Guidepost

CYBER ATTACKERS CHOOSE THE PATH OF LEAST RESISTANCE: THE EDUCATION SECTOR

From private schools to K-12 school districts and from learning centers to universities, cyber attackers have expanded their targets to include the numerous entities that make up the education sector. Their ultimate goals remain the same: obtain sensitive information, hold these institutions (staff, faculty, students) as ransomware hostages and/or steal financial records to resell on the black market.

It is not surprising that cyber attackers have chosen to feed on this sector. This target is typically viewed by cyber attackers as a "path of least resistance" in comparison to global companies.

Cyber attackers are well aware that education facilities typically do not have adequate staffing to tactically and strategically address a comprehensive cyber threat mitigation plan. Additionally, many of the attack tools recently used to target the education sector were originally designed to pursue larger corporations. As a result of enduring the agonizing experience of a breach or other cyber-attack, these larger entities bolstered their cyber security through devices, staff, policies and procedures. Their enhanced cyber controls have rendered those early attack methods to not be as effective, *until now*. Cyber attackers are repurposing their attack tools, often without the need to create anything new, to hunt the resource-lacking education sector.

Below are several key steps to help the education sector combat cybercrime:

1. **Conduct periodic "Security Awareness Training" sessions** for all of your personnel, including faculty, coaches, administrative staff, and others. Often times, your employees can be the first line of defense. Educating them about cyber breaches, phishing scams, etc., will strengthen their ability to detect and prevent future cyber-attacks.
2. **Perform a comprehensive Threat-Vulnerability-Risk Assessment (TVRA) in-context with its environment** (whether it be a K-12 school district or a higher education institution). This process identifies, quantifies and documents the probability of various types of threats related to a specific learning facility

which may cause a disruption in operations.

3. **Develop an overall "Incident Management Playbook"** to cover reported incidents (emphasized in the above Security Awareness Training session) and how to properly address those incidents. This includes procedures for communicating to affected parties.
4. **Create a prioritized list of risks** (based on the TVRA above) and associate those risks with adequate controls (e.g. technology, services or additional procedures) to mitigate risk. Depending on the current security posture, these controls may need to be developed or enhanced. Identifying top-level risks now can serve as a catalyst for additional controls or defenses in the future.
5. **Reassess your risk environment, continuously**, through the TVRA process. This will put closure on previously found risks, ensuring they have been mitigated to an acceptable level, and determine whether new risks have evolved since the prior assessment.

Since most education facilities do not have the internal resources to develop, implement and continuously monitor a cyber defense plan, finding an objective security company will be critical.

When vetting security firms, keep the following suggestions in mind to ensure your security firm is providing the best strategies available:

1. Choose a firm that does not sell security products. These firms may push you to purchase tools that may not be ideal for your specific security issues or environment. Their focus tends to be on products and not on security assessments and planning.
2. Consider a security company with specific expertise in the education sector. Its professionals understand the operational and physical security needs to protect employees, faculty and students, and how those aspects tie into the cyber component of an overall security plan.
3. Review the backgrounds of the project team that will be working with you. Ensure their credentials and experience include providing overall security assessments, plan development and implementation, as well as specific cyber security consulting.

Keep in mind, the cyber mitigation plan you ultimately implement will only be as good as the staff using your systems. As emphasized above, all staff should receive specific cyber security training. By choosing a program with hands-on training and testing, your employees are more likely to retain vital information.