Cyber Security in the Education Sector

Haroon Malik

Introduction

The education sector has seen a significant increase in cyber-attacks. Institutions have been a target for several years now, with malware and phishing attacks increasing in ferocity and frequency. With the ongoing pandemic and a major move to remote work and online learning, this sector is often the prime target. The lack of preparedness seems to be a major reason why this sector is a prime focus for most threat actors.

A survey which was conducted by the UK Department for Digital, Media and Sport showed the education sector experiencing the greatest number of cyber-attacks compared with other industry sectors, with over 80% of further education institutions identifying cyber-attacks or data breaches over the last 12 months. Moreover, Microsoft reports show more than 60% of malware attempts in Microsoft 365 monthly, are focused on the education sector.

It is crucial to protect schools and universities by making them understand the magnitude of cyber risks, mainly because the impact of a cyber-attack on institutions goes beyond data theft and into operational disruption and reputational damage.

The average cost of a data breach in 2020 was

$3.9 million

in the education sector

Why Is the Education Sector at Risk?

The attacks on the education sector have increased for the last few years due to a plethora of reasons, which we look at in this section.

A Data Treasure Chest for Threat Actors

Education institutions store huge volumes of sensistive data (students and staff), research information, intellectual property, payment details, strategic partnerships and information on third parties. This creates a huge ‘data treasure chest’ for the threat actors out there, who plan to sell such vast and valuable information to a third party or use it as a bargaining tool to extort money.

Doing More With Less

Many schools lack sufficiently skilled cyber security resources and do not have sufficient budgets. A low priority for security protection investments can lead to major vulnerabilities and impact an institution’s ability to defend against cyber-attacks and data breaches. Schools and universities often rely on outdated security tools.

Melting Point of Devices and ‘Always On’ Connectivity

The number of new students joining schools, colleges and universities, coupled with a melting pot of data assets and a relatively 'open' technology environment introduces many cyber risks. This type of vulnerable network is already seen as difficult for administrators to effectively secure, leading to an increasingly large 'attack surface'.

Lack of Cyber Awareness Culture

Did you know human error is the number one cause of data breaches? Unfortunately, cyber security is still largely seen as a technical IT issue in the education sector, as opposed to an enterprise-level risk. Everybody in an academic environment has a role to play in protecting data and information.

How Can Education Providers Protect Themselves?

Schools and universities must start implementing **basic technical measures**, such as end-point protection, patching and application security. It is crucial that leaders play an active role in cyber security programmes and must be able to ask the right questions. Here are 10 important questions to get you started.

- Do we have a **named individual or group accountable** for cyber security for our institution?
- Do we have cyber security included as a **major risk on our latest risk register**?
- If we had a cyber attack, how soon would we know? Do we have **effective monitoring systems** in place to know when a breach has occurred?
- How are we **raising awareness** of cyber threats amongst our staff and students? How are we measuring the effectiveness of this training?
- Have we identified the **high-value critical assets** within our digital estate and how confident are we that they are secured appropriately?
- Do we know **who to contact** if we become a victim of a cyber attack (e.g. ransomware)?
- Do senior staff have a **good understanding** of the cyber security threats and their potential impact (e.g. social engineering, phishing).

- How effective is our **cyber incident response process** and when was it last tested?
- Do we have a **disaster recovery and business continuity process** and if so, when was it last tested?
- Do we have **cyber security insurance**?

Even though this eBook is short and sweet (just the way we like it) we understand this is a lot to take in and action. To help you stay in the right mindset, the #1 thing to keep in mind is that by just implementing some basic technical measures, schools and universities can become more cyber resilient.

It is crucial that education institutions take the time to review their current cyber security posture and develop a holistic cyber strategy that covers:

People, Process and Technology.