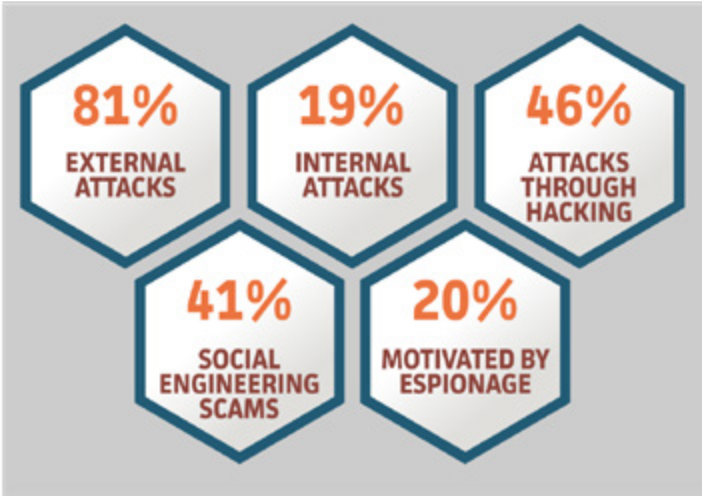
K-12 BLUEPRINT

Security Threats to Prepare For

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 2018 Data Breach Investigations Report, there were 53,308 security incidents and 2,216 data breaches in 2018.

In the education sector, 81% of these attacks were external while 19% were internal. Forty-six percent of these attacks were through hacking, while 41% were through social engineering scams targeting faculty personal information used to commit identity fraud. In addition, 20% of attacks were motivated by espionage.



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 2019 Threat Predictions Report report that: "Bypassing artificial intelligence engines is already on the criminal to-do list; however, criminals can also implement artificial intelligence in their malicious software."

  So, to fight fire with fire, AI-based cybersecurity solutions are poised to thwart these increasingly sophisticated threats: empowering school and district IT to protect vulnerable areas and detect breaches faster than ever.

- **The proliferation of cloud-based applications** have made cloud security a huge concern for schools and districts. In fact, McAfee estimates that there was a 33% increase in users collaborating on sensitive cloud data in 2018, with savvy cybercriminals seeking more targets. Automation can help school IT teams to better monitor cloud security issues and deal with potential incidents in real-time.

- **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.

Learn more

Learn more about data privacy for K-12 education at **CDW.**