CONTENTS

Freshers' week

Few would dispute that the last 12 months has been the most difficult period for the education sector since World War 2. With the pandemic shutting students and staff out of universities colleges and schools for months, the sector has had to struggle with the same financial and logistical challenges as every other part of the economy.

Less noticed is that education has had to cope with a second pandemic of cybercrime, which after years of steady growth has started causing damage that might in less unusual times be considered a crisis. Cybercrime doesn't usually put lives at stake, but it is increasingly risking livelihoods, as well as storing up data loss problems that could seriously affect many of Britain's young people for years into the future.

An illustration of this is was what happened to the University of Portsmouth in April 2021, when it was forced to suspend IT services for 12 days after a severe ransomware attack. A deliberate element of the attack was that it unfolded only days before the start of the University's summer term, adding to the pressure on defenders to pay the ransom.

The University of Hertfordshire experienced an identical attack in the same month, again timed to coincide with the beginning of term, which caused teaching to be suspended. This followed a spate of attacks in the last year, including one against the University of Newcastle in which data was also reportedly stolen.

And it's not just higher education that has come under the cosh of the extortion gangs with a series of attacks reported against schools, which included several in Nottinghamshire, against laptops belonging to an education trust in Leicester, and an attack on 50 primary and secondary schools in London which left 36,000 pupils without access to email at a time remote learning. These incidents are only a taster of the huge wave of cyberattacks the global education sector has experienced in recent years, the majority of which are not reported.

The risk is now so significant that in September 2020 the National Cyber Security Centre (NCSC) issued a warning to the sector after a large spike in attacks on institutions a month earlier. The NCSC's assessment of the risk is not simply bureaucratic – it is to this Government agency that universities and schools often turn for support and advice when the cybercriminals strike. This followed a 2018 pen test by a Joint information Systems Committee (Jisc) team which found it was possible to gain access to 100% of university networks using simple phishing attacks.

During a May 2021 education sector webinar run by Sophos, 90% of the 158 respondents agreed that ransomware was now their biggest cybersecurity fear, with only 6% citing credential theft. When asked whether they agreed that students and staff were the weakest link in their security, 93% either agreed with this or thought it was more correct than incorrect.

Data loss

The direction of travel here is not good, with the number of disruptive incidents growing year-on-year in an industry where any interruption of service can cause lingering academic problems. Beyond that lies the sheer cost of incidents for institutions where money is always in short supply and the sums demanded in ransoms keep rising. In other parts of the public sector such as UK local authorities, recent attacks on Copeland, Redcar and Cleveland, and Hackney, the sums involved in clean-up ran into tens of millions, requiring direct support from central government. Clearly, attacks on universities have drained resources but the potential for costs to spiral beyond their means is now a real possibility.

But the biggest worry of all is arguably the one not always associated with ransomware, namely data loss. Until recently, ransomware attacks were defined by an MO in which files, applications and sometimes backups are encrypted with ransom required to retrieve the keys. In the last year, this has rapidly shifted to a double extortion technique where the threat to release sensitive stolen data is being deployed as the primary incentive to pay. The Sophos State of Ransomware Report 2021 (see box Is paying ransoms a good idea?) uncovered evidence that in a growing number of incidents this might now be the primary motivation with the file encryption and on-screen messages simply a way of grabbing defenders' attention.

Data target

The issue of ransomware data loss can be ambiguous. Is a ransomware attack even a notifiable data loss incident or not? Officially, ransomware does not necessarily breach a disclosure threshold unless an organisation believes that personal data has been stolen. But as many experts have pointed out, if attackers can reach databases to encrypt them then stealing them is a small additional step, regardless of whether the evidence indicates this. Add to that the increased targeting of data as part of double extortion and data loss should be assumed by default in every ransomware attack.

The idea of schools and universities losing control of the data of their staff and students should be of societal concern. Once data is lost, it cannot be retrieved and is gone forever, which in the case of young people will be many decades. Identities cannot be changed and are now likely to be traded for years to come between cybercriminals or malicious nation states. No matter now inured people become to the idea of disruptive cyberattacks, the potential long term implications of the loss of personal data should be a huge motivation to act now.

Why education?

A July 2020 freedom of information study of 134 UK universities by B2B agency TopLine revealed that of the 105 which responded, 35 admitted being affected by ransomware since 2013, most since 2017. Many attacks were not successful although, possibly significantly, 43 universities refused to confirm whether they'd suffered an attack or not. One university, Sheffield Hallam, admitted to an extraordinary 42 attacks. The wide variation in replies – including some large universities that claimed they'd never recorded any incidents – raises the possibility that some are either not recording incidents with enough rigour or would prefer not to discuss the issue for fear of becoming a target in future.

Although the education sector is far from the only one to experience bad cyberattacks, it is interesting to attackers for reasons that predict attacks won't stop soon.

Universities are full of IP

It's been known for years that certain nation states aggressively target intellectual property and research data, with universities one of the obvious places to get hold of this. A possible example of this is the February 2021 attack on the University of Oxford's Division of Structural Biology (Strubi) in search of Coronavirus research data. Possibly stolen to order, news of the incident only became public after a news report. The attack was customised enough

An expanding attack surface

Universities and schools have become hugely dependent on computing infrastructure to function, as underlined by studying the range of University of Hertfordshire systems disrupted by the ransomware attack discussed above: university logins and password services, Microsoft 365 access, Teams, Zoom, the backbone network, campus Wi-Fi, VPNs, data storage, staff and student email, and university applications. This mix of student-facing services is now typical, any one of which can cause pain if it becomes unavailable. Universities are probably reluctant to lock public-facing infrastructure down as might other industries for fear this will compromise the sector's commitment to openness and accessibility.

Limited resources?

It's a mistake to generalise about the resources available to educational organisations. In the case of some larger and better funded universities they might be well resourced enough to block attacks before they do damage. But ransomware is an industry in which the devil takes the hindmost; many smaller institutions and schools have little experience of being targeted and will not have invested as heavily or at all. To ransomware attackers, they make a perfect target. Where tight budgets can really bite is its effect on resilience. Once a ransomware attack starts, many organisations find they lack the extra resources needed to recover quickly. The Sophos State of Ransomware Report 2021 found that 30% of education respondents admitted to security weaknesses that might aid ransomware attacks, the joint highest sector along with local government.

Building better defences

The payments demanded by ransomware attackers have spiralled in the last three years, with the biggest attacks leading to reported multi-million dollar pay-outs. Some believe the growth of ransomware insurance as a way of underwriting ransoms could even be encouraging this inflation. Regardless of whether this is true or not, for most organisations a much bigger cost will always be the price of putting their network back together after an attack.

How can organisations defend themselves from this fate?

One place to start is the Sophos Active Adversary Playbook 2021, which analyses real-world incident response investigations, 61% of which were of ransomware. Several pattens emerge from this, including that the average dwell time of attackers (the time it takes before an attack executes or is detected) is around 11 days. Although ransomware is shorter than this, it still means that by the time a ransom note appears on a screen the malware has probably been inside the network for a week or longer.

RDP + authentication

A second pattern is that Remote Desktop Protocol (RDP) played a part in 90% of attacks, both for external access but also, importantly, to achieve lateral movement around a network. RDP is often presented as a threat when external -facing connections are not secured; the evidence shows that internal RDP access can also be dangerous because it allows attackers to spread further after a compromise. Other popular routes into an organisation include the exploit of a public-facing application, a phishing attack on credentials/account compromise, and – intriguingly – a supply chain compromise via a third party.

The standard advice from this is to minimise the attack surface on those routes, carefully managing ports such as RDP, mandating multi-factor authentication on all accounts, especially privileged ones. Working from home access for staff should be over a VPN as a minimum while taking care to ensure it works reliably from the client end.

Offline backup

Beyond that, offline backup is an important insurance, with tape backup a good option for doing this. This can be on-premises or via a cloud service although assurance needs to be sought regarding the nature of the latter to ensure it meets guarantees about security and the ability to reinstate data within certain timescales. All backup accounts must be protected using a layer of authentication.

Penetration testing

Penetration testing offers a good baseline for every network's security but must be done regularly to take account of new weaknesses that appear over time. The first page of a pen test report will mention software vulnerabilities, which will offer insight into how good a job the organisation is doing in terms of patching priorities. A red teaming exercise is better still because it tests the whole of an organisation's defences - including its employees and physical security - although this is likely to be beyond the budget of organisations in the education sector.

Incident communication

During an incident, normal email communication might either be unavailable or have been compromised by attackers. It is essential, therefore, that organisations agree a backup channel in advance of an incident, which should be accessible by IT admins and management. Mobile apps such as Signal of WhatsApp meet this requirement. Organisations can improvise this channel during an incident but setting it up in advance will save valuable time.

Incident response skills

It is important that organisations objectively assess whether they have the right inhouse skills to cope with a serious ransomware attack. If they don't, they should firstly contact the Government National Cyber Security Centre (NCSC) Incident Management (IM) team. Depending on the nature of the attack, they may be advised to bring in a third-party incident response company. It is a good idea to have researched and talked with these organisations in advance of an attack because you don't want to be negotiating in the middle of a breach.

Choosing a security partner

There will be emergencies situations when an organisation needs to reach out for help. In the case of ransomware, it is critical that the managed services provider (MSP) or partner has extensive direct experience of ransomware attacks, including the tactics, techniques, and procedures (TTPs) of the common campaigns. This soft of deeper knowledge is absolute critical when it comes to finding how the compromise happened and making sure a threat has been removed from the network.

Incident response – what to do

The member of the IT team receives a confirmed report that a ransom note has appeared on the screen of an employee. Now what? It's the worst-case scenario but it highlights the first and most important part of every response plan – good training and careful pre-planning. That person must know exactly what to do, and not do, and in what order. "Organisations typically plan to call for external help at some point, but in the seconds and minutes after it becomes clear that ransomware has reached one or more machines, the organisation will usually be on its own," comments Sophos director of public sector, Jonathan Lee. His recommendation is to start with a simple checklist, which includes:

1. Immediately communicate with other members of the IT team as well as employees, bearing in mind that the email system might be compromised, for example by using phones or a separate mobile messaging platform.
2. The affected system should be shut down and physically disconnected from the network after identifying the specific type of ransomware involved. Other non-essential endpoints should immediately be shut down and isolated, as should Wi-Fi access points and the employee VPN.
3. Staff should analyse how big the attack is, checking for reports on other PCs, servers, shared drives, and cloud backup systems. This might require looking at logs and checking RDP for access or weak accounts.
4. A check should be run on core resources such as the integrity of Active Directory controllers, the email server, and major applications/servers.
5. The response plan will mention the need to start reinstating secure backups to machines inside VLANs ASAP to minimise disruption.

Threat analysis and response

"This checklist will differ between organisations and is only a guide. Defenders still need to assess the extent of an attack and trace it back to its root cause," says Lee. "What counts here is to employ security products that work in concert to cope with every element of a ransomware attack." Using Sophos as an example:

1. On the endpoint where Sophos CryptoGuard monitors Window PCs, servers, and Macs for unusual file encryption, providing rollback where necessary.
2. Intercept X with endpoint detection and response (EDR) additionally detects ransomware attacks that may have gone unnoticed and search for indicators of compromise across the network.
3. Where services are needed, Sophos offers Managed Threat Response (MTR) and Rapid Response offer 24/7 automated and manual threat response actions understand and mitigate the most extensive ransomware attacks. These are also useful for post-incident analysis such as tracing an attack's origins.
4. The Sophos XG firewall with integrated Intrusion detection, the ability to lock down RDP (a common target for ransomware), and the ability to segment the network into VLANs to limit the spread of ransomware.

Getting ahead

Incident response always begins with preparation ahead of time. This starts with threat intelligence to become acquainted with the real-world ransomware campaigns circulating at that moment in time. Says Lee: "All ransomware encrypts and steals data but knowing the enemy is about understanding the differences between one kill chain MO and another." He also recommends adopting the approach set out in the Sophos Incident response plan:

- Identify critical assets (i.e., admin accounts) and establish response workflow.
- Nail down these with maximum authentication and careful patching.
- Run fire drills to test response.
- Implement access control.
- Invest in high quality investigative tools.
- Conduct awareness training (for example Sophos Phish email attack simulation).
- Hire an MSSP as backup after assessing what the provider will and won't do, and on what timescale.

On the final point: "Even organisations with an inhouse IT team will still have gaps in their coverage, for example at weekends and holidays. Good MSPs will offer a depth of knowledge of specific ransomware attacks and be experienced at incident response," says Lee.

Is paying ransoms a good idea?

Ransomware is costing victims more and even those who pay ransoms rarely get all their data back. These are two findings from the Sophos global State of Ransomware Report 2021,which questioned 5,400 IT managers from 30 countries, including 499 in education. The headline finding was that this type of attack has become a universal experience affecting all sizes of organisations, business types and countries. In total, 44% of education respondents said they'd suffered an attack in the previous year, one of the two highest percentages across all sectors. Of organisations whose data was encrypted, 32% paid a ransom, up from 26% in 2020, with education organisations among the most likely to do so at 35%. A significant finding is that even those who paid only got back an average of 65% of their data, with only 8% retrieving it all. Meanwhile, 57% got their data back using old-fashioned backup in a year when remediation costs in the UK (downtime, staffing, ransom costs) doubled to $1.96 million per incident. Conclusion: if ransomware attackers visit your network every penny spent on detection, remediation, backup, and incident response will pay for itself within hours.