Is your school a virtual backdoor?

Cybersecurity in schools goes beyond students and teachers

Cybersecurity has never been more important

And its role in the security of educational buildings cannot be understated. Today, the need for cybersecurity extends beyond the classroom to the built environment and school architecture itself.

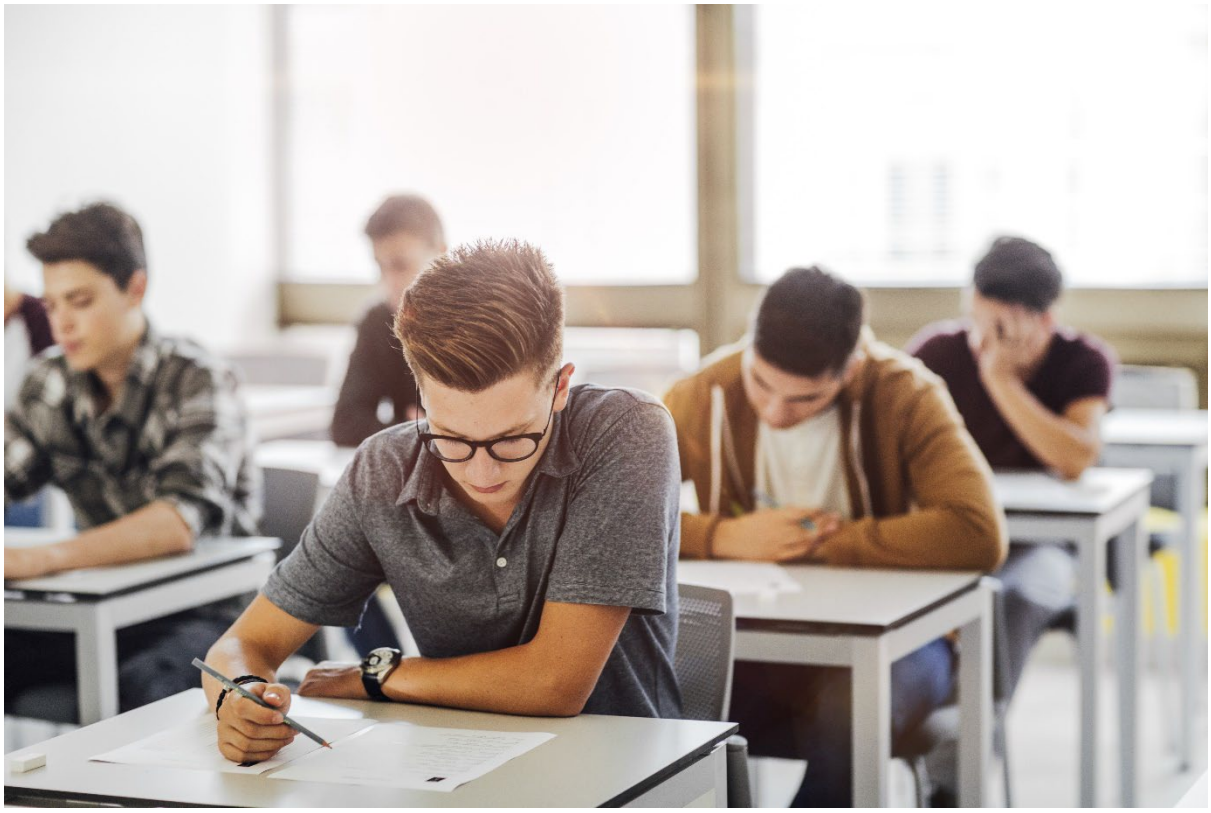
Buildings are now a potential target for infiltration as more schools modernise their technology. Years ago, modernising a building would have a limited impact on building technologies such as HVAC systems.

That approach, however, resulted in disconnected building systems, opening a virtual backdoor to the building's IT network. Schools hold valuable data that requires protection. Cyberattacks compromise this data and can disrupt day-to-day operations, potentially impacting sensitive information and the wellbeing of staff and students.

For protection against cyber threats, robust security measures are mandatory – for IT and building technology alike.

For protection against cyber threats,
robust security measures are mandatory.

Safeguarding information in school IT systems



In schools, cybersecurity involves safeguarding sensitive information such as student records and financial data held on IT systems. It can also involve integrating access control and video surveillance.

Vulnerabilities in the building's network devices can open the door to unauthorised access, data breaches and disruptions that could compromise records.

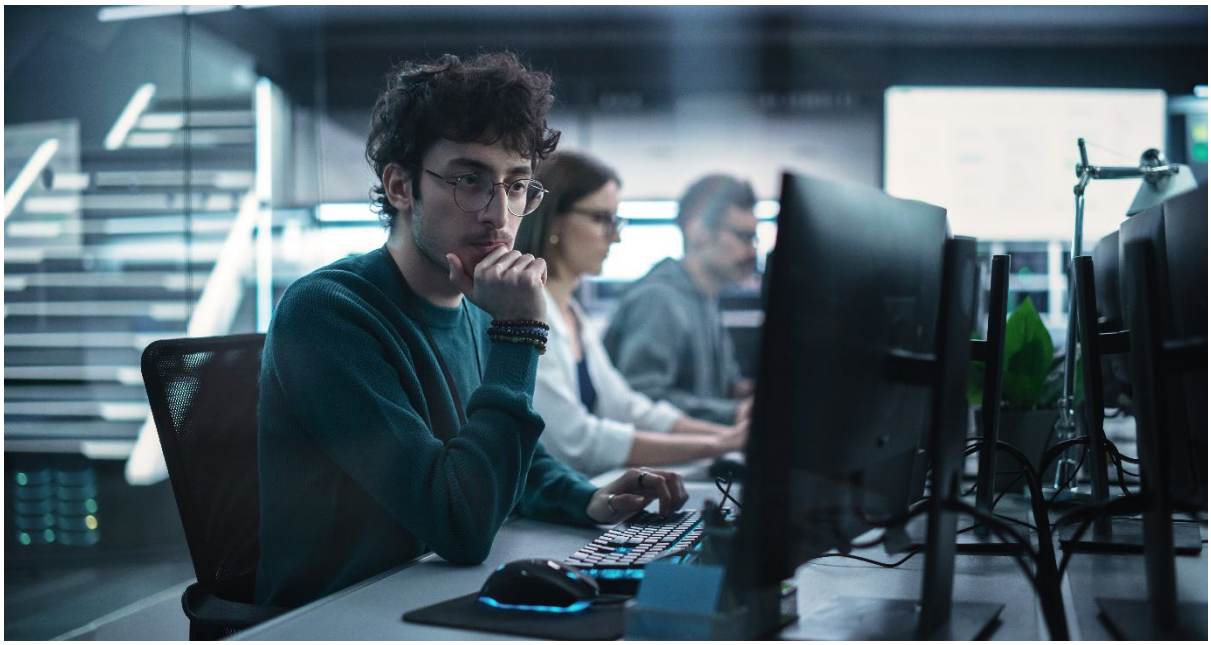
According to an audit by the National Cyber Security Centre (NCSC) and the London Grid for Learning (LGfL), published in January 2023, 78 percent of UK schools experienced at least one cyber incident.[1]

The risk increases for higher education institutions: the UK Government's Cyber Security Breaches Survey 2022 noted that 62 percent of higher education institutions experienced breaches or attacks every week.[2]

Attacks can come in various forms. Ransomware attacks, where hackers encrypt data and demand a ransom, have become common. A 2022 report by SWGfL and the University of Kent showed that almost 48 percent of cyberattacks targeting schools were ransomware attacks.

The report found that only one respondent paid the ransom to decrypt the data – yet even without the direct financial impact of a ransom, the indirect costs may be devastating.

Building out vulnerabilities



Not only are the number of cyber-attacks increasing, so are the vulnerabilities within school environments. Recently, the adoption of connected technologies and Internet of Things (IoT) devices in schools has increased, opening possible entry points for malicious attacks.[3]

Connected technologies, such as a Building Energy Management System (BEMS), offer benefits for energy management and cost control. Without proper cybersecurity measures in place, however, the same technologies invite hackers through the backdoor of a school's IT network.

One such incident in 2013 brought widespread attention to the issue of IoT cybersecurity. Hackers broke into United States retailer Target's computer networks, accessing personal details of 70 million customers; it's believed the entry point was Target's HVAC system.[4] Earlier that year, researchers hacked the control system of the Google Australia office.[5]

In 2021, an office in Germany was the target of a cyber-attack in which three-quarters of its building systems were locked down, rendering window shutter controllers to light switches useless. The company had to manually turn off building lighting systems using the central circuit breakers.[6]

The latter case distinguishes cyber-attacks with IoT entry points and those without. In some cases, a hacker may have no financial motivation or interest in accessing sensitive data.

Instead, they may simply want to disrupt the normal functioning of the school premises – whether this is a malicious actor trying to shut down site security or an IT savvy student turning off heating systems in winter to force a closure.

Several cases share similarities: security flaws in the IoT and building systems had not been addressed. For a school's IT system, managers can take steps to maintain high levels of security and reduce the risk of devices being compromised.

These steps are part of maintaining building systems, but effective IoT and BMS cybersecurity begins during installation.

In some cases, a hacker may have no financial motivation or interest in accessing sensitive data. Instead, they may simply want to disrupt the normal functioning of the school premises.

Building in cybersecurity

Protection at the device level is typically a gap in building cybersecurity. A contractor may install a BMS controller but bypass security steps, such as setting up PIN protection or user authentication.

Fortunately, this is becoming less common as manufacturers build in security features that can't be circumvented during installation. For example, Trend's IQ5 BEMS controller requires security measures to be taken during its setup.

IQ5 also requires users to have a single sign-on with any password changes synced throughout the network. This reduces the risk of the controllers becoming an entry point for a malicious attack.

At the BEMS level, the key is built-in authentication and encryption. A school BEMS should be set up to protect user passwords and encrypt data shared between devices.

Building managers should maintain an accessible and auditable track of processes and database changes and support Lightweight Directory Access Protocol (LDAP) passwords for additional security. These features are supported by Trend BEMS and supervisor platforms like IQVISION.

Upkeep is where these systems become most vulnerable. As with any IT system, firmware should be updated regularly for the BEMS, HVAC systems and IoT devices. If vulnerabilities are identified at any point, they should be patched out.

Also, a BMS should be supported by the manufacturer. Older building management systems can still function but tend to be installed on legacy operating systems that are obsolete and no longer supported. This makes the systems ripe for cyber-attack.

Within the education market where budgets are often tight, modernising building systems may not be prioritised, putting school premises at greater risk.

In the coming years, the general cyber risk to schools will increase as digital-led teaching practices become the norm. School site teams will look to connected buildings to monitor and manage energy and costs.

Moreover, the volume of IoT-focused attacks will increase – Check Point Research found that, in early 2023, the first two months of the year had seen a 41 percent leap in the number of weekly IoT device attacks compared to 2022.[7]

Cybersecurity is built into Trend BEMS

The cybersecurity of building controls must be prioritised as much as IT systems. For educational leaders, school cybersecurity involves specifying the right technology and configuring robust security features.

Only by maintaining the cybersecurity of IoT devices and connected building controls can we work to seal virtual backdoors.

Ready to improve your school's cybersecurity?

Discover how a Trend BEMS is built with cybersecurity at its core.

ABOUT THE AUTHOR

Pradeep Singh

Pradeep is an intelligent buildings solution consultant at Trend Control Systems Ltd. Part of Honeywell Building Automation.

References

1. James Coker. *Three-Quarters of UK Schools Have Experienced a Cyber Incident*. InfoSecurity Magazine. Published January 17, 2023. Accessed March 12, 2024. https://www.infosecurity-magazine.com/news/three-quarters-uk-schools-cyber

2. UK Government. *Cyber Security Breaches Survey 2022*. Published July 11, 2022. Accessed March 12, 2024. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022

3. SWGfL & University of Kent. *Cyber Security in UK Schools*. Published April 2022. Accessed March 13, 2024.

4. Gregory Wallace. *HVAC vendor eyed as entry point for Target breach*. CNN. Published February 7, 2014. Accessed March 13, 2024. https://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html

5. Jane Wakefield. *Tomorrow's Buildings: Help! My building has been hacked*. BBC. Published April 20, 2016. Accessed March 13, 2024. https://www.bbc.co.uk/news/technology-35746649

6. Kelly Jackson Higgins. *Lights Out: Cyberattacks Shut Down Building Automation Systems*. Dark Reading. Published December 20, 2021. Accessed March 13, 2024. https://www.darkreading.com/cyberattacks-data-breaches/lights-out-cyberattacks-shut-down-building-automation-systems

7. Gaurav Sharma. *A sharp increase in cyberattacks on IoT devices: Check Point*. Security Brief. Published April 25, 2023. Accessed March 15, 2024.