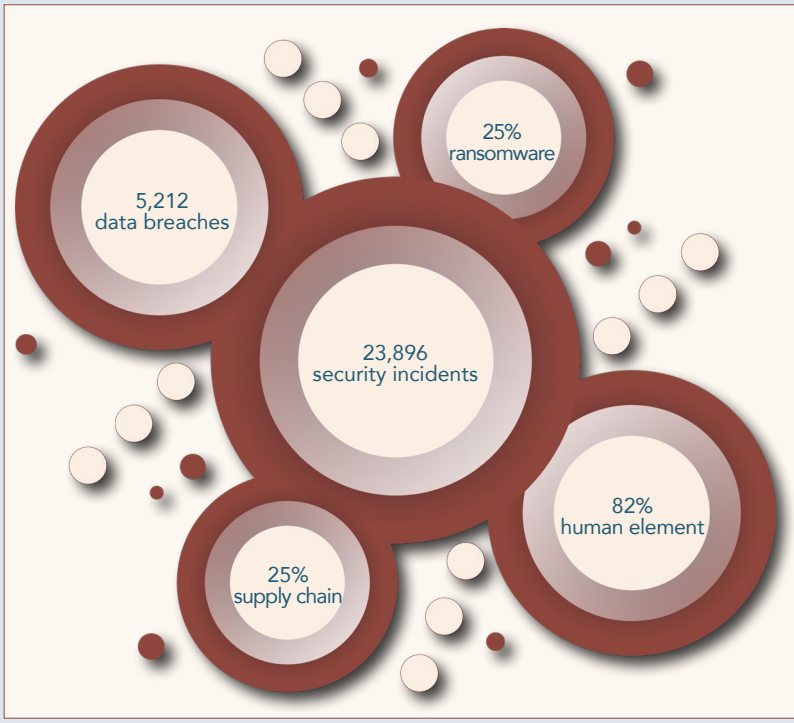
K-12 Security Threats

Education institutions are often found to have the weakest cybersecurity protections out of most industries. And while school districts are falling behind on security efforts due to budgetary and resource constraints, cybercriminals are becoming shrewder, more sophisticated, and even working in concert with other cybercriminals: becoming more efficient and able to exploit more opportunities.

Protecting your district's network from cyberattacks becomes more challenging by the second. According to Verizon's 2022 Data Breach Investigations Report, there were 23,896 security incidents, of which, 5,212 were confirmed data breaches.

Ransomware accounted for a total of 25% incidents, while supply chain issues were responsible for 62% of system intrusion incidents in 2021. Error continued to be a dominant trend, with 82% of breaches involving the human element.

In the education sector, there was a dramatic increase in ransomware attacks (over 30% of breaches), illustrating the need for protection against stolen credentials and phishing attacks potentially exposing the personal information of its employees and students. System Intrusion, Social Engineering and DoS were the leading causes of incidents.



Triple Threats

But what are the specific threats school districts should be prepared for in the coming year?

Artificial intelligence (AI) is something of a double-edged sword in terms of data security. For schools and districts, it can automate any number of tedious tasks while increasing efficiency, but it can also be used by hackers to bypass security protocols and avoid detection while infiltrating networks.

McAfee researchers in their 2023 Threat Predictions Report report that: "The creation of AI-generated images, videos, and even voices are no longer strictly left to professionals. Now anyone with a phone or computer can take advantage of the technology. Google has even made creating AI-generated videos easier than ever.

From cybercriminals to those seeking to falsely influence public opinion, these emerging next-generation content tools will empower scammers and

propagandists to take their tradecraft to the next level with more realistic results and significantly improved efficiency."

Chrome OS Threats. On the heels of the pandemic, Google reported 50 million students and educators worldwide using ChromeOS. This sets the stage for a marked increase in threats impacting Chromebook in the year to come.

In 2023, McAfee expects to see "Chromebook users among millions of unsuspecting victims that download and run malicious content, whether from malicious Android Apps, Progressive Web Apps, or Chrome Web Store extensions, users should be leery of popups and push notifications urging them to install untrusted apps."

Voice-controlled devices that are connected to the Internet can also pose a threat. Cybercriminals can write malicious code to these and other IoT (Internet of Things) devices. These infected devices can supply botnets (a network of private computers infected with malicious software and controlled as a group without the owners' knowledge) and steal sensitive data. Voice-controlled digital assistants, for instance, can be exploited to conceal suspicious activities from users, with common commands reconfigured to trigger malicious activities.

For Peace of Mind, Prepare for the Worst

K-12 IT personnel have to proactively prepare for these and other cyberthreats with limited network and security resources. Despite these challenges, maintaining a secure network isn't impossible. Here are some examples of what this technology should look like:

- A comprehensive security system combining intrusion prevention, anti-virus, anti-malware, content/URL filtering and anti-spam services.
- E-rate eligible firewalls, wireless and WAN acceleration products.
- Children's Internet Protection Act (CIPA) compliance with on-campus and off-campus web filtering.
- A robust security plan that allows an IT team to gain real-time insight into network activity.
- Flexible remote access: Consider a next-generation firewall that does not rely on a third party app, providing native VPN remote-client access for Windows, Chrome, Android and Linux devices.
- Routine patching while making updates to software to keep everything moving forward together.

Establishing strong security policies and procedures—along with implementing robust yet cost-effective security platform solutions—are essential to maintaining security from all threats, regardless of where they're coming from.