Technology and security challenges for independent schools

IT has become a critical component for most modern organisations, and ensuring delivery of an efficient, secure, 'customer focused', cost-effective and proactive service has never been more important, says *Simon Bulleyment*, director at Sibrossa Ltd.

Schools will have understood this point a long time ago, and no doubt it was well and truly proven during the pandemic, with the move to remote learning and almost total reliance on IT solutions.

The changing nature of IT

Gone are the days when IT was simply about 'keeping the lights on'. As schools put together their business strategy plans, they should also consider creating an effective technology plan. This should set out how IT will support the business plan and play a key role in achieving strategic goals, such as enhancing pupil learning experiences, improving communication with parents, providing better access to information and improving day-to-day processes and efficiencies.

Transforming IT from a purely operational function to a proactive and innovative service is no mean feat and requires staff with appropriate skills. A key role is a head of IT with a deep understanding of their school, the needs of and challenges faced by senior management and teaching staff and how technology can be used to address them. In medium and larger organisations, it is not unusual to see these roles having a title of chief information officer or chief technology officer, and a permanent position on the board.

So how can bursars work with their IT teams and heads to transform technology services? Step one must be getting the IT house in order, so that systems and infrastructure run optimally, supported in the best and most appropriate manner, all underpinned by an effective approach to cyber and data security. For most, the journey starts with the cloud.

The power of the cloud

Prior to discussing the cloud, it is worth describing a traditional approach to IT infrastructure.

This generally involves building one or more dedicated server rooms (with appropriate physical security and environmental controls), installing

Cloudy days ahead

A worrying change to ransomware has been the use of ***double extortion techniques***

Consider implementing a ***security framework***, such as the Government-backed Cyber Essentials (CE) and Cyber Essential Plus certification

Cyber insurance policies with ransomware cover can be useful but premiums are increasing

various systems (servers, storage, and network devices) and employing staff to implement and manage everything. For most organisations there has been a growing reliance on technology during the past two decades, involving numerous sophisticated applications and a requirement for them to be available on a near 24/7 basis. Aligned with this has been an ever growing complexity in underlying IT systems, an associated uplift in IT skills required to support them and a situation that started to become unsustainable. Thankfully, companies such as Microsoft, Amazon, and Google, came up with a solution – the cloud.

To try and simplify matters, it helps to think of the cloud as having three different levels (with level three generally offering the most beneficial impact:

- **Level 1** – servers are migrated to specialist hosting providers who look after the underlying infrastructure, storage, networking and provide ongoing support. IT teams simply look after server operating systems and the applications installed on them (this is referred to as Infrastructure as a Service, or IaaS).
- **Level 2** – as above and in addition, hosting providers look after server operating systems, leaving IT teams to focus on applications (this is referred to as Platform as a Service or PaaS).
- **Level 3** – as above but this time, hosting providers look after almost all the tech, leaving IT teams to simply configure applications for their own organisations. End users usually access them with just an internet connection and web browser on an any time, from any device, from any location basis (this is referred to as Software as a Service or SaaS)

Cloud transformation strategy

To provide a practical example of where SaaS has been transformational and almost universally adopted by IT teams, consider the following for email services.

Historically, IT departments would set up an application called Microsoft Exchange Server, it was complex, required specialist IT knowledge to manage and as it evolved, things only got worse. Even the simplest installation in a small organisation required multiple servers and hackers started to target poorly managed systems. Microsoft eventually provided the answer; Exchange Online – essentially an enterprise class email service on a SaaS basis. Complexity disappeared, security improved and end users could gain access to their email from a web browser, smartphone or after a few clicks from launching Outlook on their workstations.

Schools can achieve similar gains with the rest of their infrastructure once they have a cloud transformation strategy in place, outlining how systems and applications are to be migrated. If properly planned and costed, the following benefits are seen:

- a reduction in ongoing capital expenditure to replace servers and storage systems (and associated consultancy costs). This also moves IT spend from 'bursty' capital to predictable operational expenditure;
- a flexible and scalable IT environment with the ability to rapidly introduce new (or to grow existing) systems without costly and complex upgrades; ●➤

▼ Some Ransomware as a Service organisations have significant structure to them, with HR, recruitment, comms teams, and the provision of technical support services to those hiring their tools

- a reduction in the complexity of backing up systems/data as cloud-based systems include these features;
- an enhancement in security controls – cloud-based providers include sophisticated technical systems way beyond the financial reach of most schools;
- a reduction in the complexity and therefore support requirements for on-premise infrastructure;
- the increasing availability/uptime of IT services as cloud services are based on an 'always on' infrastructure with high levels of resilience and fault-tolerance; and
- the reducing complexity of 'on premise' server/comms rooms and enhancing disaster recovery (DR) – cloud services typically include features to ensure data is replicated to multiple datacentres.

While it will not be possible to move everything to SaaS from day one, the major cloud hosting providers offer a variety of IaaS and PaaS solutions for IT infrastructure. Many application vendors are offering, or planning to offer, SaaS alternatives. Once schools begin their cloud journey, it should start to free up IT time, enabling them to turn their attention from simply managing to harnessing the benefits from technology.

Cyber security and ransomware

Ask anybody in charge of IT security the question: "What is your biggest concern"? and at the top of their list, or very close to it, will be ransomware. It has been around for many years and gained prominence in 2017 with the WannaCry outbreak – a global attack that exploited a vulnerability with Microsoft Windows. It resulted in significant impact to countless organisations and, according to NHS England, affected 80 of its 236 trusts (either due to ransomware infection or IT teams proactively switching off devices).

Schools are just as at risk from ransomware as other organisations, especially with IT teams having to juggle seemingly opposing factors of keeping networks secure but also open and flexible to allow a variety of teaching applications and systems and for pupils to connect their own devices (a significant 'unknown' when it comes to security). Certain areas of the system will be holding sensitive data relating to staff and pupils (possibly including medical information), so there is much to lose if attackers gain access to or render it unusable.

Ransomware usually finds its way into networks via social engineering techniques, which dupe staff into opening infected email attachments or links. There will be very few schools not regularly receiving suspicious emails! However, attackers will also try other means, such as guessing or cracking passwords and logging in via remote access systems or exploiting vulnerabilities in externally facing servers.

X
ACCESS TO YOUR FILES AND PRIVATE DATA HAS BEEN LOCKED.
Enter your payment details to to gain access.
$300 USD / €250 EUR
Card Number
Exp MM/YY
MAKE PAYMENT
YOUR DATA WILL BE DELETED IN:
23:12:01
NOW!

While there is yet to be a follow-up on the same scale as WannaCry, ransomware and the attackers behind it are constantly evolving. When ransomware first became an issue, it generally required expert knowledge and sophisticated techniques to launch an attack. Shortly after the WannaCry outbreak, the UK's cyber security advisory body, National Cyber Security Centre (NCSC), attributed it as the work of 'state actors'.

Ransomware for hire

Ransomware as a Service (RaaS) is a relatively new concept, where developers of ransomware tools hire them out to less sophisticated attackers, with both parties taking a share of ransom payments. Some of these organisations have a surprising amount of structure to them, with HR, recruitment, comms teams, and the provision of technical support services to those hiring their tools.

However, the most worrying change to ransomware has been the use of double extortion techniques. Previously, if an organisation became a victim of an attack, as long as there was an effective backup strategy in place, the ransom note could be ignored, data restored and operations continued. However, many attacks now incorporate an initial phase of copying victim's data to an external location prior to it being encrypted (referred to as 'data exfiltration'). The ransom note will then demand payment not only to recover data but also to ensure it is not released to the public. Many schools will be alarmed at the thought of sensitive pupil data being leaked on the Internet as the reputational, financial, and regulatory risks will be significant.

Minimising risk

While being attacked might seem like an inevitability to some, there are ways of minimising the risk. Generally, when attacks are successful, it involves multiple process, human or technical control failures. It is rare for only one thing to have gone wrong!

At the top of the list should be ensuring that IT teams have put appropriate controls in place, that they are working effectively and, just as importantly, are tested on a regular basis.

The National Cyber Security Centre (NCSC) provides excellent guidance for senior management and board members, explaining what ransomware is and the types of questions to raise with their IT teams **https://www.ncsc.gov.uk/blog-post/what-board-members-should-know-about-ransomware**

They also provide practical resources, help and even cyber security training content for schools **https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools**

Schools should also consider implementing a security framework, such as the Government-backed Cyber Essentials (CE) and Cyber Essential Plus certification – a prescriptive set of controls designed to protect organisations from the most common form of cyber-attacks. CE is also a great way to demonstrate to parents that you take cyber security seriously **https://www.ncsc.gov.uk/cyberessentials/overview**

Cyber insurance policies with ransomware cover can be useful in the event of an attack and historically, insurers have generally paid out when required. However, with the ongoing rise in the number of attacks, premiums are increasing, restrictions on cover are being applied and insurers are demanding that organisations have effective security controls in place.

Cyber security improvement should be an embedded process within all schools. Risk assessments should be kept updated to deal with ransomware and other types of cyber threats. Once in place, a plan should be created to prioritise the implementation and improvement of controls, and associated spend.

How to get help

Having covered a number of challenges in this article (the changing nature of IT, cloud adoption and dealing with sophisticated and evolving cyber threats, such as ransomware) how can schools tackle them?

While some will already have effective IT managers or directors in place, for others there might be less certainty. In both circumstances, it may be useful to engage outside expertise to either validate existing or introduce new skills. Bursars might ask the following questions about their IT systems and teams:

- Is the structure of the IT team appropriate for our school and do staff have the correct skills?
- Do we have an effective IT strategy in place? If not, where do we start?
- How far along the journey are we with our cloud adoption and is there a strategy?
- How effective are our cyber security controls and do staff have relevant skills and experience?

Various organisations and consultants can provide independent and expert advice. If engaging with them, questions to ask could include:

- Have they got experience of working with independent schools?
- Have they got experience of writing IT or cloud transformation strategies?
- Have they got practical experience of leading and managing cloud transformations?
- Do they have appropriate cyber security skills and experience

IT can be a daunting area for bursars to deal with, particularly if they do not have the background experience, it can be all too easy to concentrate efforts in more easily understood areas, such as finance and HR. However, given the increasing criticality of IT (and associated spend), it has never been more important to take stock of the service being delivered to your school and to ensure it is fit for current and future needs.

Author
Simon Bulleyment
director, Sibrossa Ltd

W **www.sibrossa.com**