

Insights into the Microsoft Digital Defence Report

Cybersecurity is one of the most critical challenges of our time. The widespread use of technology in schools has not only brought significant benefits and efficiency but also a host of new vulnerabilities and threats. As a global leader in technology and provider of IT software and cloud services into almost every school, business and home, Microsoft are one of the leaders in tackling these challenges. This paper takes a look at the recently published Microsoft Defence Report for 2024 and brings some context for schools and Multi Academy Trusts.

Education: A Prime Target

Education has emerged as one of the most targeted sectors by cyber threat actors, surpassing even government and national infrastructure. In 2024, the Education and Research sector became the second most targeted by nation-state actors, with institutions often used as testing grounds for new attack techniques. Notably, education was the most targeted sector by threat actors from Iran and over 20% of attacks from China and North Korea were directed at educational institutions.

Top 10 Targeted Sectors Worldwide		
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think Tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All Others	16%

The reasons behind this targeting are multifaceted. Higher Education often possess valuable research data and intellectual property, making them attractive. Additionally, the lack of funding for cybersecurity defence, the potential skill gaps and the open and collaborative nature of schools can create security vulnerabilities.

Microsoft believe that the prevalence of potential vulnerabilities attract threat actors to use schools as a testing ground for new attack and techniques and whilst schools do not pay ransomware fees, the potential for disruption is also a key driver by attackers.

The frequency of cyberattacks against Microsoft’s platforms is staggering, with an estimated 7,000 password attacks occurring every second. This relentless barrage highlights the importance of continuous vigilance and robust security measures to protect sensitive information and digital assets. The high volume of attacks underlines the need for automated security solutions that can detect and respond to threats in real-time, including everything from Endpoint Protection solutions or a more sophisticated Managed Detection and Response (MDR) solution.

The Evolving Cyber Threat Landscape

Cyber threats have become more sophisticated and pervasive. Among the most prevalent threats are ransomware, phishing and identity-based attacks, each posing significant risks to individuals and schools alike.

Identity-Based Attacks

Identity-based attacks, including credential theft and account takeover, have surged in recent years. These attacks target users' digital identities, allowing attackers to gain unauthorised access to systems and data. Microsoft's analysis reveals that more than 99% of identity attacks are password-based, underscoring the critical need for robust authentication mechanisms.



Credential stuffing, where attackers use stolen usernames and passwords from one breach to try and access other accounts, has become increasingly prevalent. This method exploits the common practice of password reuse, emphasising the importance of unique and strong passwords and Multi Factor Authentication (MFA).

Ransomware

Ransomware remains one of the most destructive cyber threats and can have a devastating impact on schools, with attackers encrypting victims' data and demanding a ransom for its release. The financial and operational impact of ransomware attacks can be crippling for extended periods. These attacks not only cause immediate disruptions but also have long-term consequences, including loss of reputation and trust.

Ransomware gangs have become more organised, with some even offering "Ransomware-as-a-Service" to other criminals. This model of ransomware has lowered the barrier to entry, allowing more malicious actors to launch such attacks. As a result, the frequency and severity of ransomware incidents have surged, necessitating robust preventive and responsive measures.

Phishing

Phishing attacks, where bad actors deceive individuals into providing sensitive information, continue to be a common and effective method of breaching security. These attacks often leverage social engineering tactics to exploit human psychology, making them particularly challenging to combat. Phishing emails may appear to be from trusted sources, urging recipients to click on malicious links or download harmful attachments.

In recent years, phishing techniques have evolved, with attackers using more sophisticated methods such as spear-phishing, targeting specific individuals or organisations. Business Email Compromise (BEC) is another variant, where attackers impersonate Head Teachers or other key members of staff to trick staff into transferring funds or revealing confidential information. The financial and data losses from phishing attacks can be substantial, highlighting the need for continuous awareness and training programs.

The Rise of Threat Actors

The number of cyber threat actors has seen a dramatic increase, rising from 300 to 1,500 groups within a year. This surge is further complicated by the growing involvement of nation-state actors, who bring significant resources and capabilities to the cybersecurity battlefield. Nation-state-backed attacks are often highly sophisticated, targeting critical infrastructure and key sectors such as education and research. These actors are motivated by various goals, including disruption and financial gain.

Nation-state threat actors are often well-funded and possess advanced technical expertise, making their attacks particularly challenging to defend against. They may employ a wide range of tactics, techniques and procedures, including zero-day exploits, malware and social engineering.

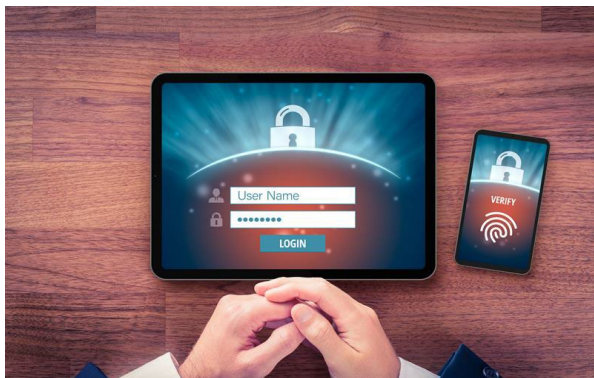
Monitoring and Mitigation Efforts

To combat these threats, Microsoft has established a dedicated team of 34,000 security engineers, monitoring an astounding 78 trillion signals per day. This extensive surveillance allows Microsoft to detect and respond to threats swiftly, minimising potential damage and exposure. The company's comprehensive threat intelligence capabilities enable it to identify emerging threats and vulnerabilities, providing critical insights to enhance security measures.

Microsoft's approach to cybersecurity is multi-faceted, encompassing advanced threat detection, incident response and proactive threat hunting. By leveraging artificial intelligence and machine learning, Microsoft can analyse vast amounts of data to identify patterns and anomalies indicative of malicious activity. This proactive stance ensures that threats are addressed before they can cause significant harm.

Entra ID and Authentication

Microsoft's Entra ID (formerly Azure AD), with 425 million users, plays a crucial role in identity and access management. The system handles over 30 billion authentications per day, providing a robust framework for securing digital identities. Multi-Factor Authentication (MFA) remains a cornerstone of Microsoft's security strategy, as it significantly reduces the likelihood of successful attacks. By requiring multiple forms of verification, MFA adds an extra layer of protection, making it much harder for attackers to compromise accounts.



In addition to MFA, Microsoft promotes the use of password less authentication methods, such as biometric and hardware-based solutions. These methods eliminate the reliance on passwords, which are often the weakest link in the security chain. By adopting password less technologies, organisations can enhance their security posture and reduce the risk of identity-based attacks.

Microsoft Secure Futures Initiative

In response to the growing cyber threat landscape, Microsoft launched the Secure Futures Initiative, aimed at reducing the potential attack surface and enhancing overall security posture. This initiative has led to the removal of 730,000 non-compliant apps and 5.75 million inactive tenants, significantly decreasing vulnerabilities and exposure. By eliminating these potential entry points, Microsoft has reduced the risk of attacks and improved the security of its ecosystem.

The Secure Futures Initiative also focuses on fostering a culture of security awareness and best practices across the industry. Microsoft collaborates with various stakeholders, including customers, partners and governments, to promote cybersecurity education and training. By empowering individuals and organisations with the knowledge and tools they need to protect themselves, Microsoft is contributing to a more secure digital environment.



Conclusion

The Cybersecurity landscape is constantly evolving, presenting new challenges and threats that require innovative and adaptive responses.

The Microsoft Digital Defence Report provides an alarming insight into the scale and growth in cyberattacks, as well as the sheer volume of transactions processed by Microsoft themselves. This highlights the importance of vigilance, innovation and collaboration protecting schools and Multi Academy Trusts against ever-evolving threats.

For a full copy of the Microsoft Digital Defence Report 2024, please [click here](#)

About Virtue Technologies

Virtue Technologies is an education-focused IT company with nearly 20 years of experience working collaboratively with Schools to deliver fit for purpose technology solutions.

Founded in 2006 we have gone on to become a leading provider of IT solutions to Primary and Secondary Schools, Multi Academy Trusts, Further Education Colleges and Universities.

About the Author

Will Stead works closely with Schools and Multi Academy Trusts to support the development of IT and Cybersecurity Strategy and Plans. He has over 35 years of experience in the IT industry, with the last 15 years in education.