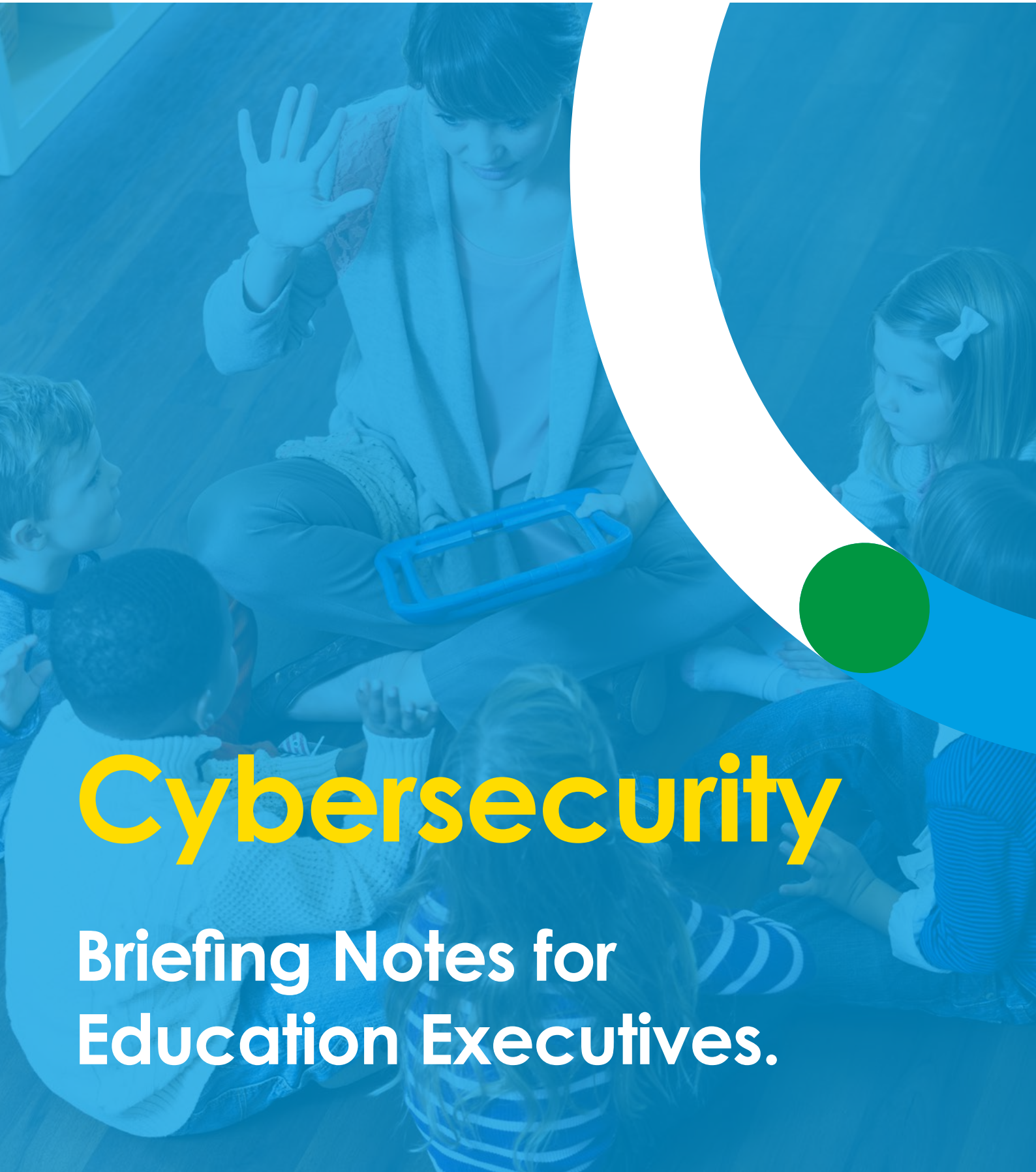
our learning CLOUD



Cybersecurity

Briefing Notes for Education Executives.

Context

In March of 2021, the National Cyber Security Centre (a part of GCHQ responsible for making the UK a safe place to live and work online) alerted that "[…] an increased number of ransomware attacks have affected education establishments in the UK, including schools, colleges and universities"[1] and beefed up their guidance for the education sector[2].

This alert was itself an update of a similar NCSC Alert from September 2020 that reported several ransomware attacks against education providers the previous month[3].

Looking to the remainder of 2021, cyberattacks are predicted to increase and become increasingly sophisticated[4], with the FBI describing ransomware as the fastest growing form of cyberattack[5].
In this changing landscape, education organisations of all sizes need to take action to avoid joining a rapidly growing list of high[6] profile[7] victims[8] both in the UK and more widely[9].

What is the risk and impact of cybersecurity?

There is a perception that because cybersecurity contains the word 'cyber' it's an IT and systems issue. The sort of thing that you perhaps add to the job description of an IT manager to make sure there is "cybersecurity in place at all times".

In a survey last year, almost 80% of IT professionals were concerned about the perils that businesses face[10]. If something is worrying them that much, then the leadership of any responsible educational organisation should have cybersecurity up there with safeguarding as a key responsibility which is driven from the top down.

The biggest reason that education leaders should pay attention to cybersecurity is the potential impact of it. While cybersecurity itself is obviously related to technology, the effects very much aren't.

Aside from the impact on learning, which we'll come to, depending on the nature of the cyberattack the impact could be financial and lead to significant reputational damage. If a cyberattack results in loss of control of your data and that loss of control has the potential to cause "physical, material or non-material damage" to any student or employee then there is also a requirement to report a data breach[11], which could lead to further collateral impact such as GDPR, safeguarding and other compliance failures. That loss of control includes accidental or unlawful destruction of data[12], not just having it stolen or disclosed. The same collateral risks apply to the loss of financial records.

Related Links

1. More targeted ransomware attacks on UK education - NCSC.GOV.UK
2. NCSC beefs up support for education sector after spate of attacks (computerweekly.com)
3. Cyber alert issued after attacks on UK academia - NCSC.GOV.UK
4. www.wired.co.uk/article/ransomware-trends-2021
5. www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
6. Ransomware attack on London schools highlights warnings (computerweekly.com)
7. Blackbaud Hack: Universities lose data to ransomware attack - BBC News
8. Cyber threat to disrupt start of university term - BBC News
9. Ransomware halts classes for 115,000 Baltimore pupils - BBC News
10. Source: ESG Research Report, The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies, June 2020
11. IT Governance Blog: school data breaches - to report or not to report?
12. Art. 4 GDPR – Definitions | General Data Protection Regulation (GDPR) (gdpr-info.eu)

Are we really a target?

Given some of the highest[13] profile[14] serious[15] cyberattacks[16] (some twice[17]) in the past few years globally, you'd be forgiven for thinking that education is a relatively low priority target. After all, if you're not handling money then is there really any interest for cyber attackers?

The answer unfortunately is yes, you are a target in at least two ways.

Firstly, there is the plain statistical risk. Cyber attackers don't always target specific organisations and many just run applications that scan the Internet looking for any organisation unfortunate enough to have misconfigured security in some way or forgotten to update their firewall. Where they find a vulnerability like this, the applications then do the breaking in for them.

This is a common approach especially for ransomware where, once inside your network, it can spread from computer to computer encrypting all the data it can find. It's relatively low effort for a cyber attacker, but also fairly low yield because it's indiscriminate. For the affected organisation the impact is still typically serious.

Secondly, there is the targeted attack. The education sector processes a wealth of personal data[18]. Aside from staff pay and bank accounts, there is also a huge dataset set of parental names, addresses, emails, and phone numbers that comes complete with contextual data like children's names which helps make an email or text message scam look considerably more authentic. Then there are your detailed safeguarding records, social care indicators, other sensitive fields, and perhaps even the passwords for your cashless payment platform or a school's online banking credentials.

This type of attack can be silent, where the first you know about it is when parents start getting odd text messages, or it can be accompanied by a ransom demand threatening to publish the data online.

Students and learning delivery

So far we've not considered one of the more unique impacts on education – the impact on learning and outcomes. Especially in the current blended learning climate, how would your education provision and student outcomes be affected if any of the following happened:

- Your email services became unavailable;
- Your MIS server was lost, or remote access had to be blocked;
- Your students couldn't log in to access their learning resources;
- Coursework in your care was encrypted or otherwise made inaccessible;
- Staff laptops, interactive whiteboards and office PCs become inaccessible;
- Your phone system couldn't be used.

These are things that can and do already happen at the best of times, and when they do it's usually one of them for a day or so at worst. It would be disruptive but ultimately recoverable.
Thinking about these in the context of a serious cyberattack though, what about all of them happening at the same time? How long would it take to rebuild and redeploy each of those services and restore the last backup? What if the last backups contain whatever the cyber attackers used to get in and it happens again?

Related Links

13. Experian Data Breach Hits Estimated 24 Million Customers - Infosecurity Magazine (infosecurity-magazine.com)
14. Equifax Data Breach Settlement | Federal Trade Commission (ftc.gov)
15. SolarWinds hack explained: Everything you need to know (techtarget.com)
16. Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom - Bloomberg
17. Experian hack exposes 15 million people's personal information | Experian | The Guardian
18. Why do higher educational institutions keep getting hacked? | News | Chemistry World

Changing risk of cyberattacks, and how do they get in?

The events of 2020 and early 2021 have had a significant benefit to cyber criminals. In the mad rush in the first lockdown to get some sort of remote working and education delivery provision available, new risks were introduced, and at the time the priority was firmly on operational delivery. There were undoubtedly a few technical decisions made with a view that "we'll need to come back shortly and do this properly."

In technology circles we call this the "attack surface", the things that you have which could be used to enable a cyberattack. In those same technical terms, the real big shift in 2020 was reducing the influence of a thing called "perimeter defence" – where you have 'inside your network', which is somewhat safe, and 'outside your network', which is not safe. The seismic move to home working and home learning eroded the ability of perimeter defence to do its job and, a double whammy, because extra holes were made in what was left of the perimeter defence so staff could remote into work computers.

As a result, most education organisations now have numerous employees and students accessing their network from external devices that aren't necessarily managed, sanctioned or up to date, and doing so without necessarily having full training in how to keep their devices safe and free of risk.

For cyber attackers, this is gold.

The most common entry points for cyberattacks are either through weakness in technology or weakness in people:

- **VPNs** – either through compromised or weak passwords, or through a failure to keep the VPN hardware or software updated under subscription.
- **Remote desktop access** – especially when those services are set up without VPN without using a secure cloud platform. Some ways of setting up remote desktops are trivially easy for cyber attackers to break into, and there are always ones with weak passwords too.
- **Weak or compromised passwords** – organisations that don't user two-factor (or multi-factor) authentication aren't protected from cyber attackers who have obtained or guessed a real username and password.
- **Email scams** – known as 'Phishing attacks' or social engineering attacks. These are emails that typically either encourage a user to run a program (for example disguised ransomware) or sends the user to a fake login page that sends their username and password to the attackers who then try to use it. They often take the form of an urgent call to action or offer some form of social intrigue like the first half of an email from somebody they know, so that the victim acts before thinking it through.
- **Newly discovered software or hardware flaws** – hackers, both good and bad, spend a lot of time looking for flaws and vulnerabilities in prevalent software. When they find one it is called a "zero-day", because that's how many days your organisation has to address it. A good recent example is the major global impact of four zero-days found in Microsoft's Exchange email server that enabled cyberattacks[19] on 7,000 UK email servers, including ransomware encryption[20]. Office 365 was not affected.
- **Lateral movement and privilege escalation** – technical terms, but it means that once in the door, a cyber attacker will run applications to look for other computers they can break into, so they can establish a bigger foothold and cause greater impact. They may then also use other security flaws to obtain administrator permissions so they can deploy ransomware more deeply or delete audit logs and backups.

Related Links

19. Microsoft vulnerabilities exploitation - updated advice - NCSC.GOV.UK

20. 2021 Microsoft Exchange Server data breach - Wikipedia

Addressing the cybersecurity threat

The NCSC provides some excellent[21] guidance[22] on mitigating malware and ransomware attacks, which is one area of cybersecurity, but their guidance and the risks you need to consider should be interpreted in an education context which just isn't as simple as a small- or medium-sized business.

As an education provider the cybersecurity elements of your overall digital strategy should cover:

- **Working with knowledgeable service providers who specialise in education**
  Education is a very specialist space and experienced cloud service providers in the education marketplace have specialist knowledge and experience in helping multiple organisations migrate safely to the cloud. While some of these are just commercial resellers and managed service providers, others like Our Learning Cloud have the very credible provenance of being formed from a forward-thinking academy trust who have already done this for their own 20,000 users across 36 academies.

- **Training staff in securing blended and remote learning**
  Cyberattacks commonly happen by exploiting weaknesses in people. As the cybersecurity landscape continually changes, make sure your staff are upskilled not only to deliver a safe and high-quality learning experience regardless of where they or their students are, but also in how to identify potential cyberattacks, avoid falling victim to them and how to educate their students to protect themselves too. As a Microsoft in Education Global Training Provider, Our Learning Cloud have hands on experience in training their own teaching staff across their academies and transforming their learning from special measures to Microsoft Showcase Schools.

- **Using well established cloud platforms for your core systems**
  Cloud providers like Office 365 and Google Workspace have dedicated security teams that work together and in competition to proactively find and close security weaknesses, assuring end users the safest and most protected experience. They also handle such significant volumes of email that they can proactively detect and block new email threats emerging. Our Learning Cloud makes use of carefully selected services like Azure Active Directory, Azure Monitor Logs and Azure Security Center, a collection of security services and capabilities that provides their dedicated teams with a simple and fast way to understand what is happening right now in their Azure deployments.

- **Reducing DIY and in-house IT**
  There is an inherent limit to what you can realistically achieve with the resources and budgets you have available. Cybersecurity is such a large area that it's hard for a small organisation to keep up, and that's before you get into things like availability and disaster recovery plans if your datacentre is compromised by ransomware.

  Cloud services offered by the likes of Microsoft Azure are designed to significantly reduce not only the risks of cyberattack through both passive and proactive means, but also to reduce the knock-on impact of anything that does get through. Our Learning Cloud uses Microsoft Azure data centres to ensure that education and organisation services are always available from multiple locations within the UK, with automated security patching by Microsoft ensuring that zero-day attacks are prevented almost immediately, and the overall probability of cyber threats is reduced.

Related Links

21. Mitigating malware and ransomware attacks - NCSC.GOV.UK
22. More targeted ransomware attacks on UK education - NCSC.GOV.UK

- **Use cloud service suppliers audited by a Crest Approved cybersecurity specialist**
  The Crest Approved[23] scheme provides access to highly skilled, knowledgeable, and competent information security companies that meet a detailed independent certification and follow industry best practices. Your cloud service suppliers should be using those Crest Approved companies provide independent audit and testing of their cybersecurity measures and technical processes, along with guidance and detailed technical engagement on how to continually improve the safety and security of services as new cyberthreats emerge. Our Learning Cloud works very closely with their Crest Approved security partner Equilibrium, an information security and assurance organisation who specialise in the removal of cybersecurity risks.

- **Overall governance and monitoring of your IT estate**
  Detecting suspicious activity across your digital estate is a key part of protecting against cyberattack, not only in spotting attempts to break into your network but also in detecting activity that indicates a successful break-in is trying to spread. Centralising this monitoring is the only way to spot what are otherwise small and innocuous activities that only betray themselves when seen together all at once in context. Our Learning Cloud uses a Cloud Access Security Broker (CASB) that provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all of their Microsoft and third-party cloud services.

- **Plan for an incident**
  Like any other material risk to your organisation, prepare and practice your response to a cyberattack. What will your response be if a member of staff reports seeing a ransomware message while logging into their remote desktop? Will they even know to report it? How will you isolate the threat and prevent it spreading? How will you know if there is further suspicious activity in your network? How will you identify which systems to clean down and redeploy from backups? How will you know that you have the relevant backups and that they're working? How would you handle a major event that meant you had to stop multiple critical IT services across your organisation? How would you staff such a major rebuild activity and how long would it realistically take?

  Our Learning Cloud is built on the experience of seasoned education and IT professionals, with the support of leading cloud infrastructure and security suppliers, and has the experience to help you build a strategy that not only answers these questions but also encompasses the bigger picture writing your overall future proof digital strategy.

Related Links

23. CREST (crest-approved.org)

Our Learning Cloud
Greenwood House
Private Road No 2
Colwick Quays Business Park
Colwick
Nottingham
NG4 2JY

w ourlearningcloud.org
e info@ourlearningcloud.org