools such as cloud services or the implementation of IOT devices, put a district at risk through security vulnerabilities or through lack of sufficient data backup.

Again, this is not meant to be an exhaustive list; it's meant to provide the foundation for additional conversations within the organization that NEOnet can help to facilitate.

Methods

At this point, we have identified what information is subject to being attacked as well as who is doing the attacking, but we haven't yet identified how it can happen. This is why it's important to be familiar with security buzzwords commonly discussed in the news and in technology. Some of the most common methods include:

- Viruses/Malware/Ransomware – malicious programs that give access to data or hold data hostage
- Social Engineering/Phishing – techniques used to trick a user into providing access to important data by delivering an attack that looks to be legitimate
- System Exploits - Flaws in software that give attackers a vector of attack



Prevention

The most complicated part of a school district's journey is understanding and mitigating the risk associated with a security breach. Why, you may ask? There isn't one simple answer to providing comprehensive security. Security has to be a holistic approach and a marriage between cost and effectiveness which NEOnet can provide to school districts. Here are some things to prioritize in an effective prevention strategy:

- ***Prepare*** – Identify the individuals responsible for responding to a security incident such as a data breach. NEOnet's cyber security incident form can aid districts in outlining the response process. This helps clearly define who will be taking the necessary actions toward addressing the district's problem.

- ***Policy*** – Identify who can use what data, when and where. This, at the very least, tells staff members how they are allowed to access the data and removes any doubt of the district's position on the subject.

- ***Leverage*** – Look to your ITC to provide as much security as possible. This could include hosting and backing up your data as well as providing additional security tools. They can provide multiple solutions to threats facing schools.

- ***Insure*** – Make sure your district has a cyber-liability insurance policy. Not only does this help reduce financial liability of a data breach, but it also gives the district additional resources to help if one occurs.

- ***Educate*** – Providing security awareness training and recurring testing for your users is very important. Even the best security products on the planet can't prevent a user from giving someone the keys to the castle.

NEOnet is Here to Safeguard Your District Against Breaches

NEOnet offers school districts the perfect solution to protecting against data breaches. By following NIST (National Institute of Standards and Technology) standards, schools can rest assured that their data is organized, integrated and compliant with the help of NEOnet's secure server hosting.

NEOnet is also proud to assist school districts in adopting cyber liability insurance. Now is your chance to protect your district's data against breaches with NEOnet—contact us to find out more about our security processes.