Cyber risk and education

Cyber risk is a growing concern for many organisations and we've recently conducted research that shows education establishments are no exception. As a result of our research, we've put together some information to help schools protect themselves from cyber threats.

Examples of cyber risk in schools

It's clear that many establishments still feel uneasy about whether their school is fully prepared for a cyber attack. Our research revealed that over two thirds of educational establishments are concerned with the impact of cyber crime but it is not the only risk. Below are several examples of cyber risks experienced by schools.

1 Independent school cyber attack

Last year, Insurance Times[1] reported a phishing attack on an independent school. The target had been school fees and the attacker had emailed parents asking them to pay the terms fees via a link. This link however, had nothing to do with the school and fees were paid to a rogue website.

It's very difficult to defend against this type of attack but creating awareness of how to recognise rogue communications may help prevent parents and teachers becoming victims to the crime. You can find examples of phishing emails and what to look out for from HMRC.
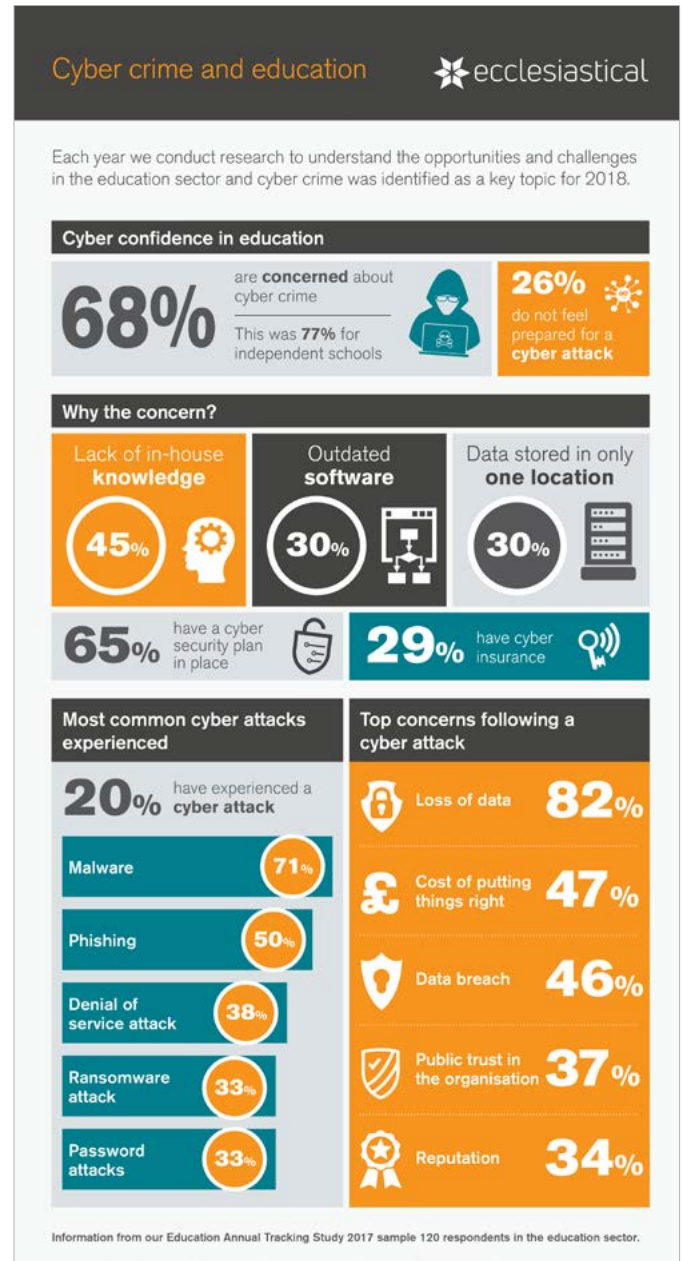
2 The insider

Tech-savvy children can also pose a threat to schools.

In cyber terms, 'the insider' is possibly the most difficult threat to defend against as they already have access to your systems.

Famously in 2014, several pupils used a keylogger to hack the system and change their grades. Keyloggers can come in the form of software or hardware and record input from the user's keyboard. Passwords and other information can then be extracted and used, in this case, to change grades.

Cyber crime and education — ✴ ecclesiastical

Each year we conduct research to understand the opportunities and challenges in the education sector and cyber crime was identified as a key topic for 2018.

Cyber confidence in education

68% are **concerned** about cyber crime — This was **77%** for independent schools

26% do not feel prepared for a **cyber attack**

Why the concern?

Lack of in-house **knowledge** 45%

Outdated **software** 30%

Data stored in only **one location** 30%

65% have a cyber security plan in place

29% have cyber insurance

Most common cyber attacks experienced

20% have experienced a cyber attack

Malware	71%
Phishing	50%
Denial of service attack	38%
Ransomware attack	33%
Password attacks	33%

Top concerns following a cyber attack

Loss of data	82%
Cost of putting things right	47%
Data breach	46%
Public trust in the organisation	37%
Reputation	34%

Information from our Education Annual Tracking Study 2017 sample 120 respondents in the education sector.

1. Hackers are targeting school fees, warns cyber insurance firm, Insurance Times, 15 December 2017

✴ ecclesiastical

3 Data Breach

All educational establishments will hold sensitive data about students and staff. Ensuring this data is stored safely is extremely important.

When we think of a data breach, today we often automatically think of cyber criminals gaining access to the data in the system. But a data breach may not be caused by criminal activity.

For example – a staff laptop could be lost or stolen - data may be stored to the desktop, or confidential paperwork downloaded or a there may be a USB stick which holds data records, in all cases this would be considered a data breach.

Carelessness is sometimes a factor too and the accidental release of data can be as unintentional as sending an email correspondence to the wrong person.

An example of the latter took place when a school in East London accidentally revealed the names of seven primary school pupils feared to be at risk of radicalisation as they had received a Freedom of Information request from a parent. This would not necessarily be viewed as a cyber crime, but it is the unauthorised publication of data. [2]

Defending against a cyber attack

Though it's unlikely any organisation will be able to completely eliminate the risk of a cyber attack, basic cyber security measures are often the most effective and can be carried out without extra IT support.

You can find more information in our guide to Cyber security. Or visit the Cyber Essentials website for advice from the National Cyber Security Centre for advice and helpful checklists.

Cyber insurance for schools

Cyber insurance acts as a safety net. As we mentioned, it's impossible to completely eliminate cyber risks even with sophisticated cyber security controls in place.

What does cyber insurance cover?

Ecclesiastical cyber insurance for schools includes the following cover:
- Computer, data and cyber risks, designed to meet the needs of small and medium sized organisations.
- Costs of dealing with data breaches excluding legal fines.
- Costs of dealing with cyber liability claims.
- Cover for business losses from a cyber event.
- Cover that helps organisations with the impact of cyber crime.

It also includes access to expert advice and support when an incident occurs to help mitigate the financial impact or reputational damage.

2. http://www.bbc.co.uk/news/uk-england-london-34942431

About the author

Faith Parish, ACII – Director of Heritage, Education & Art & Private Client

Faith was appointed Director of Heritage, Education at Ecclesiastical Insurance in July 2015. Since joining Faith has focused on developing new products and propositions for Education, Heritage and Art & Private Client customers. Faith has over 19 years' experience in the insurance industry having previously been employed with Zurich in a number of senior underwriting and marketing roles and is a qualified Chartered Insurer.

For further information visit
www.ecclesiastical.com/broker

PD2832 1 03/21