Cyber Security in UK schools

How well protected are schools and colleges in England and Wales?

Results of a survey carried out
September to December 2021

April 2022

University of Kent | Institute of Cyber Security for Society (iCSS)

SWGfL Safe, Secure, Online

Bitdefender®

Forward

SWGfL, in partnership with the University of Kent and supported by Bitdefender are delighted to release this, our first report into the state of Cyber Security in UK Schools.

Whilst there is a range of data about education and the risks cyber attack presents we set out to conduct an up-to-date review of the state of cyber security. We were delighted by the number of clicks on our survey with nearly 350 respondents visiting the survey form representing around 66,800 children in education.

The findings of our research confirm many of the behaviours, issues and risks we see in our work across the UK. Supporting and highlighting that there is much room for development in UK educational establishments with regards to protection against cyber attack. This research discloses the variation in approach and attitudes to cyber security clearly indicating a need for a shift in policy.

SWGfL has been supporting schools since 2001, most recently a core focus of our work has been the development of the cyber security agenda. The need for improvement in cyber security parallels the original drivers for change to the online safety remit; a lack of policy, training and knowledge about the risks and potential for harm. This is no surprise, headteachers and school leaders have often not been skilled in recognising the need for cyber security nor in how to address an identified need. This research identifies the continuing need for resources and support in order to accelerate change to better protect against cyber attack.

'SWGfL has been supporting schools since 2001, most recently a core focus of our work has been the development of the cyber security agenda.'

Key findings

1

62% of schools have not received any cyber security training.

Staff represent the biggest risk and the largest barrier to attack, investment in training represents a significant risk reduction strategy.

2

17% of schools reported a cyber attack, with 48% of these being ransomware.

It's clear from this, and other data, that schools must develop a strategy to protect against the effects of a ransomware attack. Training and backup/recovery processes are key to this strategy.

3

Risk and business continuity plans are not well developed

in 54% of responses with only 35% reporting that these are regularly updated. A vital component of strong recovery is the knowledge about which systems should be prioritised and a clear, connected and well thought out process for recovering from attack.

4

31% of respondents do not have an IT security policy

meaning they are unaware of the risks and may have no connected approach to protecting key data assets.

5

17% say that they have no cyber security concerns.

This potential apathy towards cyber security places an organisation at additional risk and whilst a low percentage, nevertheless, represents a possible attack vector for criminals.

6

With 76% of respondents stating that the internet is key for their job,

as a core tool for education, we need to be treating the protection of ourselves and our learners online as core component of education.

Findings

Section 1 - Overview and demographics:

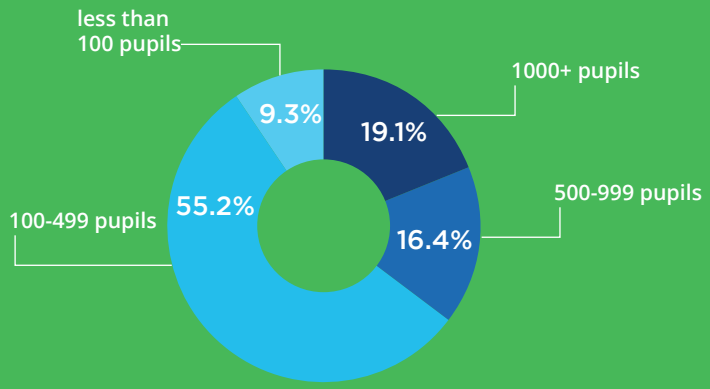
There were 183 valid responses to the survey overall. We did not ask participants to disclose the identity of their school, so the number of schools covered is unknown, but judging from the combinations of different school attributes we saw 174 schools with different attributes, so the number of schools ranges from 174 to 183. These schools are from 126 different local authorities. The school attributes we asked each participant to provide include school size (the number of pupil enrolled), ISCED levels of pupils the school catered for (e.g., 0: early years education, 1: primary level education, 2: lower secondary level education, 3: upper secondary level education, 4: further education), school type (e.g., academy, local authority (LA) maintained school, religious affiliated school, special school, independent school or a pupil referral unit (PRU), other type not stated), local authority the school belongs to, etc. Since the number of schools is close to the number of valid responses, in the following do not differentiate these two numbers, in order to simplify our analysis. Note that schools with the same attributes may still be different schools.

The findings are only indicative of the schools in this sample; small numbers of certain demographics took part in the survey (e.g., a very small number of independent schools and pupil referral units (PRUs) took part.

What is the size of your school (number of pupils)?

Most of the schools represented by responses to the survey has between 101 and 499 pupils (see Figure 1), with a mode of 102 schools (56%). Schools that had a population of less than 100 pupils were the least represented in responses (16 schools; 9%), yet only 34 schools with a large population (1000 pupils or more) (19%) were represented in responses collected.

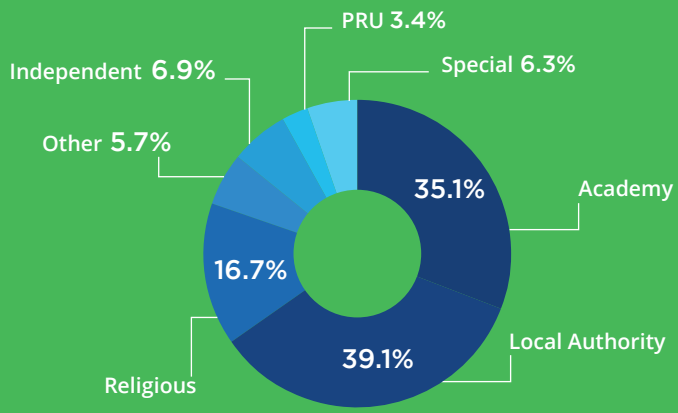
Figure 1 A chart showing the sizes of school (number of pupils)



Which categories most closely match your type of school?

Different types of school were represented in the responses to the survey. Academies (as defined by the Academies Act 2010) and schools maintained by local authorities together constituted for 65% of schools that responded to the survey. Other types of school (e.g., special schools, independent schools and pupil referral units) were less represented in the responses collected. Findings pertaining to these types of school provide an overview of the schools that responded to the survey, and may not be indicative of UK-wide distribution for these types of schools. Some schools that responded were outside of given responses, for example further education colleges (presented in Figure 2).

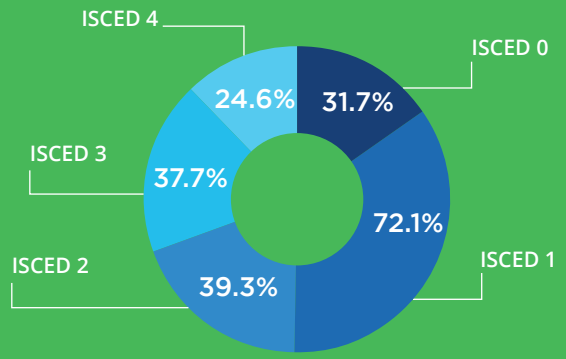
Figure 2 A chart showing different school types that responded



Which age group(s) are in your school?

Most responses to the survey appeared to come from schools which catered to pupils at ISCED level 1 (primary education) (72.1%)as shown in Figure 3. The next most populous category was ISCED level 2 (lower secondary education), with 39.3% of responses. The lowest number of responses came from schools providing for ISCED level 4 (further education).

Figure 3 Percentage of schools per level of educational provision (ISCED level)



Section 2 - Cyber security of the schools:

Which of the following technologies does your school currently deploy?

Staff who were IT teachers, online safety co-ordinators, IT support staff or third party IT support were asked about technologies deployed to protect schools from cyber attacks. Respondents reported deploying a variety of technologies to support the cyber security of their schools. When examining which technologies were the most popular, firewalls (93.7%), antivirus/malware/security technology (96.8%) and data backup (90.5%) were reported as used by most responses within our sample. As can be seen in Figure 4, multi-factor authentication was reported as being in place at the schools of 49.2% of respondents. Air gapped data backup was the least utilised technology, with only 22.2% of respondents reporting this being used in their schools.

When examining the technologies used by each type of school, the distribution of responses per technology deployed appeared to broadly echo the broader distribution. The chart also shows that more responses were gained from academies and local authority maintained (labelled as LA) schools overall.

Figure 4 Statistics of responses using each technology to protect from cyber attack

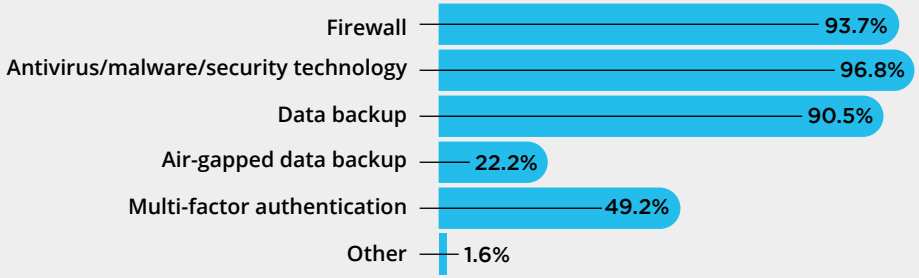


Figure 5 Statistics of responses using each technology to protect from cyber attack per type of school

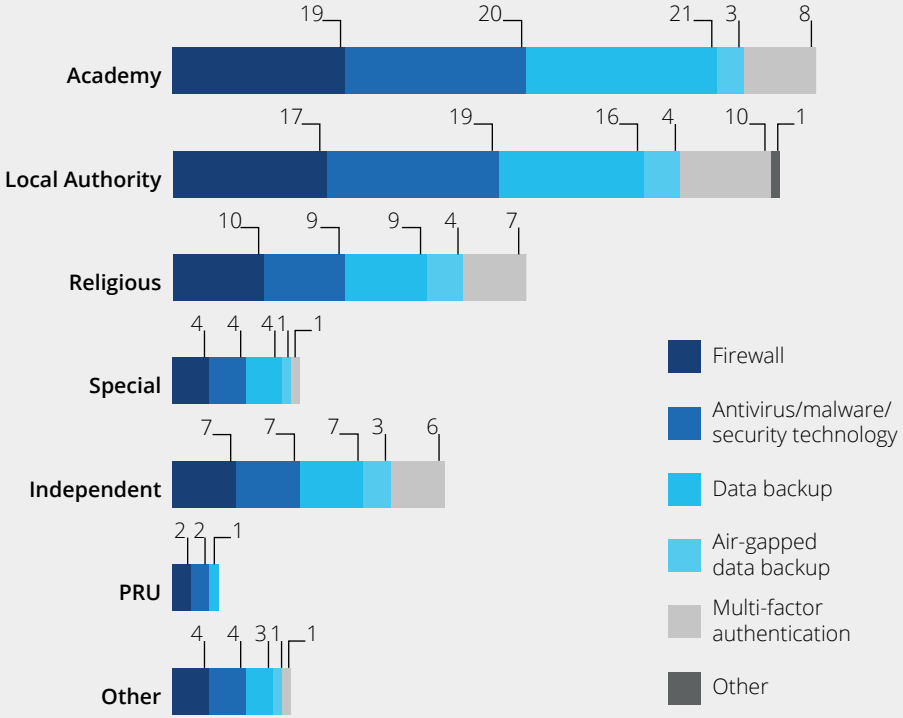


Figure 6 Statistics of responses using each technology to protect from cyber attack per school size (pupils)

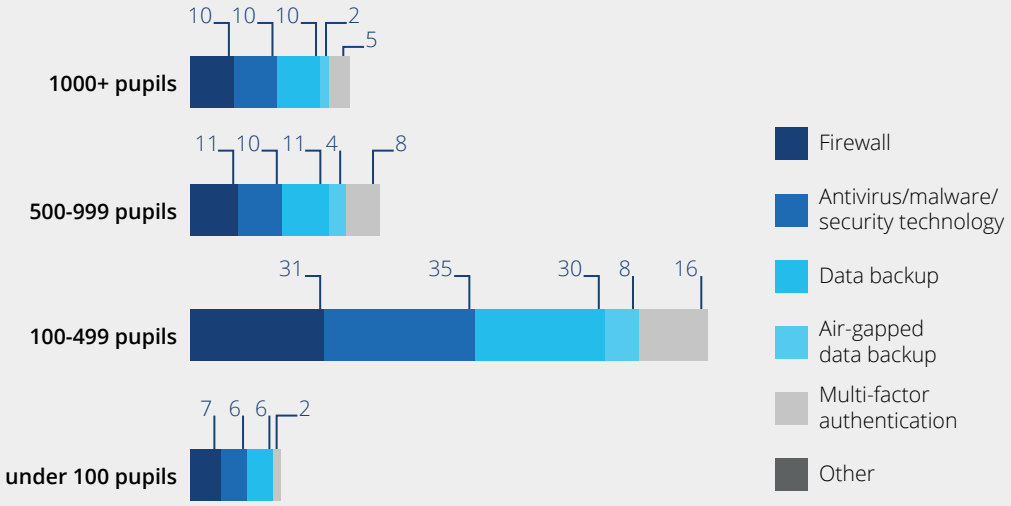
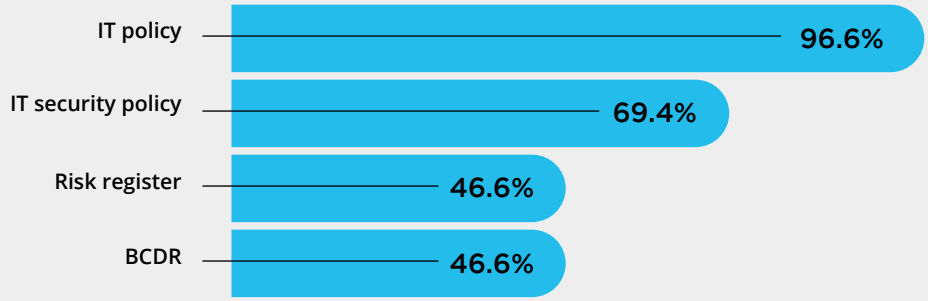


Figure 7 Statistics of schools with cyber security relevant policies and procedures



'business continuity and disaster recovery plans (BCDR) were reported by 46.6%'

'Air gapped data back up was not reported as used by respondents from schools with under 100 pupils in this sample'

This distribution was further iterated in the analysis of the technologies schools used according to school size (number of pupils), with firewalls, antivirus/malware/security technology and data back up all being the three technologies the most endorsed by respondents. Air gapped data back up was not reported as used by respondents from schools with under 100 pupils in this sample, and only 2 respondents with over 1000 pupils use air gapped data back up.

Which of the following policies/procedures are in place at the school?

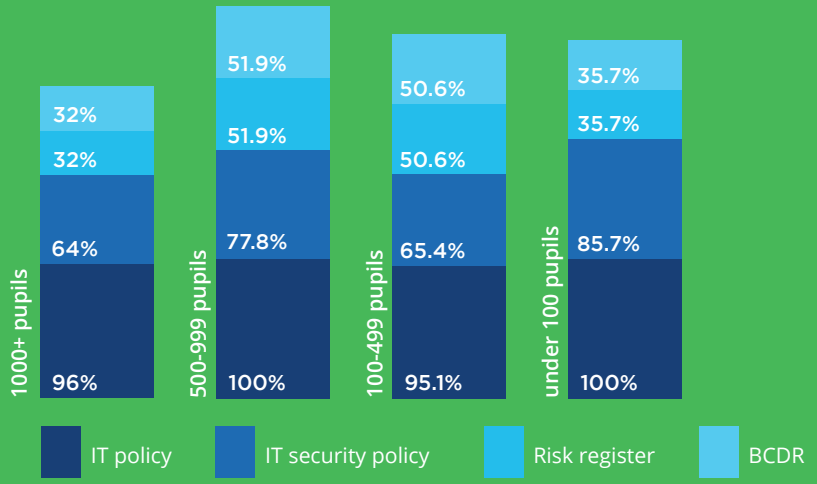
All survey respondents were asked about the policies and procedures in their schools focusing on cyber security. The majority of respondents reported their school having an IT policy (96.6%). Other policies were reported as being present and/or known of less frequently: IT security policies were reported by 69.4% of respondents. Risk registers and business continuity and disaster recovery plans (BCDR) were reported by 46.6% of respondents each (see Figure 7).

When examining the presence of policies and procedures relevant to cyber security, results analysed by type of school appear to mostly echo the findings given in Figure 7. Schools endorsed with fewer responses (e.g., special schools, independent schools, PRUs and other types of schools) also appear to mostly follow the findings given by other types of school (for example, academies and LA maintained schools). BCDR policies were not commonly enforced across all school types of our sample, with academies, LA, religious and PRU reporting less than 50% of them enforce a BCDR policy.

Figure 8 Statistics of schools with cyber security relevant policies and procedures

Pupil population level also did not appear to provide findings which were different to Figure 7. All responses from schools with under 100 pupils and schools with between 499 and 999 pupils report having an IT policy, and BCDR policies remain poorly enforced across school sizes.

Figure 9 Statistics of schools with cyber security relevant policies and procedures per school size (number of pupils)



Which of the following policies/procedures have been updated in the last year?

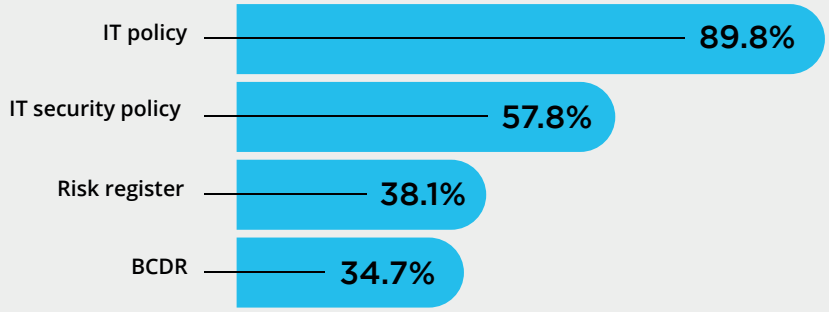
The distribution of policies and procedures related to cyber security which were updated in the last year (Figure 10) appears similar to results regarding the enforcement of these policies and procedures (Figure 7). In Figure 10, IT policies were reported to be updated the most often (89.8% of responses), with BDCRs as the least reported as updated in the last year (34.7%). With a lower number of respondents reporting the enforcement of a BCDR, it is not a surprise that it is the policy which is reported as the least often updated by our sample.

'BDCRs as the least reported as updated in the last year (34.7%)'

In comparison to the enforcement of such policies and procedures, fewer responses indicated that these policies were updated. For example, 69.4% of respondents reported having IT security policies in their schools (or being aware of such policies) but only 57.8% reported these had been updated in the last year. Further differences are observable on a descriptive level for risk registers (46.6% present, 38.1% updated in the last year and BCDRs (46.6% present, 34.7% updated in the last year). These differences between the number of respondents reporting their enforcement and whether they have been updated in the last year shows that not all cyber security relevant policies in schools represented by the respondents are updated annually. Risk registers especially have not much meaning if they are not kept up-to-date.

'not all cyber security relevant policies in schools represented by the respondents are updated annually'

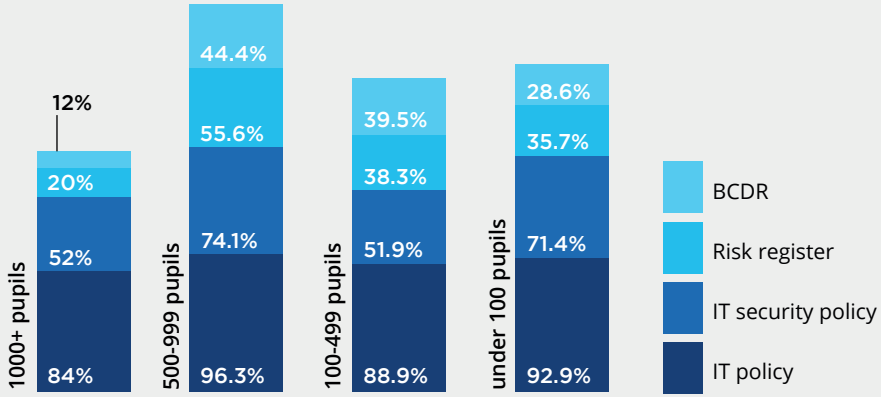
Figure 10 Statistics of cyber security relevant policies/procedures have been updated in the last year



Examining the type of school (Figure 12) and pupil population size within the school (Figure 11) follow the results from Figure 10, with IT policies being reported more often as updated in the last year in comparison to other policies and procedures across different school sizes and types of school.

None of the responses in our sample who came from a PRU or 'other' type of school reported that their BCDR was updated annually, and equally low numbers across the rest of the types of school (range between 18.2% (special schools) and 30.9% (LA maintained schools; range = 12.7%).

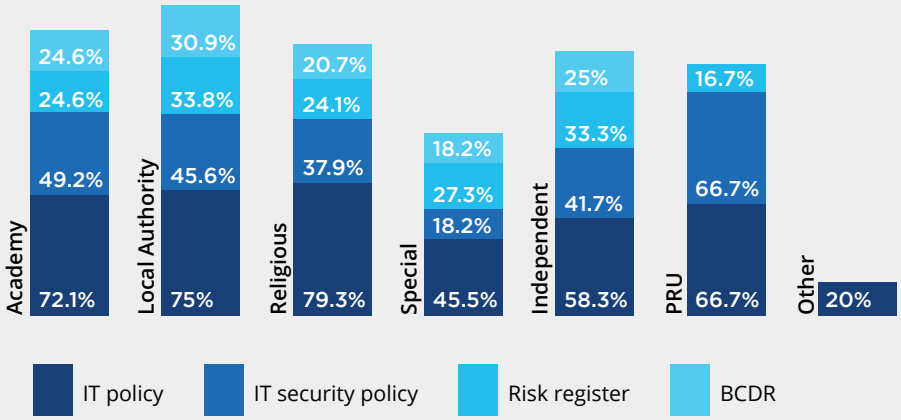
Figure 11 Statistics of cyber security relevant policies/procedures have been updated in the last year by type of school



As can be seen in Figure 11, BCDRs remain the least often updated policy, with only 12% of responses from schools with over 1000 pupils as updating their BCDR policy in the last year. This is in comparison to schools with between 499 and 999 pupils, where 44.4% of responses updated their BCDR policy within the last year (range between over 1000 pupils and 500-999 pupils= 32.4%). A much smaller range is found with IT policy updates, with only a 12.3% difference between the highest and lowest responses between categories (over 1000

pupils (84.0%) and 500-999 pupils (96.3%) (range= 12.3%). This smaller range shows that in our sample, IT policies appear to be more consistently updated annually, perhaps because of their perceived importance in contrast to other policies.

Figure 12 Statistics of cyber security relevant policies/procedures have been updated in the last year by type of school by level of educational provision by pupil population size

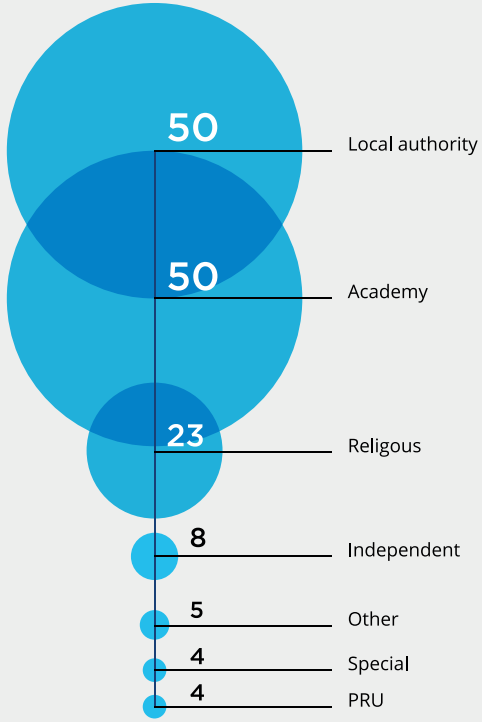


Does your school ensure that all updates are promptly installed on devices (patching)?

The majority of respondents reported that their school ensured that soft updates were promptly installed on devices (also known as patching) (93.2%). 10 respondents in our sample did not report that their school ensures that updates are promptly installed. Hard updates were not asked about at this time. The type of device was not specified and could refer to staff laptops, pupil laptops or desktops, or other devices used (e.g., iPads, smartphones). When examining if there are any differences between types of school (Figure 13) or size of school (Figure 14), no large differences were found. In our sample, only 4 PRUs (out of a total of 6) reported that their devices were promptly updated in Figure 13, which was lower than other types of school within our sample.

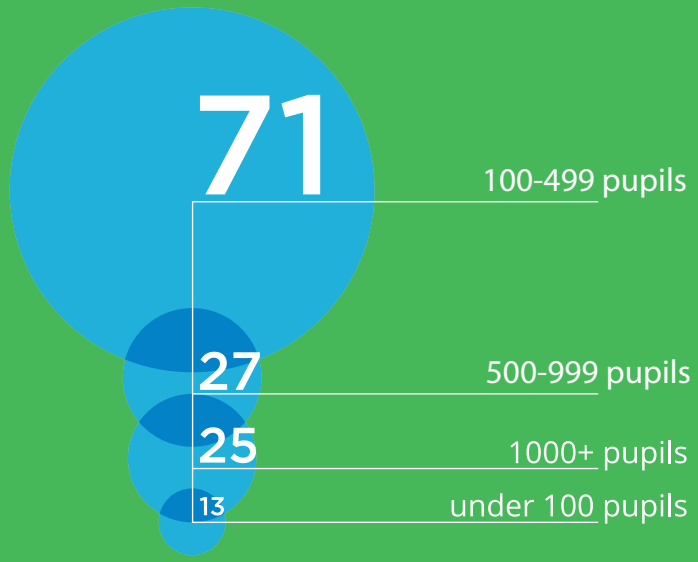
Although most respondents reported that their school ensured that soft updates were promptly installed on devices, the responses that reported that this does not occur in their setting indicate that some schools may be vulnerable to cyber attacks in this manner.

Figure 13 Statistics of schools which ensure updates are promptly downloaded on staff devices by type of school



'Although most respondents reported that their school ensured that soft updates were promptly installed on devices, the responses that reported that this does not occur in their setting indicate that some schools may be vulnerable to cyber attacks in this manner. '

Figure 14 Statistics of schools which ensure updates are promptly downloaded on staff devices by size of school (number of pupils)



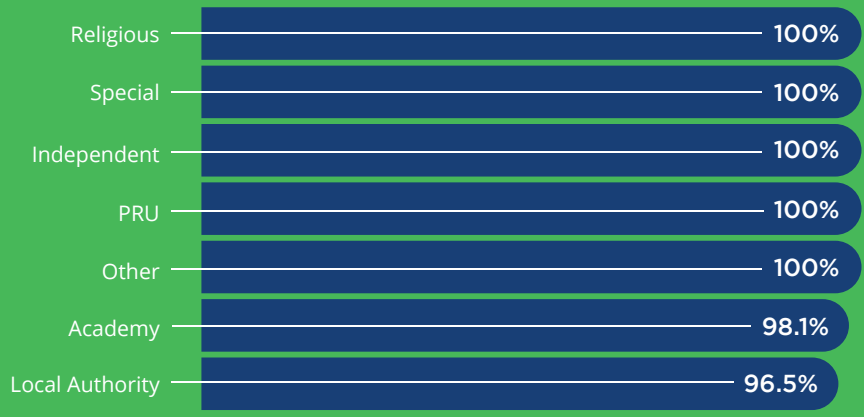
Does your school place restrictions on the apps you can install?

Across all schools, 98.0% of respondents reported their school placed restrictions on which applications can be installed. Only 3 respondents within our sample indicated that their school did not place restrictions on the applications which can be installed. These schools are potentially at risk from malware or viruses being downloaded and installed onto school devices, placing the cyber security of their school at risk.

'98.0% of respondents reported their school placed restrictions on which applications can be installed'

Figure 15 shows that within our sample, schools that did not have 100% of schools restricting the applications that could be downloaded were: academies and LA maintained schools.

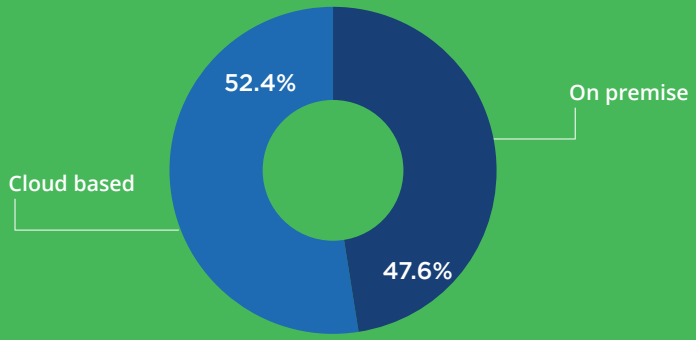
Figure 15 Statistics of schools placing restrictions on applications installed per type of school



Which is more important - EndPoint protection that is on premise or cloud based?

Preferences in Endpoint protection did not differ greatly. When all responses were considered together, 47.6% had a preference for Endpoint protection which was on premises, and 52.4% had a preference for cloud based Endpoint protection (see Figure 16).

Figure 16 Statistics of preferences regarding Endpoint Protection



When examining the pupil population size (see Figure 17), different sized schools within our sample appeared to opt for different preferences of Endpoint protection. More schools with over 1000 pupils opted a preference for on premises Endpoint protection (60%) , yet schools with between 499 and 999 pupils appeared to indicate a preference for cloud based Endpoint protection (81.3%). This distribution indicates that size appears not to influence the preference for on premise or cloud based Endpoint protection.

The type of school also shows a variety of preferences between on premise and cloud based Endpoint protection. School types which had more responses in preference for an on premise solution in our sample include: academies (60.0%), independent schools (66.7%) and PRUs (100%). LA maintained schools (63.6%), schools with a religious affiliation (57.1%), special schools (100%) and other types of school (75.0%) indicated a preference for a cloud based Endpoint solution. Only respondents from special schools and PRUs within our sample only selected one preference of Endpoint solution.

Figure 17 Percentage of preferences regarding Endpoint Protection per school size (pupils)

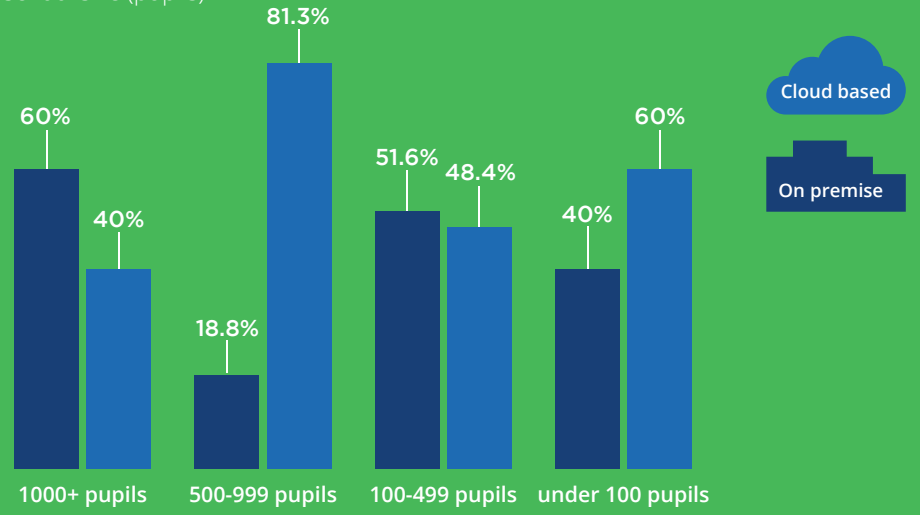
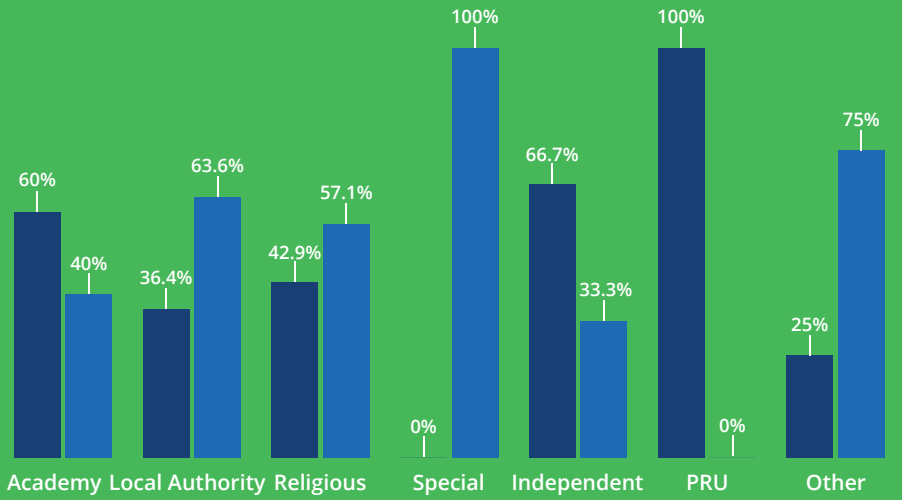


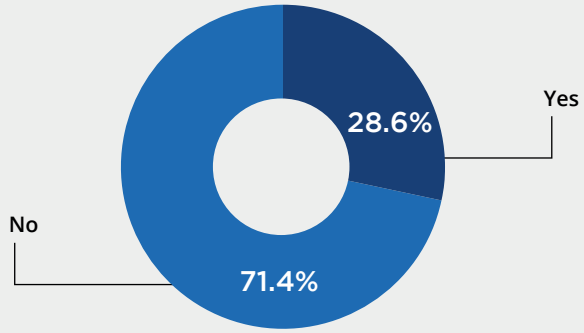
Figure 18 Percentage of preferences regarding Endpoint Protection per school type



Do you have resource challenges that could be resolved through some sort of managed EndPoint protection service? If yes, which of the following would be most helpful?

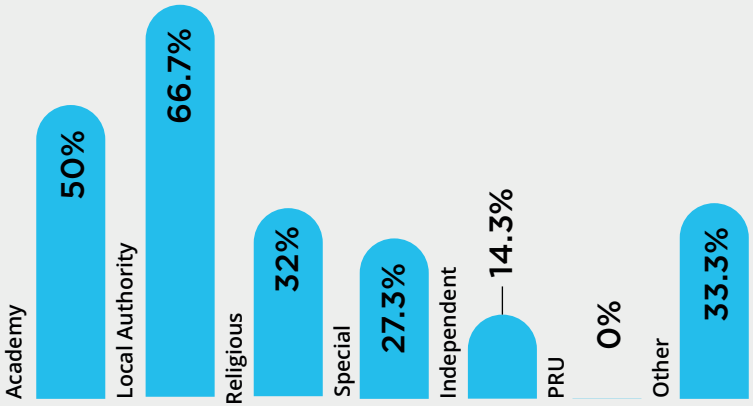
In regards to resource challenges, most respondents of our survey reported their school not having challenges that could be resolved through some sort of managed EndPoint protection service (71.4%) (see Figure 19).

Figure 19 Statistics of schools reporting having challenges that could be resolved through some sort of managed EndPoint protection service



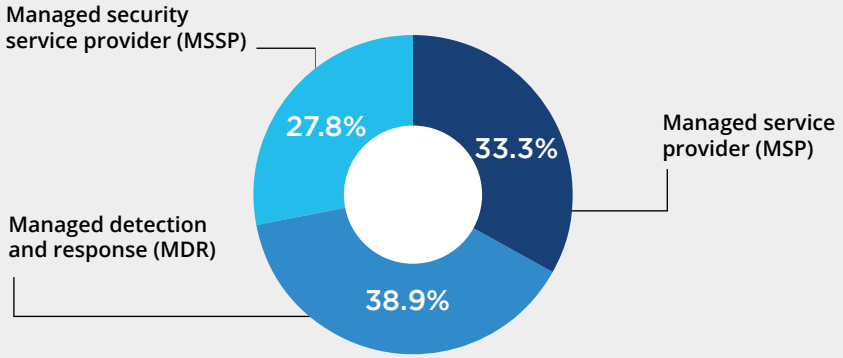
Different types of school represented by respondents to our survey indicated differing levels of resource challenges which could be resolved through some sort of managed EndPoint protection service. No responses from special schools in our sample reported resources challenges that could be resolved through some sort of managed EndPoint protection service, however 50.0% of PRUs and 66.7% of other types of school reported having challenges that could be resolved through some sort of managed EndPoint protection service. This wide range (range=66.7%) shows the diversity of schools represented in our responses and their needs.

Figure 20 Statistics of schools reporting having challenges that could be resolved through some sort of managed EndPoint protection service per type of school



In regards to the Endpoint solution which respondents indicated a preference for, only 18 responses were given, and these appeared to be relatively evenly split across the 3 given options: managed service provider (33.3%, 6 responses), managed detection and response (38.9%, 7 responses) and managed security service provider (27.8%, 5 responses). No overall preference is indicated between the 3 options, perhaps indicating that different provision is useful for different schools.

Figure 21 Statistics of schools reporting having challenges that could be resolved through some sort of managed EndPoint protection service



From a cybersecurity perspective – what keeps you up at night?

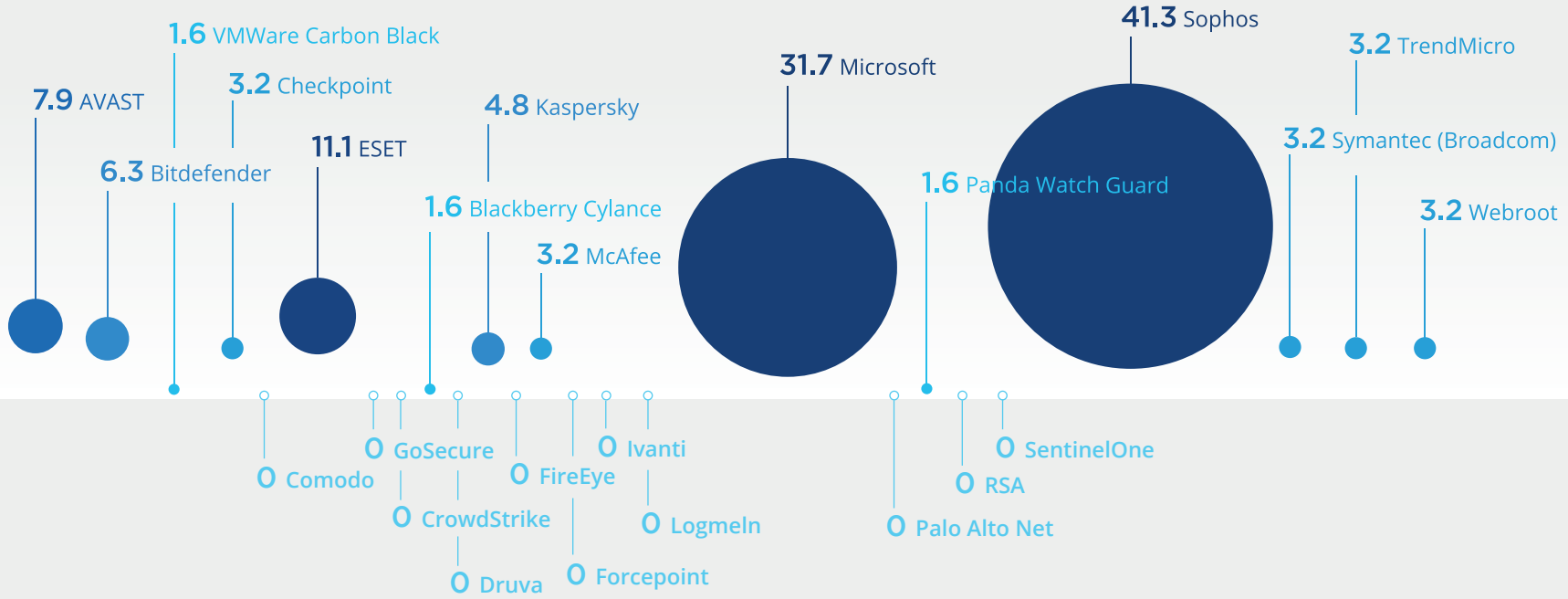
When asked about concerns which keep them up at night from a cyber security perspective, a variety of responses were given. This range included: data theft, data security and GDPR, awareness of users and users following policies, network safety and the increasing complexity of cyber attacks. 12 respondents (17%) reported having no concerns from a cyber security perspective.

What Endpoint protection solution do you currently use?

The most popular current Endpoint protection solution used across the schools represented within our sample was Sophos (41.3%), with Microsoft (31.7%) being the second most popular Endpoint protection used within our sample (see Figure 22).Some Endpoint protection services, for example, VMWare Carbon Black and Ivanti, were not used by any schools within our sample. 10% of respondents did not know what Endpoint protection solution their school currently uses. This could be indicative of schools using support companies to assist with cyber security matters or the delegation of set tasks to certain employees within schools, and the individual with the knowledge required not responding to the survey.

'(17%) reported having no concerns from a cyber security perspective.'

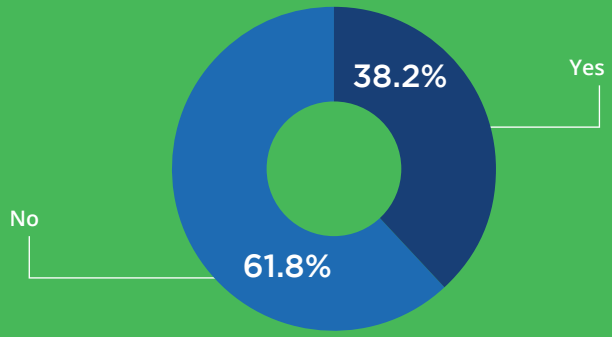
Figure 22 Statistics of endpoint protection solutions used



Has your school undertaken whole-school cyber security training?

38% of responses (21 responses) reported having had whole-school cyber security training (see Figure 23), meaning the majority of respondents' schools had not undertaken whole school cyber security training at the time of completing the survey. A lack of whole school cyber security training may have implications for the cyber security of schools.

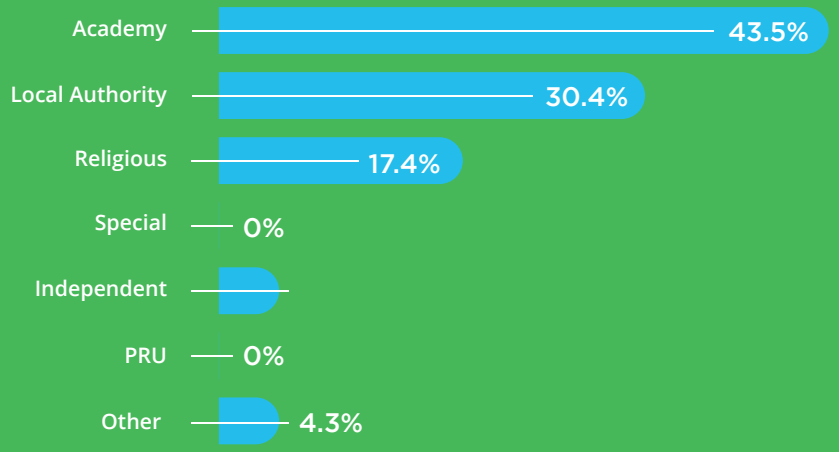
Figure 23 Statistics of schools that have undertaken whole-school cyber security training



From our sample, it appears that different types of school have had differing percentages that have had whole-school cyber security training (see Figure 24). Academies within our sample reported the highest number of schools that had whole-school cyber security training (10 responses), whereas special schools (no responses) and PRUs (no responses) reported the lowest percentages within our sample of schools which had whole-school cyber security training).

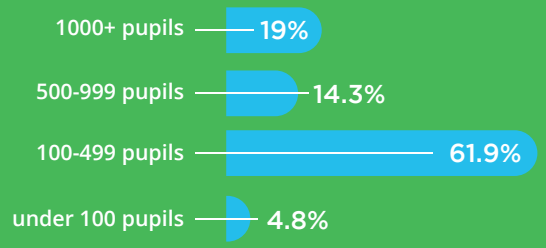
'38% of responses (21 responses) reported having had whole-school cyber security training'

Figure 24 Statistics of schools that have undertaken whole-school cyber security training per type of school



Upon examining pupil population size (see Figure 25), schools with between 100-499 pupils reported to have had whole-school cyber security training the most often (13 responses), with schools with less than 100 pupils within our sample having the highest number of responses indicating that their school had whole-school cyber security training, with 1 responses representing these schools in our sample having had whole-school cyber security training. Larger school sizes had a number of responses between 1 and 13.

Figure 25 Statistics of schools that have undertaken whole-school cyber security training per school size



Is there any extra training for 'high-risk' staff?

Extra training for 'high risk' staff was reported by only 30.9% of responses across all schools (see Figure 26), meaning that alike the provision of whole school cyber security training, most of the respondent's schools do not provide this.

Figure 26 Statistics of schools that offer extra training for 'high-risk' staff

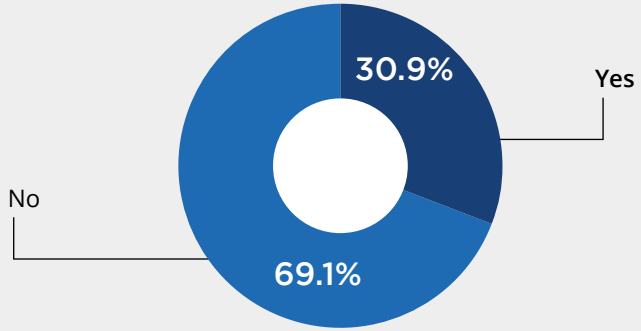
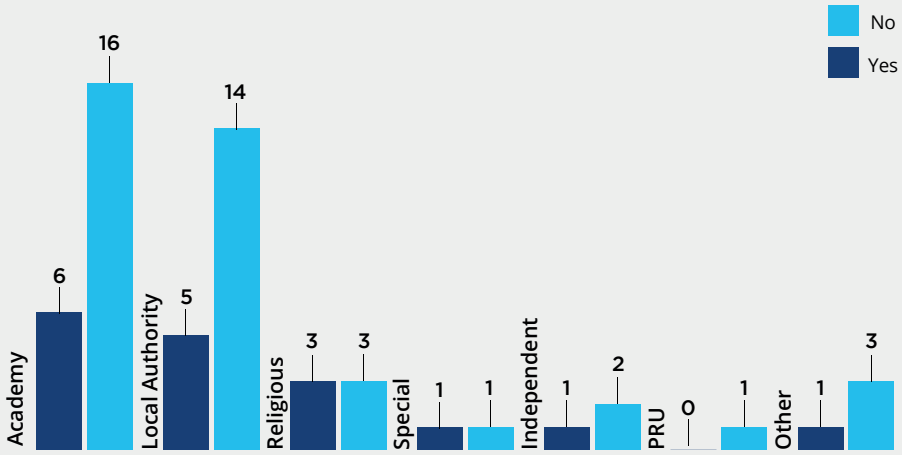
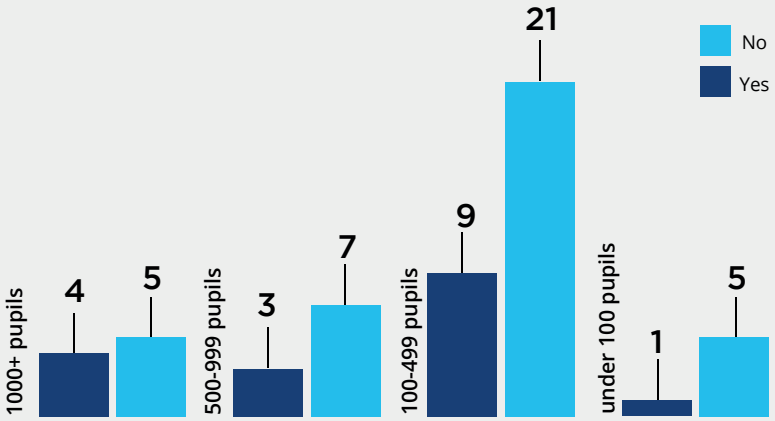


Figure 27 Statistics of schools that offer extra training for 'high-risk' staff by type of school



When examining the type of school in regards to the percentage of 'high risk' staff who are offered extra training, religious affiliated schools and special schools within our sample reported offering this more often (50%) than other schools. 26.3% of respondents from LA maintained schools and 0% of PRUs within our sample reported their school extra training to high risk staff (see Figure 27).

Figure 28 Statistics of schools that offer extra training for 'high-risk' staff by school size (pupils)

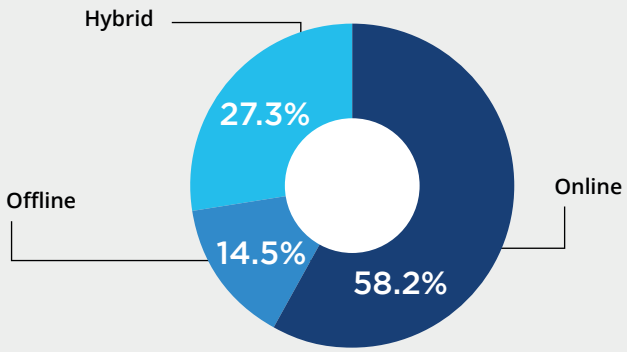


As seen in Figure 28, analysing by school size (number of pupils) also shows across all sizes of schools within our sample that most respondents indicated that their school does not provide extra training for high risk staff. This difference is particularly prominent in the schools with under 100 pupils, where only 16.7% (1 response) indicated that their school provides extra training for high risk staff. Much like the implications of not undertaking whole school cyber security training, these can be negative in regards to the cyber security of the school.

Is your cybersecurity training mostly online, offline (face to face) or hybrid?

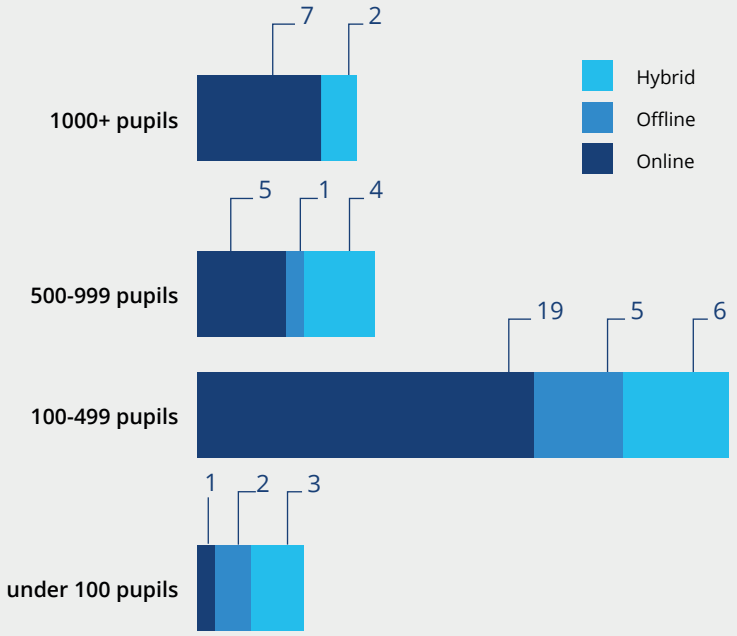
In regards to the mode of cyber security training undertaken by schools represented by respondents to the survey (Figure 29), just over half (58.2%) of respondents reported that the cyber security training they undertook was online. Only 14.5% of responses stated that the cyber security training they undertook within their school was offsite and face-to-face. In the current context of the COVID-19 pandemic, it is not surprising that many responses are indicating that training is happening online, with lockdowns over the last 2 years, many services having moved online and a move towards remote and hybrid modes of working.

Figure 29 Statistics on the mode of cyber security training undertaken



There were no observable differences in the distribution of results when analysing the mode of cyber security training by the school size for schools larger than 100 pupils. Most of the respondents from these schools indicated that their cyber security training had occurred online (31 responses) compared to offline (6 responses) or hybrid (combining elements of online and offline training) (12 responses). This is however in contrast to responses in our sample who indicated their school has less than 100 pupils. Online training was the least endorsed mode for this size of school (1 response) compared to offline training (2 responses) and a hybrid approach to training (3 responses). It is possible with fewer staff in a very small school, that offline, face to face training is more convenient compared with schools with larger staff.

Figure 30 Statistics on the mode of cyber security training undertaken per school size



Would losing access to the internet prevent you from doing your job?

76.4% of respondents reported that losing access to the internet would prevent them from doing their job.

Has the school ever been disrupted by a cyber incident or attack?

17% of schools that were within our sample reported having been disrupted by a cyber incident or attack; of these, 17%.4 of incidents occurred within the last year, and 82.6% were within the last 5 years.

Has anyone ever lost money as the result of an attack, i.e., school, parent, school staff?

8.1% (11 of 135 responses) reported that they or someone related to them (e.g., a parent, carer, member of staff) have lost money as a result of a cyber attack on their school.

Has your school ever paid a ransom to recover stolen data?

Only 1 response (of 134 responses, 0.7%) has paid a ransom to recover stolen data.

'17% of schools that were within our sample reported having been disrupted by a cyber incident or attack;'

'76.4% of respondents reported that losing access to the internet would prevent them from doing their job.'

Which of the following types of cyber attack have impacted your school?

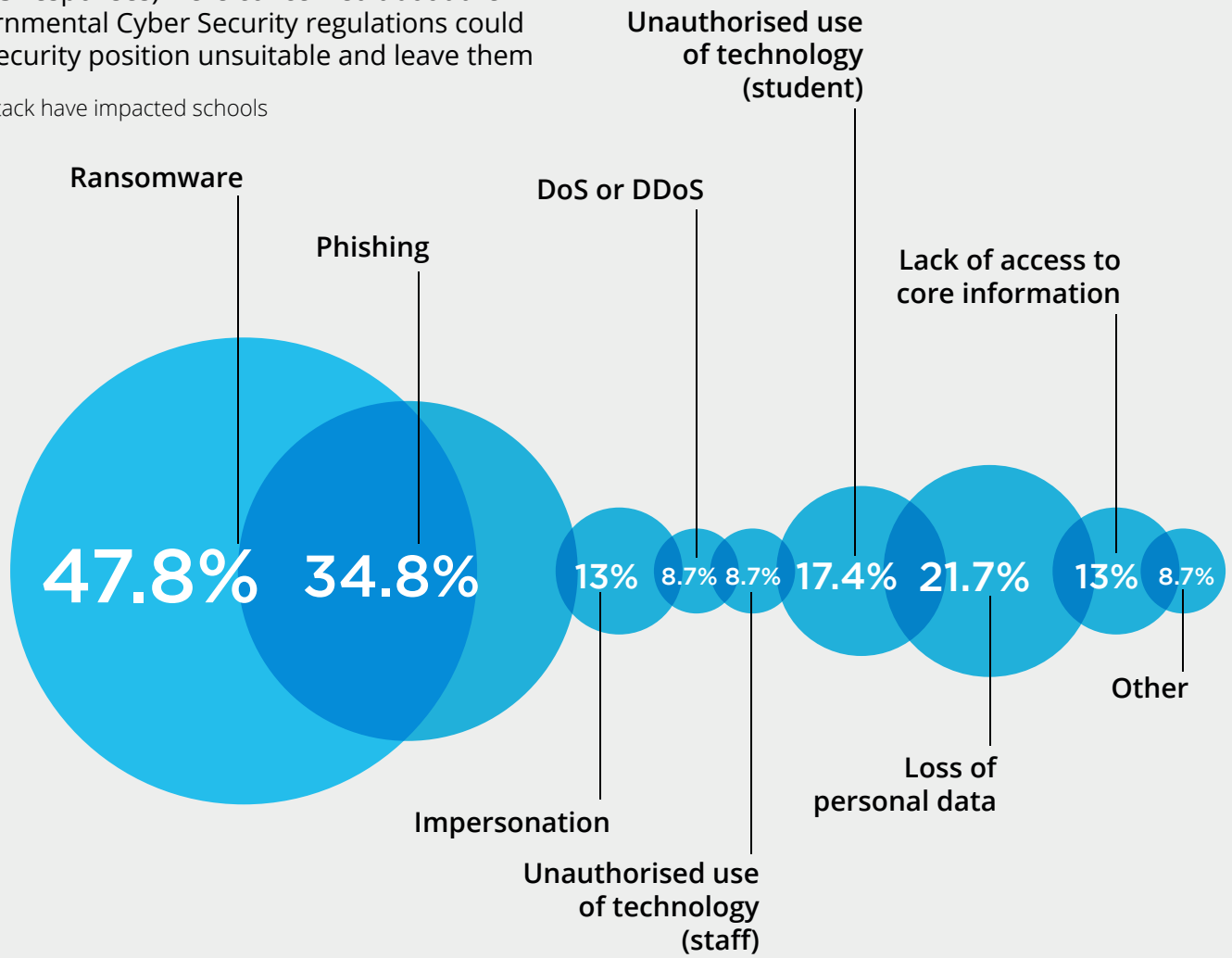
In regards to types of cyber attack have impacted schools, only 23 responses to our survey reported attacks that have impacted their school. The most common type of cyber attack was ransomware (11 responses, 47.8%). 34.8% of the reported attacks included phishing (8 responses), and 21.7% (5 responses) concerning lack of data. All types of cyber attack were endorsed by at least one respondent, which shows the diversity of cyber attacks which have targets the schools represented by the respondents to our survey.

'The most common type of cyber attack was ransomware (11 responses, 47.8%). '

Are you concerned that future as yet undecided Governmental Cyber Security regulations could render your current security position unsuitable and leave you with challenges driven by budget, resource and time constraints?

53.8% of responses (43 responses) were concerned about the potential future Governmental Cyber Security regulations could render their current security position unsuitable and leave them with challenges driven by budget, resource and time constraints. 7 responses wrote about the impact of restricted budgets and how tight current budgets currently are, including one which labelled themselves as a 'small school'. 3 responses discussed a lack of resources.

Figure 33 Types of cyber attack have impacted schools



Conclusion

SWGfL would like to thank you for reading this far and all our supporters and project funders in producing this, our first report into cyber security. We hope that this will be the first in a series exploring cyber security risks and mitigations. If you have any comments please do let us know on our socials or via our website contact form.

What does all this mean in terms of need, provision or development?

Benjamin Franklin's words "By failing to prepare you are preparing to fail." is an often used quote, but as in so many cases, it's highly relevant to cyber security in schools. Whilst there are complexities around resourcing, skills and knowledge, nevertheless, school leadership teams and school governance must recognise cyber risk as the single largest threat to education. It has the potential to severely impact attainment, finance and reputation and must, therefore, be a priority item.

Five key actions for schools:

1. Assess the risks and identify how you can reduce the impact of cyber attack on your school. Visit the SWGfL website to see how we can help you.
2. Review your current policy set. Is it fit for purpose, relevant and up to date?
3. Invest in expert advice and guidance to inform your strategy; it could save money in the long term.
4. Invest in your staff. Implement a regular approach to awareness raising – short, quick and accessible training that is compulsory for all staff. SWGfL can help you find the right way to achieve this.
5. Produce, maintain and test your risk and continuity and backup and disaster plans. Knowing what to do will improve your response to an attack.

Being cyber secure is not a static process, a do-once and forget approach.

Like many other areas of school life, continuous self-improvement is required. Cyber threats rarely stay the same for long, in the same way schools need to ensure that their systems and processes remain fit-for-purpose. Access to technology, data and the internet are so critical to successful education that doing nothing is simply not an option. The SWGfL newsletter will help you stay up-to-date.

SWGfL, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS.
www.swgfl.org.uk

University of Kent | Institute of Cyber Security for Society (iCSS)

SWGfL Safe, Secure, Online

Bitdefender®