NIC PARTNERS
Technology & Security Experts

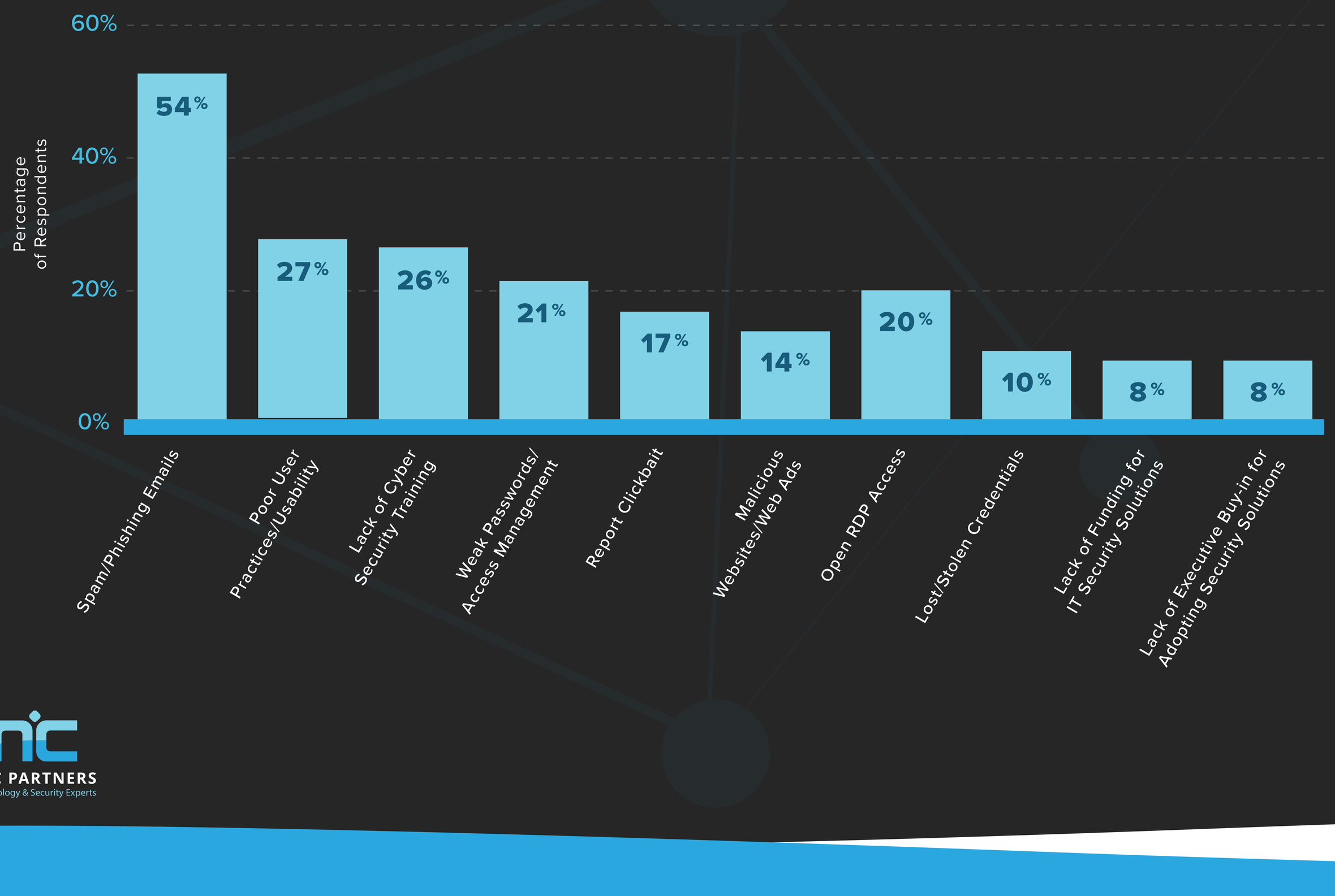
RANSOMWARE IN SCHOOL DISTRICTS: A RISING THREAT

Out of 17 industries surveyed, education **ranked the lowest** in cybersecurity preparedness. This is one reason why schools have become the priority target of hackers, with **57%** of all reported ransomware attacks in August and September of 2020 targeting schools.

When ransomware hits schools, it can be costly. Rockville Center School District paid a ransom of **$88,000** to receive a decryption code for ransomware encrypted files. On average, a ransomware attack costs schools $50,000, but the highest reported numbers often surpass **$1 million**.

The Cause of Ransomware Infections

statista



NIC PARTNERS
Technology & Security Experts

How to Prevent Ransomware in Your District

Understanding Your Environment

Do you have remote students accessing your network from locations off-campus? Consider investing in endpoint discovery and management software to keep track of your authorized endpoints. Investigate the capabilities of your network infrastructure regarding authentication for wired and wireless endpoints before they are permitted to access resources on the network. If you have applications or file shares with sensitive data, consider requiring a posture assessment for any endpoint that will be accessing those resources.

Keep Data Compliant and Secure

Is your data stored on-premises? Do you regularly backup your data in the event it is compromised? By creating frequent backups stored in unaffiliated data centers, you may be able to avoid paying ransoms altogether.

Have Plan in Place

If a security event does occur, you need to have a response plan in place so everyone understands their roles and responsibilities. The quicker you are in detecting and responding to a threat, the less likely your district will suffer important data loss or downtime.

A disaster recovery plan will need to address network access for end-users, server availability, data integrity and backup/restore options. If the Internet is critical for daily operations, then consider having a backup ISP. If your primary data center goes down, can it be brought back up at a different campus? How will your end-users route their traffic to that campus? Can you leverage cloud services if your on-premises servers fail?

Provide Content Filtering

Content Filtering can block the most well-known sources of ransomware from being accessed on your network. By preventing the access of suspicious links, you may be able to stop many attacks before they enter your systems.

An Assessment Is the First Step

How can you accomplish all of the steps above? Firstly, you must take a ransomware assessment to determine your current level of cybersecurity and to uncover any vulnerabilities in your systems. NIC Partners offers a ransomware risk assessment specifically designed for school districts. Don’t wait—take the first step to protecting your district today.

Book a consultation with us to discuss today.

CONTACT US