Independent, but insecure?

The growing cyber security risks facing the independent education sector

endsleigh

Find your possible.

Foreword

John Murphie
Chief Operating Officer, ISBA

“

The Association has a unique national (and increasingly international) perspective on the issues schools face on a daily basis. The most insidiously damaging, and most difficult to counter, are those issues that affect the school’s reputation. The risk that poorly managed cyber security poses diminishes a school’s reputation as a consequence of a data or financial loss. Often the tangible loss is uncomfortable but relatively easily dealt with, however, the intangible reputational loss is more damaging and has a far longer duration. Schools therefore cannot ignore the risk cyber security poses.

To compound the issue, the cyber risks schools face constantly change; both in terms of sophistication and the direction from which they originate. As such, one of the biggest challenges a school faces is balancing the available funds they have at their disposal against the expense of countering the cyber risks.

The risks range from curious pupils attempting to access secure areas of a school’s server through to outside entities with ulterior motives targeting weak spots in a school’s IT security, to unintentional vulnerability through accidental data breaches or loss of portable equipment.

While some within the sector may feel that a school is not as high a target for cyber criminals as a multi-national firm or public service body, schools can remain vulnerable by not following a policy of actively protecting themselves. A top-down approach is one of the most effective ways of providing a robust response to rising cyber threats, all those involved in the direction and running of a school are made aware of their responsibilities, the developing threats, and the necessary countermeasures.

Best practice will also include judging the relevance of the advice and guidance of experts within the field and using that to inform cyber security policy and actions.

Ultimately, cyber security is an issue which will continue to challenge the independent schools’ sector. However, this report will demonstrate that by increasing awareness and taking an active, and occasionally anticipative approach to mitigating the risks, schools can start to very effectively manage existing and emerging cyber threats.

21st century challenges

The state of play for cyber security in the independent education sector

The sustained integration of technology into the schoolroom over the past two decades has undoubtedly changed the art of teaching.

Yet, technological innovation has also created new vulnerabilities which can be exploited by criminals, who see schools as profitable targets. With sensitive pupil data on file, as well as the financial details of fee-paying parents and guardians, cyber security is an increasing risk for independent schools.

These cyber-risks fall into two categories: crime, where a school has been intentionally targeted; and security, which can be further broken down into intentional and accidental security breaches that could allow for sensitive information or personal data to be made available.

To fully understand awareness of and attitudes towards cyber security within the UK’s independent schools, Endsleigh Insurance Services has commissioned an in-depth survey of key stakeholders from across the sector, including Head Teachers, Deputy Head Teachers, Bursars, Governors, and other senior management professionals.

Results show over half the independent schools in the UK have experienced a cyber-attack in the last five years, and that the sophistication of cyber-threats continues to grow ahead of awareness within the industry.

Key findings

The headline statistic details how 61% of independent schools have reported experiencing a cyber-attack within the last five years.

However, just 39% of those surveyed considered their school to be a target for cybercriminals.

The disparity between the two statistics demonstrates the gap between risk and perception across the sector.

73% of those surveyed considered themselves to be fully protected from cyber security threats, with just 1% admitting to feeling highly vulnerable.

Moreover, while 75% indicated they have a dedicated plan in place to respond to a cyber-attack, just 38% monitor their cyber security policy monthly. With so many conflicting priorities that schools have to manage, it seems although awareness is high about cyber security, actively reviewing and testing cyber strategies isn't undertaken as often as perhaps it should be.

It is no surprise to see malware (58%), phishing scams (51%) and hackers (40%) at the top of the list of schools' concerns. However, while such threats are a risk to schools, and can cause damage through file encryption and deletion, extortion and financial loss, their sophistication is likely to increase.

61%

of independent schools have reported experiencing a cyber-attack within the last five years.

It is no surprise to see...

58% malware

51% phishing scams

40% hackers

at the top of the list of schools' concerns.

Analysis

James Griffiths

Director, Cyber Security Associates

James Griffiths is an ex-Army Royal Signals Senior Operator, he started as a network engineer and then specialised in information systems as a Foreman of Signals, being deployed at home and overseas, often working with special forces in hostile environments. James spent his last five years of service working as an Operator providing cyber offensive capability to the UK government at the Joint Cyber Offensive Unit based at GCHQ in Cheltenham. James is exceptionally knowledgeable across the full spectrum of cyber capability and in threat intelligence.

It is concerning that just 39% of schools surveyed think they are a target for cybercriminals, especially when over 60% of them have experienced an attack in the last five years. In terms of cyber-threats, while the survey findings indicate that schools are aware of some of the more common approaches used by criminals, such as malware and phishing scams, there are a number of emerging threats that are less likely to be on the radar.

While some criminals may target the school itself, either as part of an extortion claim or by impersonating an existing supplier and attempting to change bank account details, others can look to other tactics, such as using the school as a medium of targeting a pupil's high net worth parent.

While cybercrime is a major threat for schools, with loss of income being one of the main outcomes, cyber security breaches – which can be accidental or intentional – also have the potential to cause reputational damage to a school.

The biggest weak spots in any security system are people. For example, a staff member could open a phishing email on their personal laptop at home, which could lead to that device becoming contaminated with malware. If they then do some work at home, and email files from their personal (and potentially contaminated) device, into the school network, then malware has the potential to enter the school's IT system.

The key to mitigating the damage is training. Crucially, this should not only be aimed at staff, but pupils too.

As the first generation of digital natives, today's pupils are very IT-literate. There have been instances where pupils have used a USB stick to upload and run their own operating system on a school computer, completely bypassing the school's IT and security system.

There was no malicious intent behind such actions, just a misplaced curiosity as to what was possible. However, this is symptomatic of the risks schools may be facing. Ideally the Computer Misuse Act would feature in every child's first IT lesson, as it sets out that if you do anything which changes what a computer is intended to do, you are not in a safe environment and will be breaking the law. Children will typically assume everything is acceptable unless they learn this is not the case, so it is important to make children aware of the importance of using a computer in a safe and controlled way.

Again, staff training is vital to this, and it is pleasing to see an increasing number of Continuous Professional Development (CPD) courses emerging in this sphere. However, there are other training and education options open to schools that may not seem immediately obvious. For example, a school may have access to a Police Liaison Officer, who could be able to arrange a member of the local police force's cybercrime division to come in and speak to pupils and staff.

In terms of mitigating accidental cyber breaches, there are a number of things a school can do. As well as training, HR policies can be put in place which prevent pupils and staff emailing work home to an unsecure computer or account. If a home computer or personal email account is infected, and that device or account is used to send work back into the school email system, that could be classed as a breach. Instead, schools could use a virtual private network (VPN) to create a secure remote access point, and ring-fence their system.

Any sensitive special category data, including information covering staff or pupil race, medical conditions, or sexual orientation, should also be encrypted. This will keep it safe, and prevent it from being leaked, if someone gains access to an IT system that shouldn't, or if a laptop is lost or stolen.

This should all be underpinned by a risk mitigation plan. While 75% of schools indicate they have a plan in place, how robust is that plan? Does it include regular penetration testing of a school's IT and security system, as well as a disaster recovery framework? Such an approach needs to be managed and all roles defined. Crucially, it should be routinely stress-tested to make sure the plans are fit for purpose.

However, no system is 100% secure. As mentioned, human error has the potential to undermine a security system if a device is left unlocked, or if someone unknowingly introduces a file from a contaminated device into the IT network, or opens a phishing email while on school grounds.

The best way for schools to future-proof themselves against cyber-threats is to prioritise the risk and to be prepared.

Analysis

Kristine Scott

Partner and Head of Education
at Harrison Clark Rickerbys

Kristine Scott leads the education team and focuses on issues relating to staff, pupils and parents – from sensitive dismissals to pupil exclusions, and parental complaints. Kristine has many years' experience of child protection and safeguarding, advising on the full range of issues including allegations against staff, peer on peer abuse, 'live' matters, as well as conducting retrospective reviews.

For more than 20 years, Harrison Clark Rickerbys has had a significant presence in the education sector, and we've gained a national reputation as a key player in the field of education law. Our work covers the full spectrum of legal affairs that affect educational institutions, and we provide clear advice to help solve their problems and achieve their aims and objectives.

Having provided legal counsel to independent schools for a number of years, I would say that cyber security is now in their top three concerns.

Just as the approach to safeguarding has changed massively in the last decade, cyber security is increasingly viewed by schools as something which needs to be scrutinised.

Key to this is ensuring responsibility is clearly designated to a number of individuals, rather than just one person. Nearly all schools will have a committee (usually at governor level) that looks at risk, and the assessment of digital risks should ideally be made a standing item on the meeting agenda. For example, if a piece of flooring was loose, it would be identified as a health and safety risk and swiftly dealt with. The same attitude and approach should be taken to cyber-risks. The fact that only 38% of those surveyed review their cyber resilience on at least a monthly basis is a concern, especially given that the Senior Leadership Team (SLT) at the majority of schools will look at other risks as part of day-to-day management functions.

In my own experience, cybercriminals targeting independent schools have gone down the route of convincingly posing as suppliers, with the ultimate aim of getting the school to change the payment details to the criminal account, and closing the account upon receipt of payment. This represents a financial risk to independent schools, and if the news about a successful crime were to be leaked, it could invoke reputational damage for a school.

Other serious examples of cyber-threats facing schools include phishing links, which are designed to obtain data – including financial data – through defrauding someone into disclosure; and ransomware, which aims to extort money via a ransom following the acquisition and encryption of data or files.

Despite having seen instances of targeted cybercrime, I would say the majority of 'day-to-day' cyber-risks facing the independent education sector are accidental or unintentional data breaches. While the introduction of the EU General Data Protection Regulation (GDPR) has made schools think about data security in a different way – and from my experience, most schools are good at getting the right policy documents in place – accidents do still happen.

This could be from a staff member forgetting to lock their device, or leaving it in a public place; to someone emailing the wrong document to the wrong person. It is also good practice to have separate log-ins for different parts of a school website, such as publicly-available pages and private areas, to ensure any content only appears in the intended place.

Many of these issues can be avoided through staff training and investing in robust data management processes.

If a serious data breach does occur, which is likely to harm the rights and freedoms of individuals, swift action must be taken. It needs to be reported to the Information Commissioner's Office (ICO) within 72 hours. Individuals whose personal data may have been compromised would also need to be informed, if the risk to their rights and freedoms is high. The ICO will then provide advice and guidance on how to manage the breach and learn lessons from it so that it does not happen again. This may cover what improvements to policy documents, security measures and training the school needs to put in place. Provided these are indeed in place, if a breach is reported immediately – and the school can provide evidence it has taken swift action to contain it – it could go some way to mitigating the regulatory response.

If an independent school is a charity, the school must consider reporting a serious data breach to the Charity Commission as a serious incident.

As well as encouraging good habits amongst staff, there are a number of emerging cyber-risks schools should be aware of, including the use of mobile device apps; both for teachers, and for pupils.

There have been a number of very popular teaching apps which have risen to prominence over the last year or so. While they provide an innovative way of encouraging pupil engagement, they should also be subject to rigorous testing by the school's IT department or team prior to use.

Ultimately, the key is finding the right balance between systems which protect, and those that hinder. If a system is restrictive, or too counter-productive, people will find ways of bypassing it; and that will defeat the purpose of them in the first place.

Schools have come a long way in recent years in acknowledging the cyber-risks posed by the modern working world, but as with safeguarding, we are not resting on our laurels.

Safeguarding your future

Both Cyber Security Associates and Harrison Clark Rickerbys have highlighted the importance of having robust data management systems in place, as well as undertaking and logging regular cyber awareness and security training sessions for all staff; and creating and testing robust risk mitigation plans which cover cyber security breaches.

However, what options are available to schools if they do suffer a serious security breach, even if all policies have been closely followed? One option which can provide a viable safety net against the emerging cybercrime and security threats is a cyber liability insurance policy.

Not only does a cyber liability insurance policy typically cover loss of income related to a cyber-attack, but it can also cover the cost of third-party experts should they be required, such as a forensic investigator or ransom negotiator. As such it can form part of a proactive cyber resilience strategy.

The survey revealed just 30% of schools surveyed as part of this report currently have a dedicated cyber liability insurance policy in place.

Should an attack happen, having insurance in place could be the difference between a cyber attack being well-managed, and resolved, or a difficult process ensuing.

Cyber liability insurance policies can also be supported by online reputational risk management policy. These can include the use of 'social listening' technology to monitor your school's digital footprint.

For example, with social media being used by pupils, parents and staff, it can be very difficult for a school to keep track of any negative messaging circulating online. Given the importance of flagging any negative comments which could harm the reputation of a school as early as possible, 'social listening' technology can provide 24-hour online monitoring for a school's name, and alert stakeholders to any imminent online reputational risks. On-going legal and public relations advice can also form part of a robust policy support package.

Only

30%

of schools currently have a dedicated cyber liability insurance policy in place.

Final thoughts

William Brunwin

Head of Travel & Schools
Endsleigh Insurance Services Ltd

From phishing and ransomware, through to accidental breaches and human-error, the cyber-threats facing independent schools are far-reaching and complex.

While many stakeholders are now aware of the significance of approaching cyber security with the same scrutiny and rigour as safeguarding, our findings show there does remain some disparity within the sector as to the collective vulnerability of independent schools to a cyber-attack.

However, by acknowledging the risks and ensuring all IT security systems are routinely assessed, monitored and tested, coupled with a robust staff and pupil education programme, schools can go a long way to mitigating threats. Supplementing such practices with a dedicated cyber liability insurance policy can help close the loop and provide a contingency plan if a breach does occur, and ultimately help to support a safe school environment for pupils, parents and staff.

For more information, please visit
www.endsleigheducation.co.uk
or call us on **0333 234 1198**

Let’s get started...

For more information on cyber insurance, or other insurances for your school, pupils or fee payers, please visit:

www.endsleigheducation.co.uk

or call us on 0333 234 1198

endsleigh