SOPHOS

RESPONSE TO THE NCSC AND LGFL CYBERSECURITY AUDIT 2019

A Sophos white paper June 2020

In March and April of 2019,the NCSC (National Cyber Security Centre, part of GCHQ) and LGfL (London Grid for Learning) conducted a cybersecurity audit looking at security practices in U.K. schools. The report aimed to not only build a picture of how cybersecurity is currently managed in these organisations, and show the impact cyber threats are having on teaching establishments in the U.K., but also provide practical solutions to these threats.

Sophos in schools

As an IT security solutions company with a large customer base in the U.K. education sector, Sophos wanted to follow up on this document with some specific guidance regarding our security solutions. We work in partnership with a number of trusts, councils, and grids (including LGfL) and as such, many U.K. schools already have access to some or all of the Sophos solutions available to help mitigate these threats.

What the audit tells us

First and foremost, it's evident from the findings of the report that there is a real cybersecurity risk to schools: *the vast majority of schools (83%) had experienced at least one of the types of cybersecurity incidents asked about.*

83%

of vast majority of schools had experienced at least one of the types of cybersecurity incidents asked about.

At a high level, the report highlights that schools are putting a concerted effort into protecting themselves against these cyberattacks. Many have a cybersecurity plan, and nearly all deploy antivirus software, have a firewall, backup their data, and keep up to date with patching. However, when we start to look at more specific measures that could be used to reduce the attack surface available to malicious actors, the number of schools employing these measures starts to tail off.

The report also highlights that email-based attacks are the most prevalent, and that there is a gap in cybersecurity training and adequate planning for cybersecurity incidents should they occur.

How Sophos can help

Based on the findings of the report, we felt we should focus on the following areas.

Successfully deploying advanced measures to reduce the attack surface

As described above, nearly all schools have antivirus software and firewalls deployed. But many are not taking further steps to restrict the use of devices and applications, managing mobile devices or deploy encryption. Sophos provides a centrally-managed solution that can be used to do all of the above.

Email security and end user training

Given that fraudulent email was the most often experienced cybersecurity incident across the schools audited, and that only a small percentage of schools had offered training to non-IT staff, we wanted to highlight how our solutions can also help in this area.

A note on homeworking

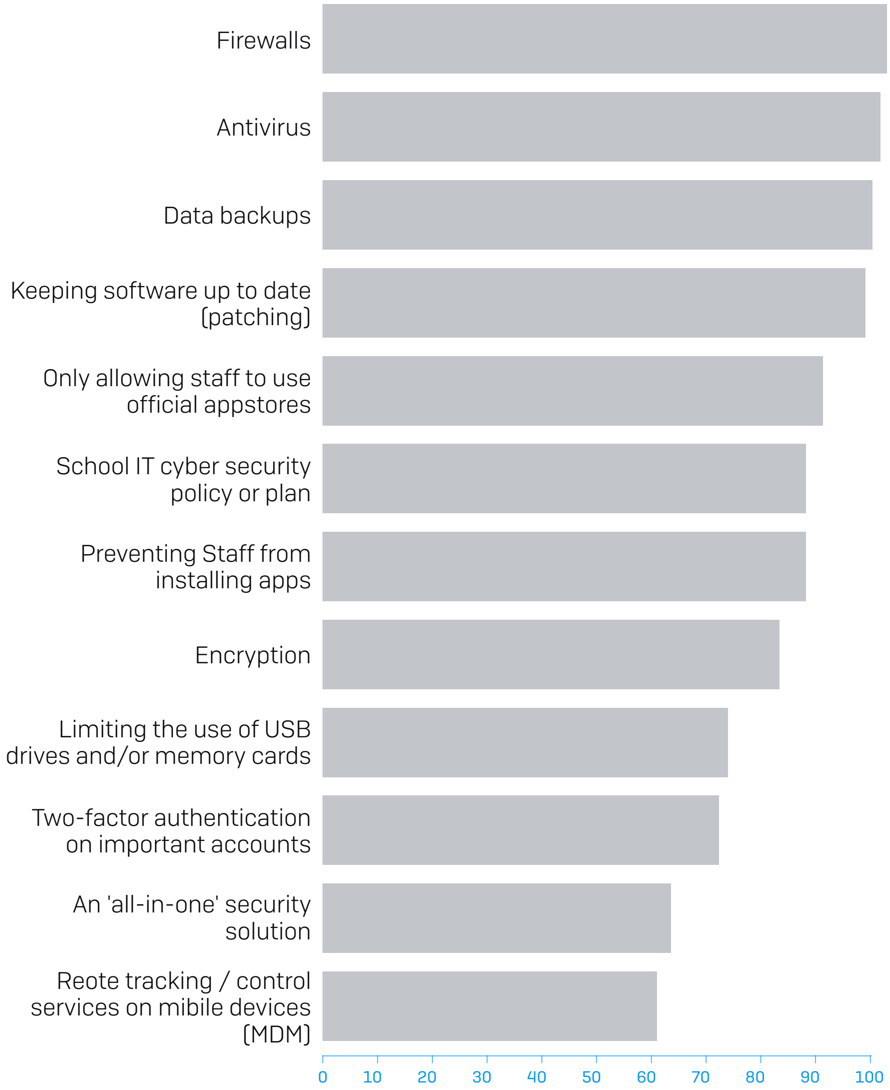
Given the timing of our response, we also felt it wise to include some further information around home working.

Successfully deploying advanced measures to reduce the attack surface

The audit shows that nearly all schools have antivirus and firewalls deployed, and yet, according to the data, many are not utilising these technologies or employing other solutions to reduce the attack surface available to hackers.

Many are not limiting the use of USB drives, managing encryption, or deploying mobile device management (MDM).

Do you have the following measures in place in your school?
(% of 432 schools answering yes)



National Cyber Security Centre, Cyber Security Schools Audit 2019

We believe that in most instances there are multiple reasons for this.

1. Complexity of managing multiple solutions/lack of granular control in older technologies
2. Cost of buying and maintaining multiple solutions
3. Use of unmanaged (BYOD) devices among staff without adequate protection or controls

Sophos have always argued that complexity is the enemy of good security and as such Sophos Central has been designed to offer easy policy management for antivirus, encryption, device control, application control, email scanning and filtering, phishing simulation, mobile device management, firewall, web filtering, and reporting via a single pane of glass. Today, 70% of our education customers are using this console.

Sophos Endpoint Protection has always provided the ability to limit the use of peripherals (such as USB devices) and applications. Sophos Central is now aware of your users (via an AD sync) and as such offers the ability to easily configure a user-based policy, which makes the restriction of these devices and applications far more usable. Even our base level of protection allows admins to restrict the use of USB and other devices to a certain user of user group and you can even go as far as limiting the USB device type right down to a specific ID if needed.

Sophos Central Encryption provides easy management for encrypted devices using either BitLocker or FileVault on Mac. The solution gives the ability to remotely manage the encryption including providing audits and key recovery.

Sophos Central Mobile Device Management provides control for Windows 10, Chromebooks and macOS devices, allowing for either full device management of just a container for BYOD devices.

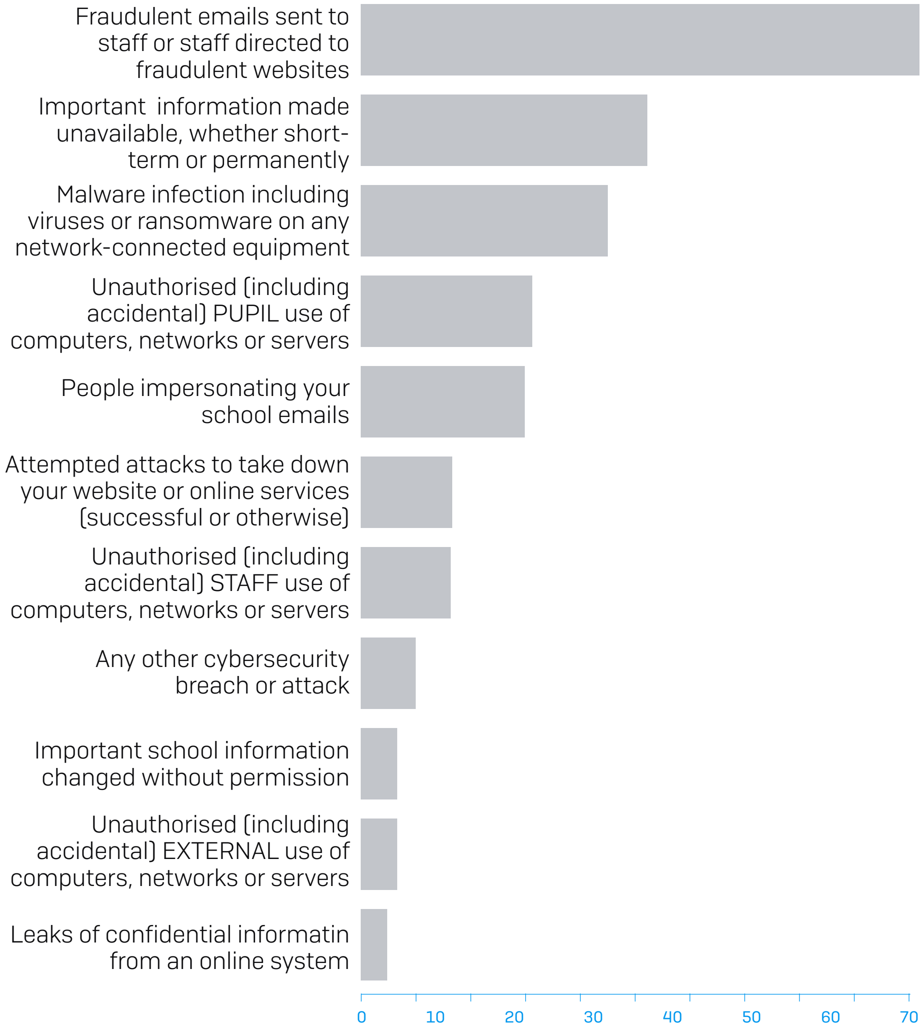
By deploying multiple Sophos solutions, users also benefit from the better protection provided by an integrated security system. For example, by deploying Sophos Central Email Protection and Sophos Central Endpoint Protection together, the solution will automatically run a system scan on a user's endpoint device if their email appears to have been compromised.

By consolidating multiple solutions under Sophos Central, we often see customers reducing their overall expenditure. They are also able to bring multiple licenses into a single co-termed agreement, leading to a reduction in the amount of time spent negotiating and agreeing renewals.

Email security and end-user training

If we look specifically at the types of incidents the schools are actually seeing:

As far as you know, have you ever experienced the following? (% of 432 schools answering yes)



National Cyber Security Centre, Cyber Security Schools Audit 2019

The largest reported incident by far is fraudulent email (Phishing): *69 percent of schools had suffered a phishing attack.*

69%

of schools had suffered a phishing attack.

Phishing attacks vary enormously both in terms of their sophistication and intent. This means we need to deploy a number of different checks and balances (and not just software and hardware) in order to protect ourselves against them. We, like other security vendors, have protections within our solutions that work to prevent malicious content finding its way onto your network via this delivery method. But it is alarming that more training isn't being conducted among school staff in order to spot and report this type of attack.

Unfortunately the schools weren't asked specifically about their email protection, but only 35% of non-IT staff had received any cybersecurity training.

As part of the report, the NCSC included some information entitled "Phishing attacks: Defending your organisation." This advises the following multi-layered approach.

Layer 1 – make it difficult for attackers to reach the user

This suggests implementing anti-spoofing controls (such as DMARC) to stop your email addresses being a resource for hackers, as well as implementing an email filter. Sophos Central Email protection provides email filtering, DMARC, SPF,DKIM protection, URL scanning, cloud sandboxing as well as a number of other features, including VIP impersonation protection, designed to prevent phishing emails making it to the user.

According to Andy Bates, Executive Director U.K. and EMEA at the Global Cyber Alliance, evangelists of the international standard DMARC, "It is obvious that the trust between parents, students, and teachers is paramount. Transactional conversations will often be conducted in email; but at least 80% of organisations do not have DMARC configured. In practice this means that anyone can impersonate a school or staff member via email, which can obviously lead to very serious consequences." – From the "Top of The Class Report" produced by LGfL

Layer 2 – help users identify and report suspected phishing emails.

Organisations should provide relevant training to help users spot phishing emails. They should also help users recognise fraudulent requests and create an environment where users can seek help via a clear reporting method. Sophos' phishing simulation tool Phish Threat enables regular and relevant training to be provided to staff using a combination of phishing simulation tests and supporting training modules. It also provides busy IT administrators with a way to automate this training schedule in advance and enrol new staff members as they join the school, and a way for staff to report both simulated and real phishing emails.

Layer 3 – Protect your organisation from the effects of undetected phishing emails.

The advice here is to protect your users from malicious websites using a proxy server and up to date browser. As well as protecting your devices from malware. Sophos offer multiple solutions and features that can assist here. We have protections to stop users navigating to malicious web content across our portfolio including within our XG appliances, endpoint, cloud email protection, and MDM. We are also industry leaders in terms of malware protection.

"it is important to recognise that this kind of email attack is not just about gathering credentials (user names and passwords) or diverting payments. Whilst both those elements can be incredibly costly, Proofpoint research found one million phishing emails containing the Emotet trojan in a single day." – From the "Top of The Class Report" produced by LGfL

Layer 4 – Respond quickly to incidents.

Detect incidents quickly by encouraging users to report to suspicious activity. Again, Sophos solutions can help here. Phish Threat provides users with the ability to report suspicious emails. Sophos Intercept X can provide information around any malicious content that has been detected (even if the user doesn't know this happened or hasn't reported it to IT).

In addition to the recommended layers outlined by the NCSC, Sophos Central Email protection also contains the following features:

- Advanced URL protection. This is designed to outsmart attacks aiming to slip phishing URLs past traditional gateways by delaying the upload of malware to websites until after the email is delivered. Sophos time of click protection checks the website reputation before delivery and at the time users click.
- By deploying Sophos Email and Sophos Phish Threat together, organisations are also able to identify staff who may need additional training support. Identify users who have been warned or blocked from visiting a website scanned by Sophos Email, and providing a fast path to enrol those users into awareness training.
- Display name and lookalike domain checks allow customers to identify and permit legitimate emails while blocking imposters.
- SophosLabs global threat intelligence network provides the latest spam and malware detection.
- Protect Sensitive Data Secure sensitive data and make compliance easy with Sophos Email push-based encryption and DLP.
- Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs.
- Comprehensive Reporting: Sophos Email provides statistics reports within the Sophos Central console in the form of tables and graphs – and all with custom date ranges selectable.

A note on home workers

With recent events, every school in the U.K. has had to embrace working and studying from home. This obviously presents its own security challenges. Having staff working on their own unmanaged devices is not something that we would recommend under normal circumstances (although it is not that unusual in the education). We would implore customers to consider the supply of managed devices with a full suite of security solutions to anyone who is accessing the network. However, as was highlighted in the audit, many do not have the tools or hardware currently in place to offer this.

To help address this challenge, Sophos is offering its premium home solution to staff and students at schools who deploy a Sophos solution free of charge. We would ask that, if you haven't already, you reach out to your Sophos provider to request these licenses. Although this solution doesn't allow the school to manage security policy, it does provide a level of protection on devices which are currently likely to have privileged access to school networks.

To learn more about Sophos' cybersecurity solutions and to start a no-obligation free trial, visit www.sophos.com, or speak to a Sophos representative.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS