QBE Commercial Combined

Cyber security and schools

Schools, colleges and universities are increasingly being targeted by cyber criminals. We are seeing more and more reports of educational establishments being the victims of phishing and ransomware attacks, with some resorting to handing over money to criminals to get their systems back up and running.

In addition, security experts have warned of a campaign against private schools and the parents paying school fees, whereby hackers breach school IT systems and then email parents with fake invoices asking for payments to be made to a new bank account.

The cyber risk to the educational sector is very real and is growing.

PROTECT YOUR SCHOOL

Cyber crime is one of the biggest risks today.

In 2017 a London university was hit by a ransomware attack that brought down its student management system.

Data breaches at British universities have doubled in the past two years.

In 2017 a US college paid a $28,000 ransom to hackers after being locked out of their computer systems.

Ransomware is big business for cyber criminals, estimated at over $5 billion dollars in 2017.

What can schools do to protect themselves?

Have robust IT processes:

- Safeguard computer networks with a firewall
- Encrypt all sensitive data and personal information
- Keep operating systems and all software updated
- Backup data regularly
- Use up-to-date antivirus / anti-spyware software and subscribe to a threat alert service
- Avoid using easy passwords
- Avoid using the same passwords across several systems
- Discourage staff from bringing in their own devices
- Delete suspicious emails without opening
- Be wary of clicking on links in emails
- Test your website and web hosting for any vulnerabilities

Examine all physical security and anti-theft measures:

- Protect all computers, laptops, smartphones, USB sticks, hard-drives and routers
- Secure the school premises with alarms and CCTV
- Use data shredding to securely dispose of sensitive documents
- Securely remove data from old laptops and computers by wiping their hard-drives

Consider risk management and cyber training:

- Secure all IT networks and systems
- Protect customer data
- Safeguard confidential information and intellectual property
- Minimise business interruption and downtime
- Reduce the risk of any fines and financial penalties
- Reduce reputational damage and a public relations crisis
- Have systems in place for staff and students to flag up any suspicious activity
- Train staff to be wary of the social engineering tricks that criminals use to gain information

QBE Business Insurance has a specialist offering for independent schools and educational establishments to make sure that they have the right insurance cover in place, which can include a swift response in the event of a cyber incident.

Ask your insurance broker about QBE.

qbeeurope.com/products/commercial-combined

Made possible QBE

QBE European Operations
Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 **QBEurope.com**

8705/MAR2018