TEXT100

YouGov

Geekileaks

A Sophos independent survey conducted by YouGov

SOPHOS

Security made simple.

www.sophos.com/ukeducation

Who we talked to

Education is under threat by cybercriminals. To find out what educators think about IT security, we interviewed 348 educators who influence IT policy and make decisions about security. The professionals we talked to included:

- 63% senior-level teachers (e.g. key stage leader or assessment leader)
- 20% Deputy or Assistant Headteachers
- 16% Headteachers or Principals

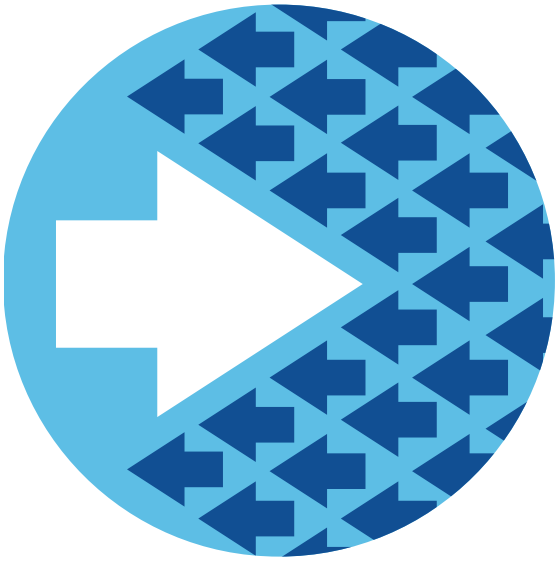
The type of schools represented vary: 24% are state-funded primary schools, while 23% are academies. A further 19% are state-funded secondary schools, and 6% are independent secondary schools. State-funded sixth form colleges represent 4%, while Independent primaries, free schools and grammar schools account for 1% each, and 20% comprise other kinds of learning institutions.

Finally, 92% are mixed-sex schools, 4% are girls-only schools, 3% are boys-only schools, and 1% don't know.

This report summarises our findings and offers you a glimpse of what educators think about IT security and how they're responding to the challenges they face.

Key findings:

- Nearly half (47%) believe their students know more about IT than they do.
- Over a third (34%) say that data loss is one of the biggest areas of concern for their school's IT security.
- Over a quarter (27%) say their school has some form of encryption in place.
- More than 1 in 4 (26%) say there's a greater focus in the past three years on monitoring students' activities online through the school's IT systems, school tablets, etc.
- Over a third (37%) schools do not have, or are unaware of, a radicalisation policy for the school or deem their policy insufficient to protect students.
- Over 1 in 3 (36%) say there's an increase in the use of cloud storage services, such as Dropbox and Google.
- Over half (52%) say their school does not use a system to monitor students' activity on school-owned IT devices, or they're unaware of any monitoring system used.
- Nearly half (47%) say additional training would help make them more confident about their ability to protect students from online threats.



In transition

The vast majority of schools are undergoing operational changes

The economic climate has had a dramatic impact on schools since 2015, with 57% facing budget cuts and 27% letting staff and employees go. Schools are evolving to meet the challenges they face, with 37% undergoing organisational restructuring in some way, be it the structure of departments or how departments operate. This is in line with the National Audit Office's report that schools will need to use staff more efficiently.

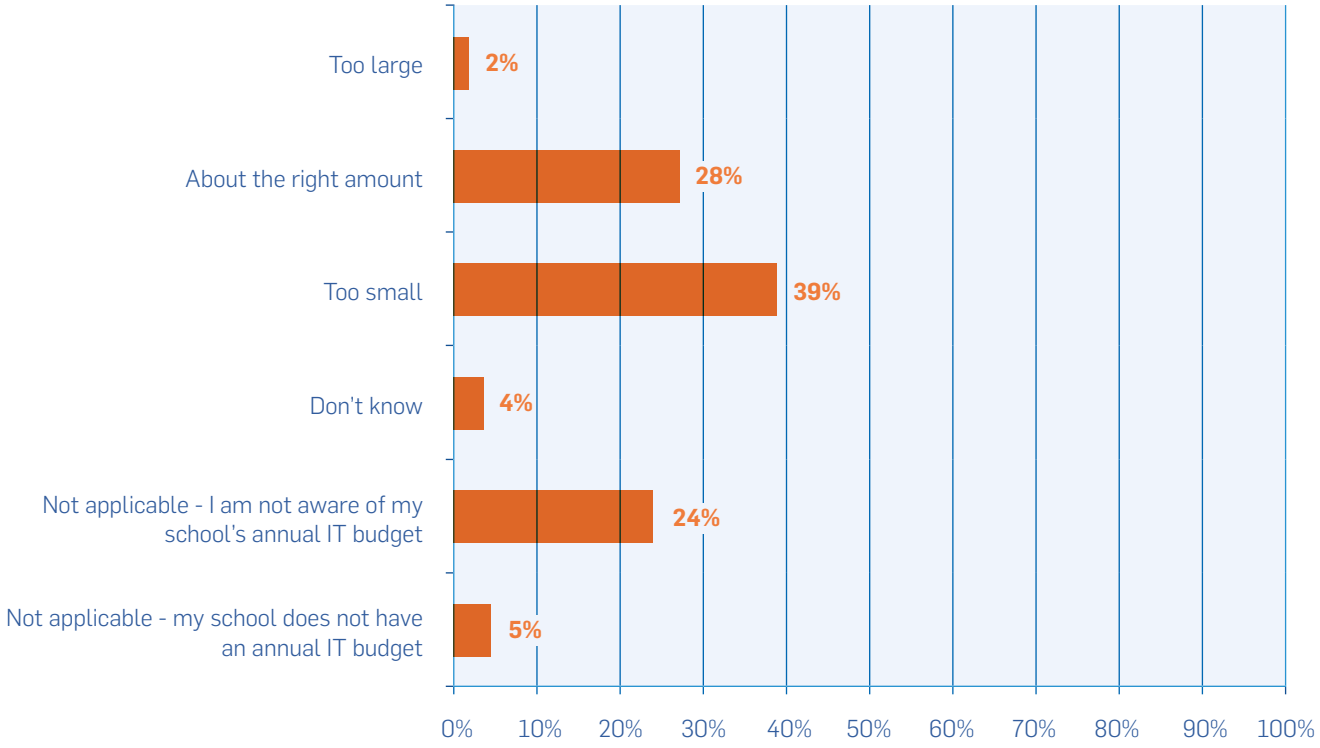
The prevailing wind might account for why 26% report a change in strategy or focus. A further 3% have become academies, which reflects the recorded slowdown of schools rushing to convert.

More schools are hiring (59%) to meet their changing needs. Those changing needs include increasing their digital capabilities, with 16% investing in software, hardware and hiring IT proficient staff. Other schools – 39% – think their IT budget is too small, suggesting they would like to invest more than they currently are.

Only 3% have seen their overall budget increase, while 9% have not experienced any changes whatsoever in the last 12 months.

Most schools feel their IT budgets are too small

"In general, do you think your school's current annual IT budget is too large, too small, or do you think it is about the right amount?"



Unweighted base: GB senior teachers (348)

Embracing digital

Moving away from paper is the biggest change to IT working practices

We asked respondents what changes have occurred at their school since December 2013. The majority (54%) said they're relying more on electronic student records.

Another 54% said staff are increasingly using electronic devices in the classroom, such as computers, mobile phones and tablets. According to 49% of respondents, these devices are being used for tasks such as registering students and recording grades.

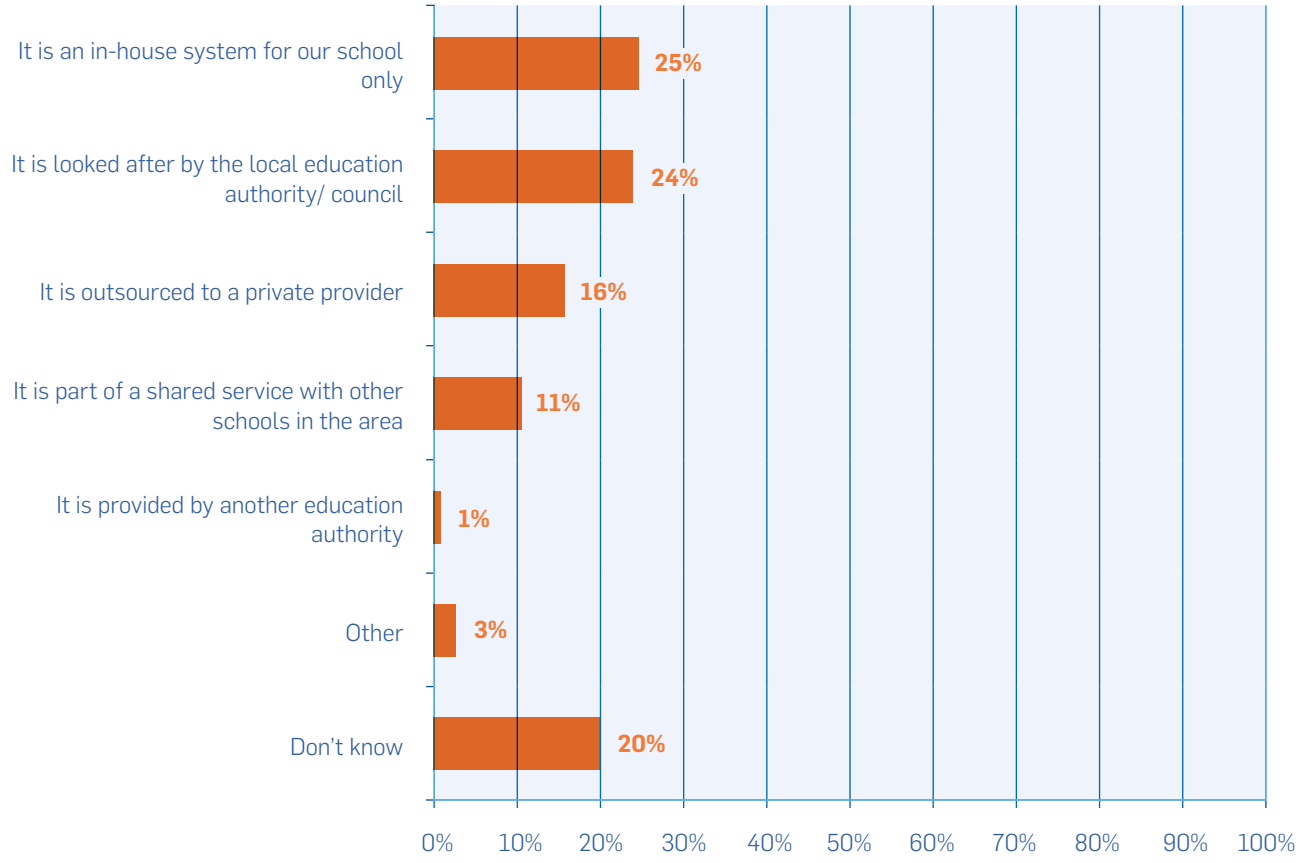
The study also reveals that 41% are seeing an increase in teachers and/or students using computers and laptops to draft and submit work, while 36% said teachers and students are choosing to access textbooks online. Cloud storage is gaining in popularity with 36% seeing increased usage in Dropbox, Box, Google Docs, and other cloud options.

While most schools are evolving with digital, a minority of respondents (8%) have not experienced any changes in their IT working practices, while 10% aren't sure of any changes.

News reports on high-profile data-security breaches are not reaching everyone. Only 29% noticed an increased awareness of data security as a response to media reports. Over the last three years, 26% have seen a greater focus in monitoring students' activities online via their schools' IT systems and devices.

No one IT security system is a runaway favourite among schools

"Which ONE, if any, of the following BEST describes your school's current IT security system?"



Unweighted base: GB senior teachers (348)

Students vs. teachers

Teachers feel students know more about IT than they do

"To what extent do you think students in your school know more or less about IT compared to their teachers, or do you think they know about the same amount?"

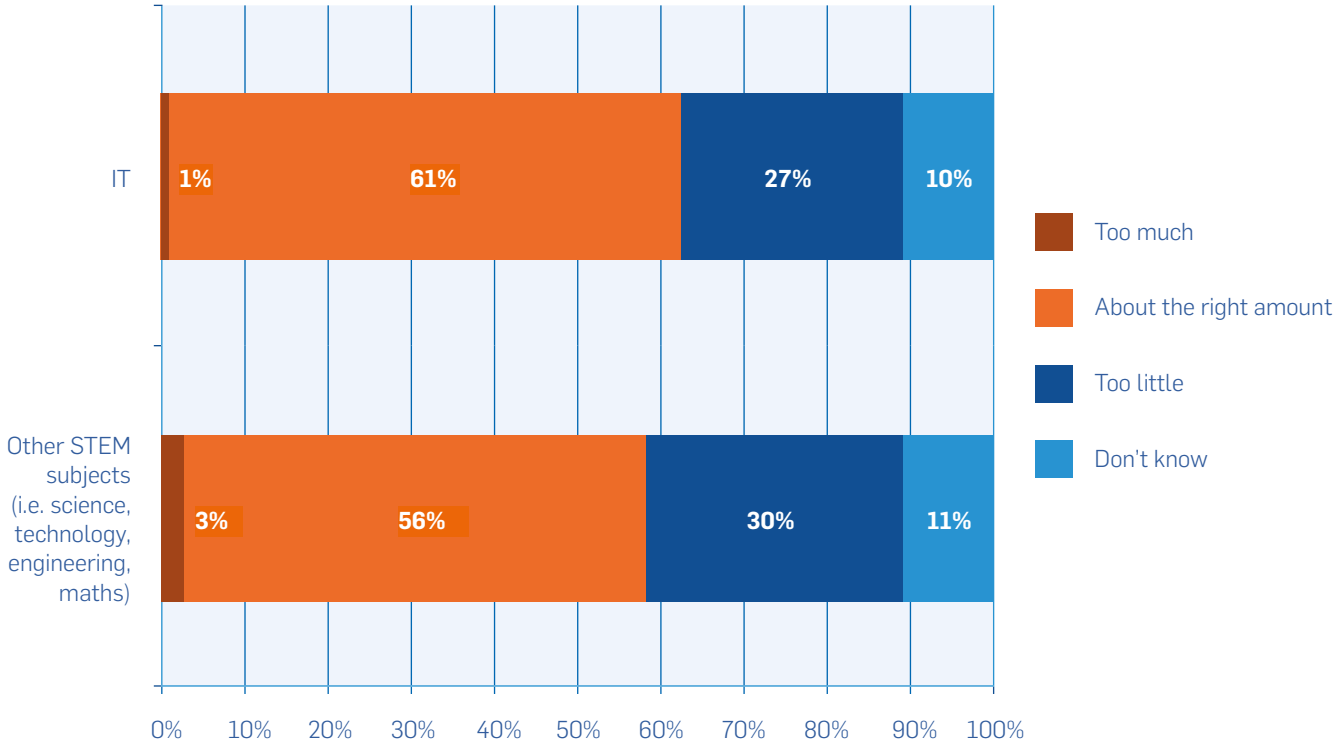
In answer to this question, 11% felt that students know a lot more, while 36% said students know "a bit more". This net 47% is more than double that of teachers who feel they know more about IT than students: 15% feel students know "a bit less" than they do and only 7% feel students know a lot less about IT, for a net 23%.

Another 23% reject both notions, feeling that IT knowledge is the same between teachers and students, and 7% don't know who is more savvy when it comes to IT.

Among the students themselves, the prevailing stereotype holds that boys are far more in tune with STEM fields, including IT, than girls. It is already recorded in a recent study by the Institution of Engineering and Technology that only 7% of British parents would encourage their daughters to go into these fields. Do schools share that sentiment?

Encouraging female students

"Do you think there is too much or too little being done to encourage female students in your school to take an interest in each of the following, or do you think there is about the right amount being done?"



Unweighted base: GB senior teachers who teach girls in their school (334)

Building confidence

The right training is important in protecting students online

The majority of those surveyed (81%) report feeling confident in their school's ability to protect students from online threats while in school. However, the self-assurance reflected in the net figure pales upon closer inspection. Only 21% feel 'very confident', while 60% say they're 'fairly confident'. Those feeling not very confident account for 13%, with 3% not at all confident.

Training in cyber security – or lack of – goes a long way to understanding teachers' level of confidence. When asked how many of their senior teachers, including the headmaster and deputy heads, receive training, 32% say all of them; 28% say some; 13% said none; and 26% don't know. For non-senior teachers who receive training: 31% say all of their non-senior teachers; 26%, some; 19%, none; and 23% don't know.

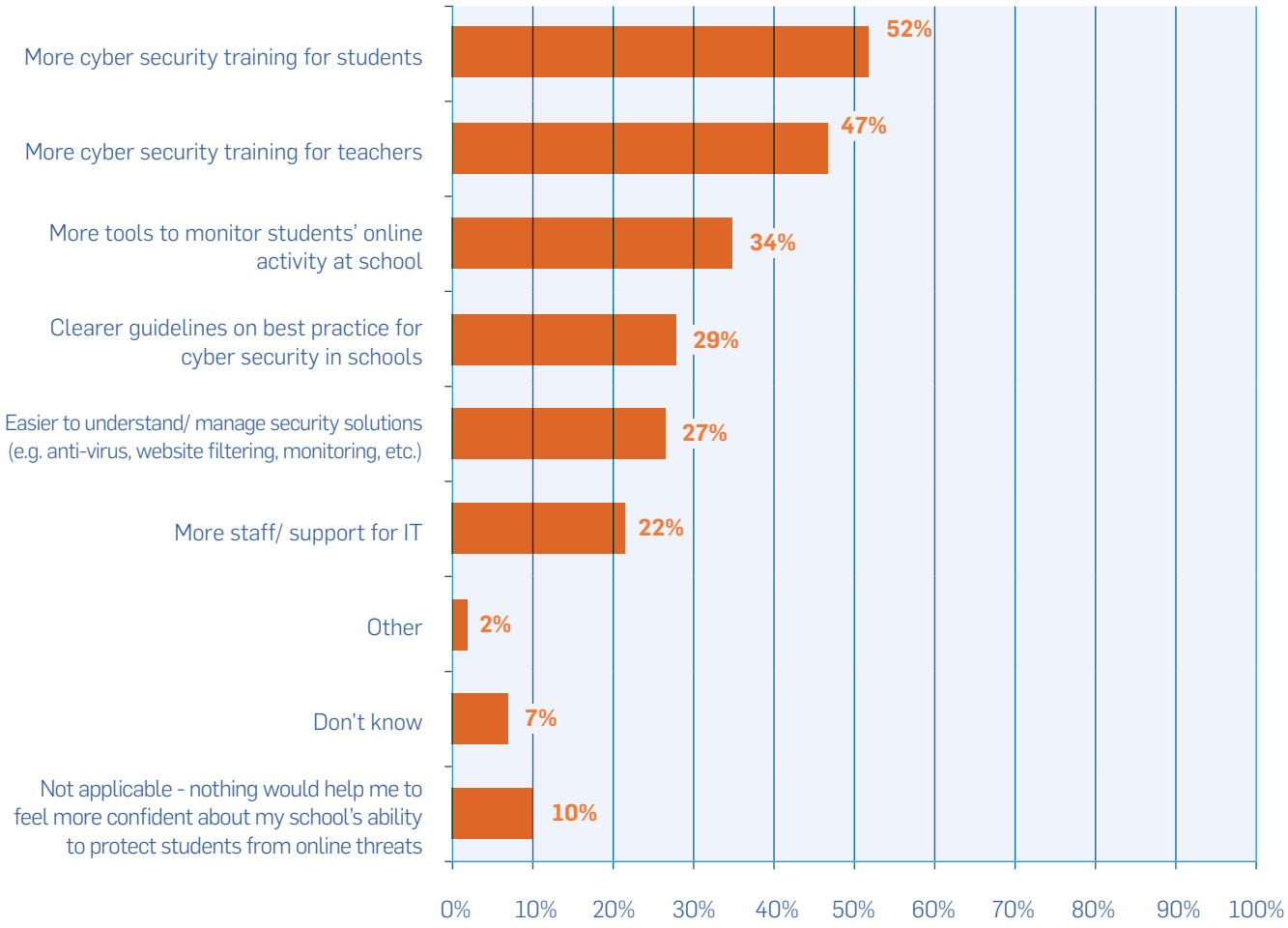
The quality of training is another issue. Did respondents feel those who've undergone training had been prepared to protect students and school data from online threats? Most were not overly confident in trained abilities. Regarding protecting students, 59% say training had prepared staff 'fairly well', compared to only 20% who say 'very well'. Negative perceptions persist among 12%, who say not very well; 2%, not well at all; and 8%, who don't know.

Numbers are almost identical regarding the safeguarding of data. More than half (58%) say they felt 'fairly well' in trained staff's ability to protect data, with 20% saying 'very well'. A minority (11%) report feeling 'not very well'; and 2%, not well at all. Some did not, or could not, commit ether way, stating they did not know.

Yet nearly everyone, even those who feel the most sure about their school's ability to protect students online, think that certain factors would strengthen their confidence.

Most teachers want students to receive cyber-security training

"Which, if any, of the following would help you to feel more confident about your school's ability to protect students from online threats?"



Unweighted base: GB senior teachers (348)

Areas of concern

Gaps in IT security reflect anxieties over cyber crime

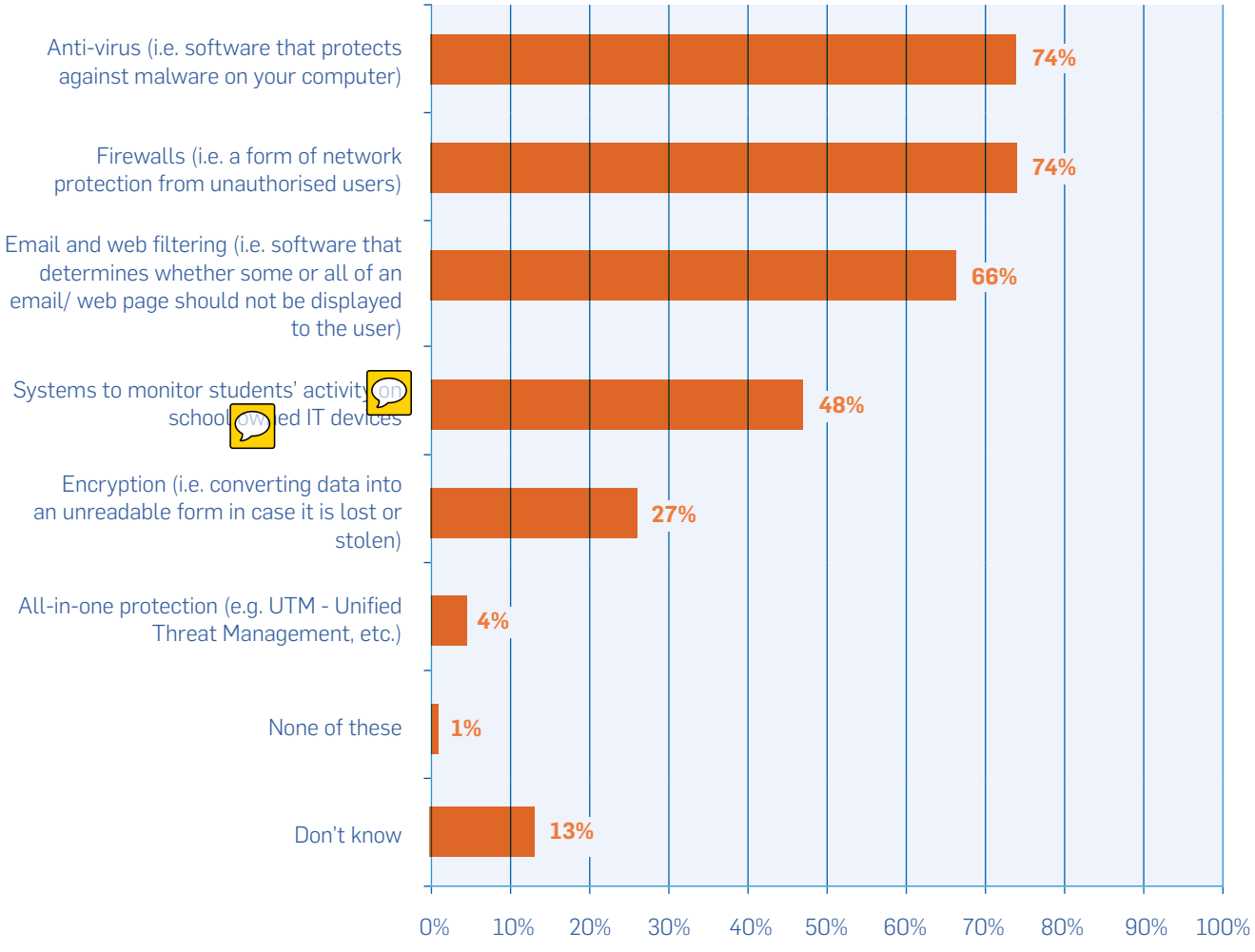
No one IT issue of concern dominates the survey. Instead, concerns are wide ranging, mirroring the multiple challenges schools face in protecting themselves. Most (34%) fear the loss of data, whether through system errors, neglect in storage, transmission or processing. This suggests a lack of confidence in staff handling data online.

The next biggest area of concern is phishing, with 22% worried about malicious emails, letters, and texts attempting to obtain personal details, such as usernames and passwords to access personal and financial information. Students using their own laptops, tablets and smartphones worry 21% of respondents, who fear the lack of security, while fewer – 14% – are concerned over teachers using their own devices in school. Interestingly, these concerns reflect the gap in IT security measures that could protect schools. Only 4% have all-in-one protection, e.g. Unified Threat Management, in place.

Targeted IT attacks raise another area of concern, with 19% worried that cybercriminals could bring down their network and access their school's data. A further 14% recognise ransomware as a specific threat, while 11% had no IT security fears whatsoever.

Only a minority of schools have high-level cyber security measures in place

"Which, if any of the following IT security measures does the school you currently work at ever use?"



Unweighted base: GB senior teachers (348)

Alarm bells

46% are aware of security breaches over the last three years

The causes for security breaches vary: 15% report a lost USB or device which contained important data. Another 11% experienced phishing emails with malware designed to obtain personal details such as usernames and passwords. A further 8% admit to falling victim to social engineering, such as being tricked to click on a fake email that triggered malware that infiltrated their school's network.

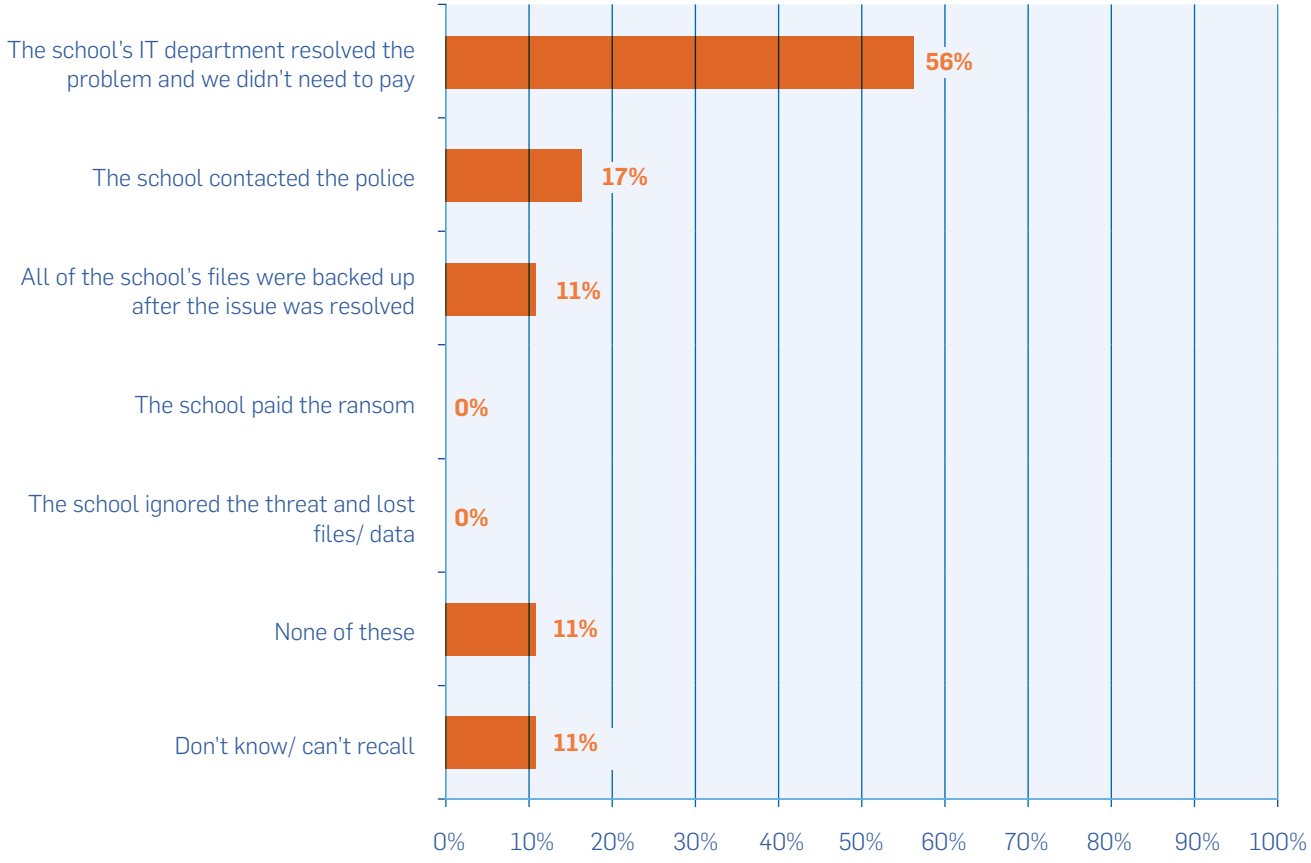
Staff are not the only direct targets, with 5% saying their school's website had been attacked with the intention of taking it offline.

Ransomware is on the rise, with 5% reporting an attack. Ransomware uses malicious software that encrypts files on the school's system until money is paid. After resolving the issue, only 11% backed up their school's files. The figure is surprisingly low, considering the turmoil and upset that ransomware causes. This could suggest that some victims felt they didn't need to back up their files, having put cyber-security measures in place to stop future ransomware attacks. Depending on how they resolved the issue – if their school retrieved the files without having to pay, for instance – it could also reflect a false sense of security.

Those that don't know the details of their security breach amount to 16%, while 48% are not aware of their school experiencing a cyber security breach. Some respondents (2%) said 'Other' than the choices presented. Interestingly, 5% prefer not to reveal their experiences.

56% say their IT department resolved ransomware without having to pay

"Which, if any of the following, describe what happened as a result of your school experiencing ransomware?"



Unweighted base: GB senior teachers whose school experienced ransomware in the last 3 years (18)

Staying alert

Almost half of schools use monitoring tools to watch students' online behaviour

Schools now have a legal duty to exercise due regard for stopping children from being drawn into terrorism. Known as the Prevent Duty, this legislation calls for schools to have robust safeguarding policies in place.

Most respondents (38%) lack enthusiasm for their school's radicalisation policy, rating it fairly good.

Only 19% consider their policy very good. A further 14% describe their policy as neither good nor poor. Delving deeper, 3% call their school policy fairly poor and another 3% describe theirs as very poor.

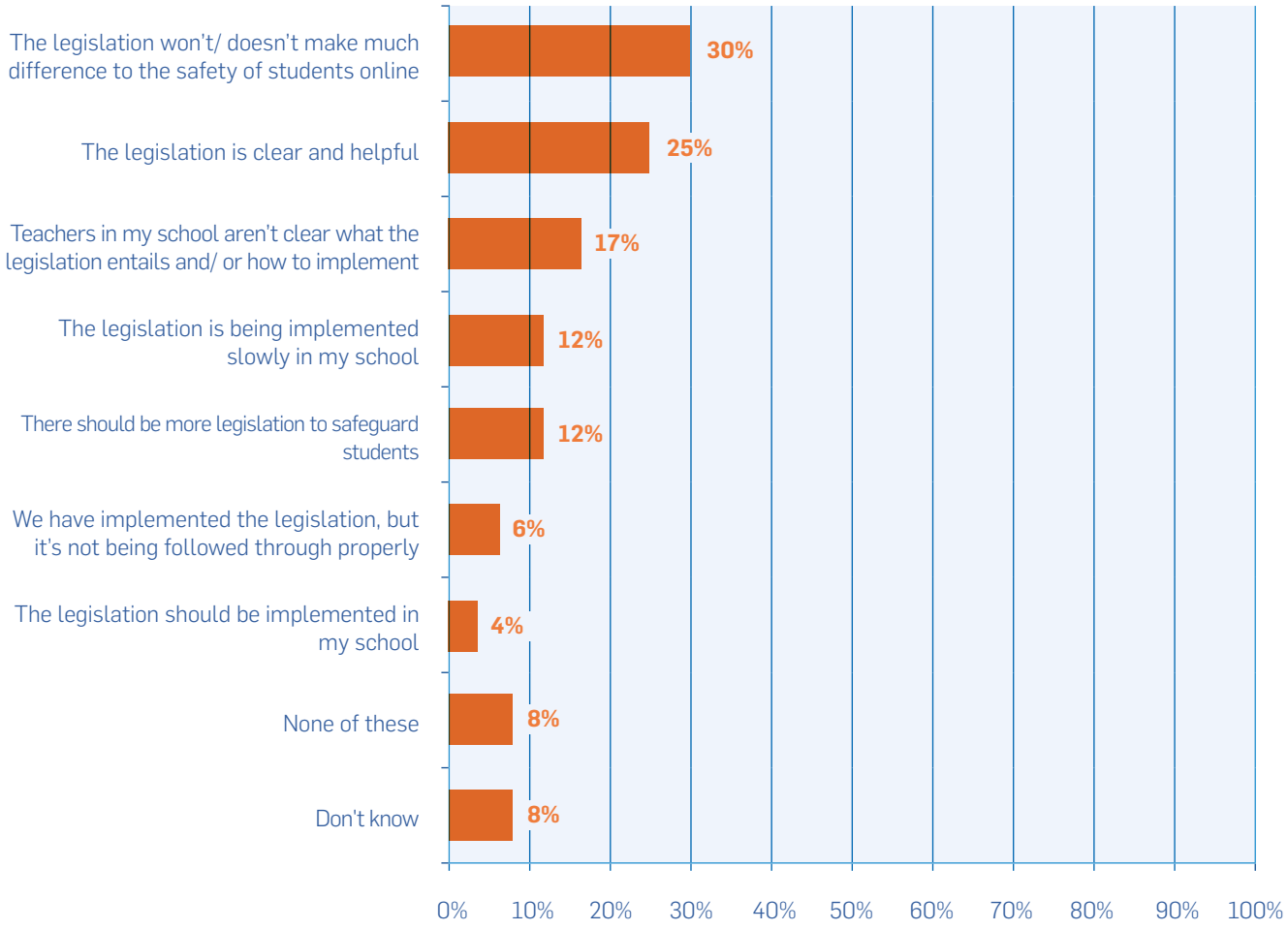
Yet some schools (10%) don't even have radicalisation policies in place. This falls in line with schools (11%) who don't use any tools to monitor students' behaviour on their school's internet-connected devices. Schools without policies might not even be aware of the Prevent Duty. Again, the percentage of schools unaware of the legislation (10%) closely aligns with those who don't have their own policies in place.

Awareness of radicalisation legislation accounts for 80% of schools, with 59%  it's being implemented in their school. This is not far off the 66% of schools who actively monitor students' online behaviour on school-owned devices. This breaks down to 48% who use a monitoring tool, and 18% who don't use a tool, but do monitor behaviour. A sizeable minority (21%) don't know if their school uses monitoring tools.

Of the 80% who are aware of legislation, 9% say it's not being implemented in their schools, while 12% are aware of it, but don't know if their school is adhering to government guidelines. A further 4% prefer not to say if they're aware of the legislation, and 6% simply don't know.

Only a quarter of respondents think the legislation is clear and helpful

"Thinking about the current safeguarding legislation to protect students against radicalisation online... In general, which, if any, of the following statements do you agree with?"



Unweighted base: GB senior teachers aware of the safeguarding legislation to protect students against radicalisation online (278)

Conclusion

The biggest area of concern for schools regarding their IT security is data loss (34%), either by failures or neglect in storing it, or via transmission or processing. Their fear is well founded, considering that only 27% use encryption to make data unreadable in case its lost or stolen. Only 4% use all-in-one protection, with most schools relying on what would be considered basic security measures, such as anti-virus software, firewalls and email and web filtering.

It's not surprising that, when asked how they view their IT budget, the majority respondents describe it as too small, suggesting they would have deeper protection in place if they could financially manage it. With 57% of schools experiencing budget cuts, money earmarked for IT is likely to squeeze tighter still.

Schools will need to increase their knowledge of IT to get better value. This will help them determine if their IT security system is giving them to most bang for their buck. For instance, a school might get more protection with an in-house system rather than having it looked after by the local education authority, or vice versa.

More effective training would also help, especially considering that nearly half of those surveyed (47%) feel their students know more about IT than they do. Currently, only a fifth of respondents felt training had prepared their schools to protect students (20%) and data (20%) 'very well'. Just over half felt their schools could protect students (59%) and data (58%) fairly well. But 'fairly well' is not good enough in the current climate.

About Sophos

Sophos is a leader in next-generation endpoint and network security  as the pioneer of synchronized security develops its innovative portfolio of endpoint, network, encryption, web, email and mobile security solutions to work better together.

More than 100 million users in 150 countries rely on Sophos solutions as the best protection against sophisticated threats and data loss. Sophos products are exclusively available through a global channel of more than 26,000 registered partners. Sophos is headquartered in Oxford, UK and is publicly traded on the London Stock Exchange under the symbol "SOPH."

www.sophos.com

SOPHOS

Security made simple.