SOPHOS
Cybersecurity evolved.

The State of Ransomware in Education 2021

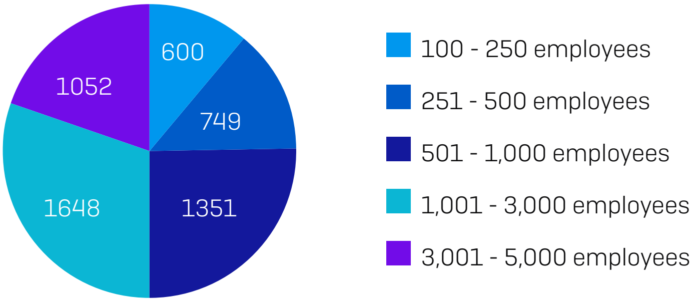
Based on an independent survey of 499 IT decision makers, this report shares new insights into the state of ransomware in the education sector. It provides a deep dive into the prevalence of ransomware in education, the impact of the attacks, the cost of ransomware remediation, and the proportion of data that education organizations could recover after an attack. The survey also reveals how education stacks up with other sectors, as well as the future expectations and readiness of education organizations in the face of these attacks.

A Sophos Whitepaper. July 2021

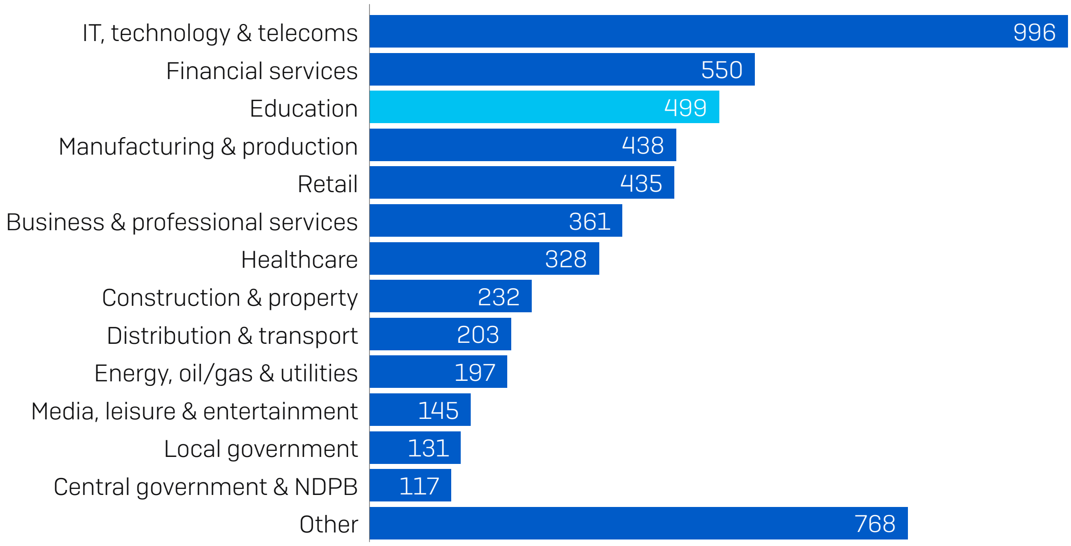
About the survey

Sophos commissioned independent research house Vanson Bourne to survey 5,400 IT decision makers across 30 countries. Respondents came from a wide range of sectors, including 499 respondents from the education sector. The survey was conducted in January and February 2021.

How many employees does your organization have globally? [5,400]



Within which sector is your organization? [5,400]



50% of the respondents in each country came from organizations with 100 to 1,000 employees, and 50% from organizations with 1,001 to 5,000 employees. The 499 education IT decision makers came from all geographic regions surveyed: the Americas, Europe, the Middle East, Africa, and Asia Pacific.

Region	# Respondents
Americas	142
Europe	138
Middle East and Africa	85
Asia Pacific	134

499 IT decision makers in education

Key findings in Education

- **44%** of organizations **were hit by ransomware in the last year**
- **58%** of organizations hit by ransomware said the cybercriminals **succeeded in encrypting their data** in the most significant attack
- **35%** of those whose data was encrypted **paid the ransom to get their data back** in the most significant ransomware attack
- The **average ransom payment** was **US$112,435**
- However, **those who paid the ransom got back just 68% of their data** on average, leaving almost a third of the data inaccessible
- The **total bill for rectifying a ransomware attack** in the education sector, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, **was, on average, US$2.73 million – the highest across all sectors surveyed**
- **55%** of those whose data was encrypted **used backups to restore data**
- **90%** of educational organizations have a **malware incident recovery plan**

2020 was a tough year for education, with the sector experiencing the highest level of ransomware attacks of all industries (tied with retail). At the same time, the rapid shift from classroom to online learning in many countries piled additional work and pressures on IT teams: nearly three quarters (74%) of respondents said cybersecurity workloads increased over 2020, the second highest rate of all sectors.

In the face of these challenges, many education organizations that were hit by ransomware paid the ransom to get their data back. In fact, the education sector has the third-highest rate of ransom payment (35%), behind energy, oil/gas and utilities (43%), and local governments (42%). However, those who paid on average only got back 68% of their data, leaving almost a third inaccessible, and just 11% got all their encrypted data back. In other words, paying the ransom doesn't really pay off!

The overall financial impact of ransomware is crippling for education organizations. The average bill for recovering from a ransomware attack is US$2.73 million, the highest by far of all sectors and 48% above the global average. This is likely due to many education organizations running outdated and fragmented IT infrastructures supported by understaffed IT teams. As a result, in the wake of an attack they are often forced to totally rebuild from the ground up, incurring major financial cost.

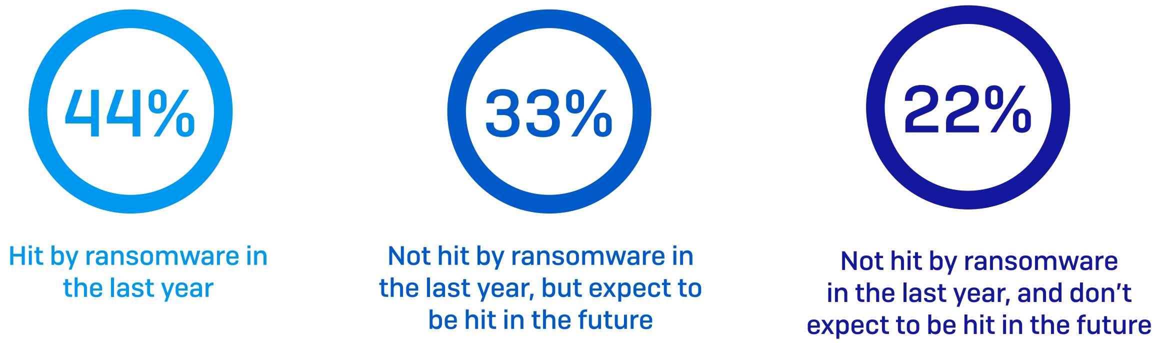
Education organizations should prioritize strengthening their defenses against ransomware. Investing in modern infrastructure, together with cybersecurity technology and skills, will considerably reduce both the overall cost and impact of ransomware.

The prevalence of ransomware in education

Education's experience with ransomware last year

When the 499 education sector respondents were asked if their organization was hit by ransomware in the last year, defined as multiple computers being impacted by a ransomware attack, but not necessarily encrypted, 44% said yes.

Educational Establishments Hit By Ransomware Last Year



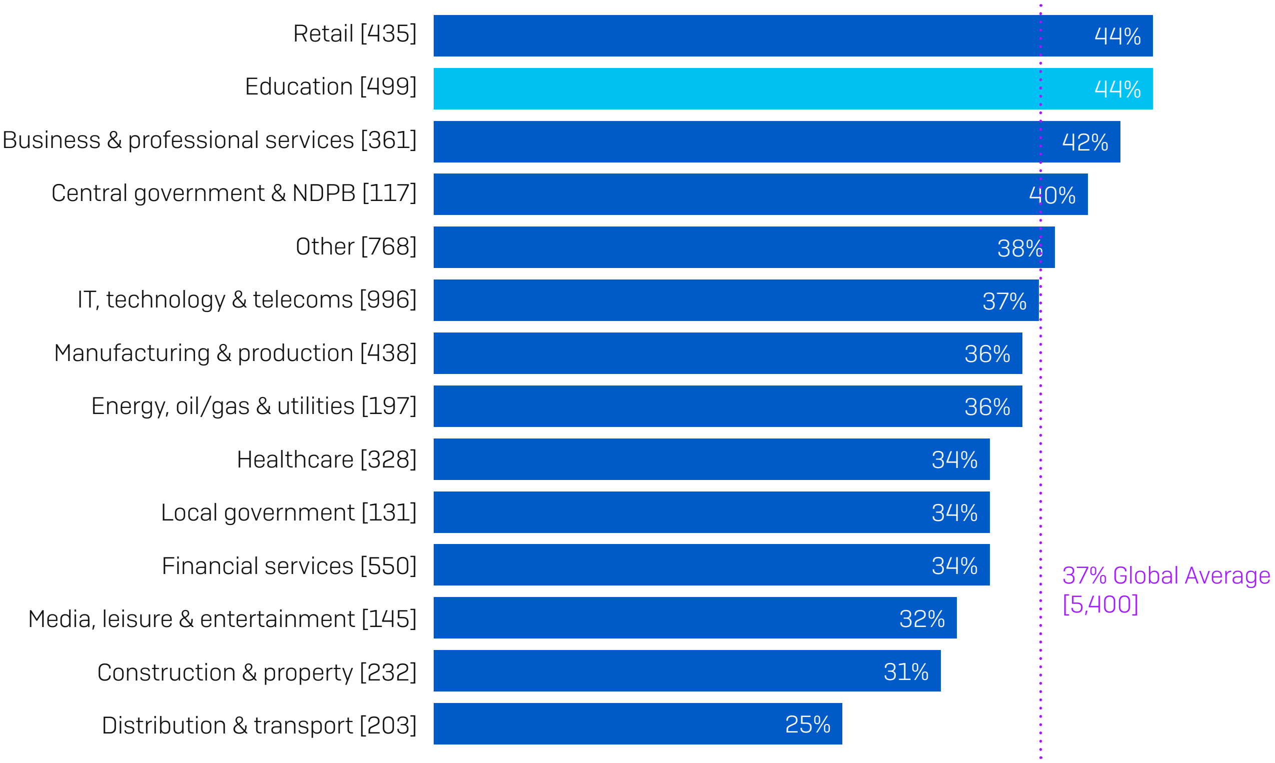
In the last year, has your organization been hit by ransomware? [499 Education respondents]

At the same time, 33% said they were not hit last year but they expect to be hit in the future – below the cross-sector average of 41%. When it comes to the percentage of respondents that weren't hit and don't expect to be hit in the future, education is in line with the cross-sector average at 22%. We'll dive deeper into the reasons behind the expectation of being hit in the future and what gives others confidence in the face of future attacks later in the report.

Education saw the highest level of ransomware attack

Looking at the prevalence of ransomware across all the sectors surveyed, **education**, along with **retail**, experienced the highest level of ransomware attacks with 44% of respondents in these sectors reporting being hit compared with a global average of 37%.

% respondents hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes [base numbers in chart] omitting some answer options, split by sector

The education sector has long been an attractive target for adversaries as it often lacks a resilient IT infrastructure. Budgets for both IT and cybersecurity are often very tight, with stretched IT teams battling to secure an outdated infrastructure with limited tools and resources. Risky online student behavior, such as downloading pirated software, also increases exposure to attack.

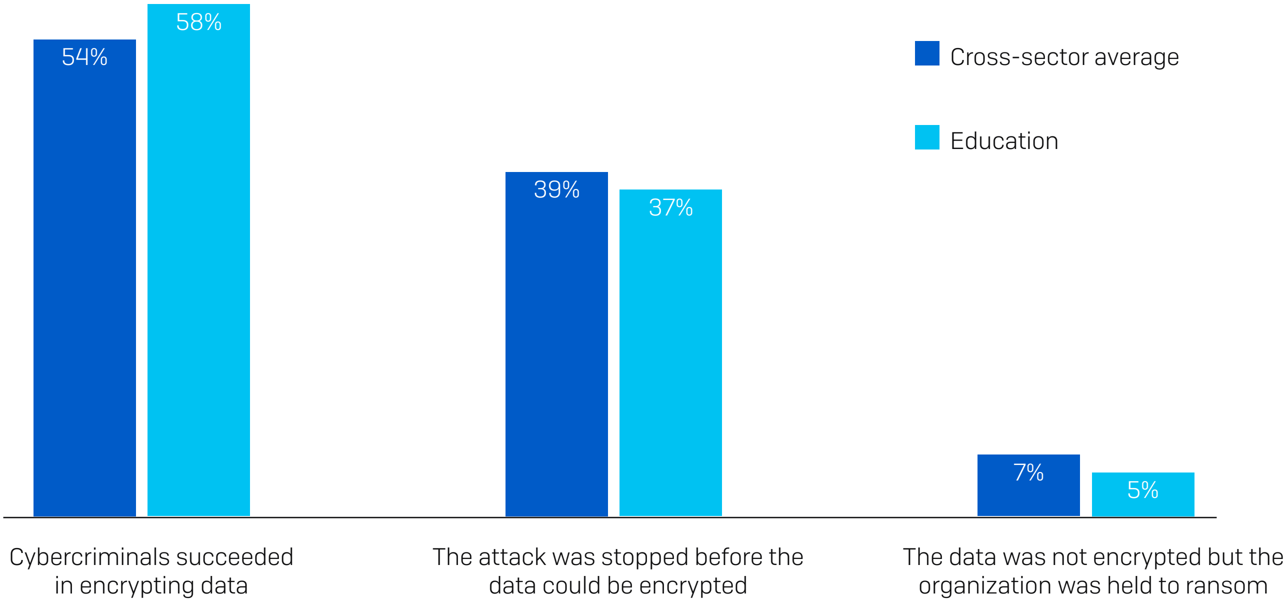
The pandemic has further exacerbated the challenge. Many education establishments switched, with short notice, from brick-and-mortar classrooms to virtual/remote learning environments, leaving IT teams little time to plan security strategies or invest in new IT infrastructure. The rapid switch also limited opportunities for cybersecurity training for teachers and students, while overloaded IT staff had limited availability to provide technical/security support.

Globally across all sectors, the percentage of organizations hit by ransomware in the last year dropped considerably from the previous year, when 51% admitted being hit. While the drop is welcome news, it's likely due in part to evolving attacker behaviors. These behaviors have been observed by SophosLabs and the Sophos Managed Threat Response team; for instance, many attackers have moved from larger scale, generic, automated attacks to more targeted attacks that include human-operated, hands-on-keyboard hacking. While the overall number of attacks is lower, our experience shows that the potential for damage from these targeted attacks is much higher.

The impact of ransomware

Attackers succeed in encrypting education data

We asked the respondents whose organizations had been hit by ransomware whether, in the most significant ransomware attack they had faced, the cybercriminals succeeded in encrypting data.



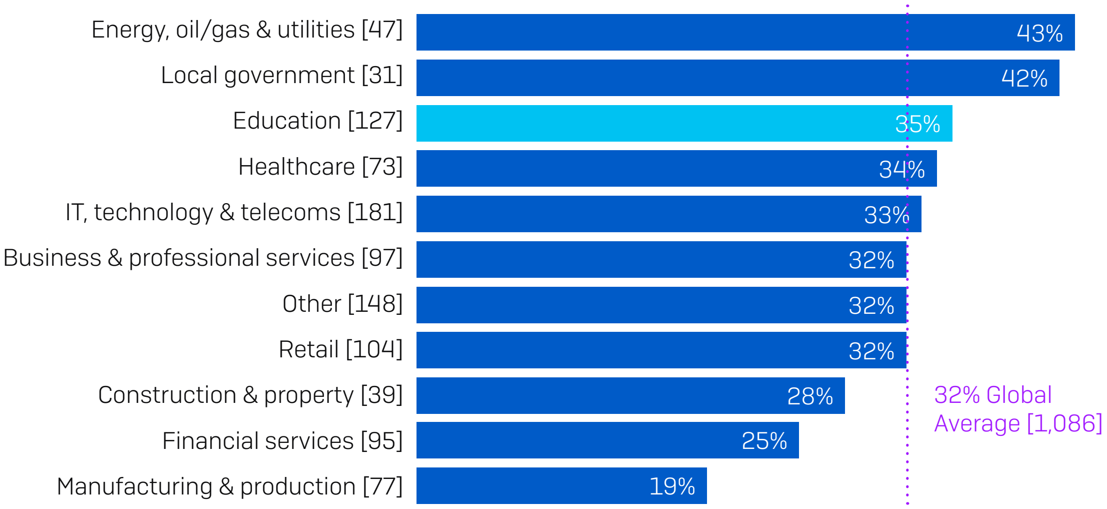
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2006 cross-sector; 219 educational establishments that have been hit by ransomware in the last year]

The survey revealed that attackers have a slightly higher success rate in encrypting data in education (58%) than the global average (54%). Educational establishments are also little less successful at stopping the encryption than the global average: 37% vs. 39%. This is likely because of the IT resource crunch and limited IT budget in most educational establishments. IT teams, already understaffed, were further stretched last year as classrooms turned into virtual learning environments due of the pandemic.

Interestingly, 5% said the data was not encrypted and yet the organization was still held to ransom. SophosLabs has seen an increase in extortion-style attacks over the last year: instead of encrypting files, adversaries steal data and threaten to publish it unless the ransom demand is paid. This requires less effort on the part of the attackers as no encryption or decryption is needed. Adversaries often leverage the punitive fines for data breaches in their demands in a further effort to make victims pay up.

Propensity to pay the ransom

% that paid the ransom to get their data back



Did your organization get the data back in the most significant ransomware attack? Yes, we paid the ransom [base numbers in chart] organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack, omitting some answer options, split by sector

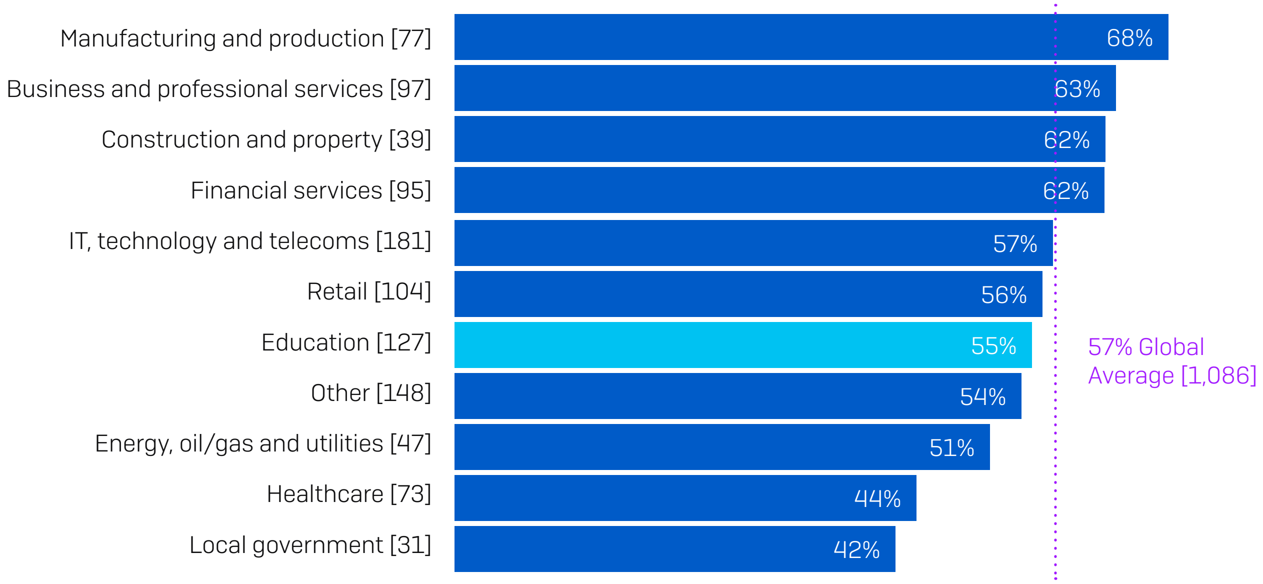
Education is one of the sectors most likely to pay the ransom, with 35% of respondents whose data was encrypted in the most significant ransomware attack admitting to paying the ransom compared with a cross-sector average of 32%. This may be due to the pressures on education teams to ensure continuity of learning, which have increased due to the pandemic. In pre-COVID times, a ransomware attack on an educational network would mean major disruption to learning. However, when learning is mostly conducted on virtual platforms, a ransomware attack can bring it to a complete stop.

Across sectors, **energy, oil/gas, and utilities** is most likely to pay the ransom, with 43% submitting to the ransom demand. This sector typically has a lot of legacy infrastructure that cannot easily be updated, so victims may feel compelled to pay the ransom to enable continuation of services.

Local government reports the second-highest level of ransom payments (42%). This is also the sector most likely (69%) to have its data encrypted. It may well be that the propensity of local government organizations to pay up is driving attackers to focus their more complex and effective attacks on this audience.

Ability to restore data using backups

% that used backups to restore encrypted data

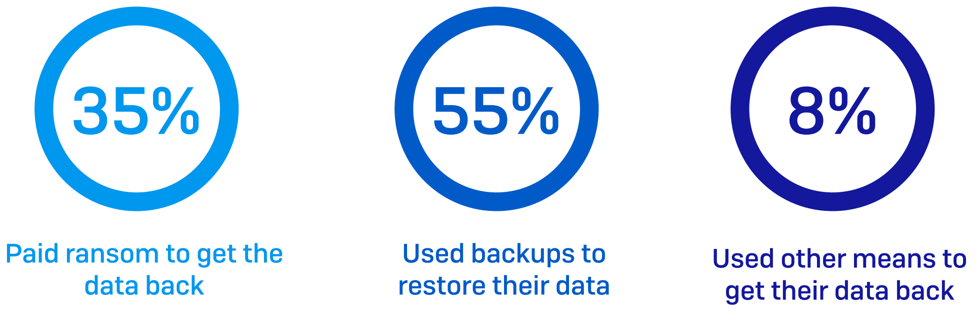


Did your organization get the data back in the most significant ransomware attack?
Yes, we used backups to restore the data [base numbers in chart] organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack, omitting some answer options, split by sector

55% of respondents in the education sector whose data was encrypted during their most significant ransomware attack were able to restore it from backups. This is in line with the global average of 57%. Backups are the best way by which encrypted data can be restored and organizations would be wise to increase their focus in this area.

98% got encrypted data back

Let’s now look at the percentage of organizations that could recover their data after it was encrypted.



Did your organization get the data back in the most significant ransomware attack? [127] Educational organizations responded.

98% of educational establishments whose data was encrypted during their most significant ransomware attack got it back. Just over a third (35%) paid the ransom, 55% used backups, and 8% used other means to get their data back.

Paying the ransom only gets you some of your data

65%

Percentage of data restored
after paying the ransom
CROSS-SECTOR AVERAGE

68%

Percentage of data restored
after paying the ransom
EDUCATION AVERAGE

Average amount of data organizations got back in the most significant ransomware attack. [44] organizations that paid the ransom to get their data back

On average, education establishments that paid the ransom got back just 68% of their data, leaving a third of their data inaccessible. This is slightly better than the global average (65%) but still leaves a considerable proportion of the data inaccessible.

11%

Got ALL their data back

32%

Got half or less of their data back

Average amount of data Education organizations got back in the most significant ransomware attack. [44] organizations that paid the ransom to get their data back

In fact, just 11% of education organizations that paid the ransom got back all their data, and 32% got back half or less of their data. Clearly paying up doesn't pay off.

The cost of ransomware

Revealed: the ransom payments

Of the 357 respondents across all sectors that reported that their organization paid the ransom, 282 also shared the exact amount paid, including 37 in the education sector.

$ 170,404

Average GLOBAL ransom payment

$ 112,435

Average EDUCATION ransom payment

How much was the ransom payment your organization paid in the most significant ransomware attack? [282/37] organizations that paid the ransom to get their data back

Globally across all sectors, the average ransom payment was US$170,404. However, in education, the average ransom payment came in almost US$58,000 lower at US$112,435. These numbers vary greatly from the eight-figure payments that dominate the headlines for multiple reasons.

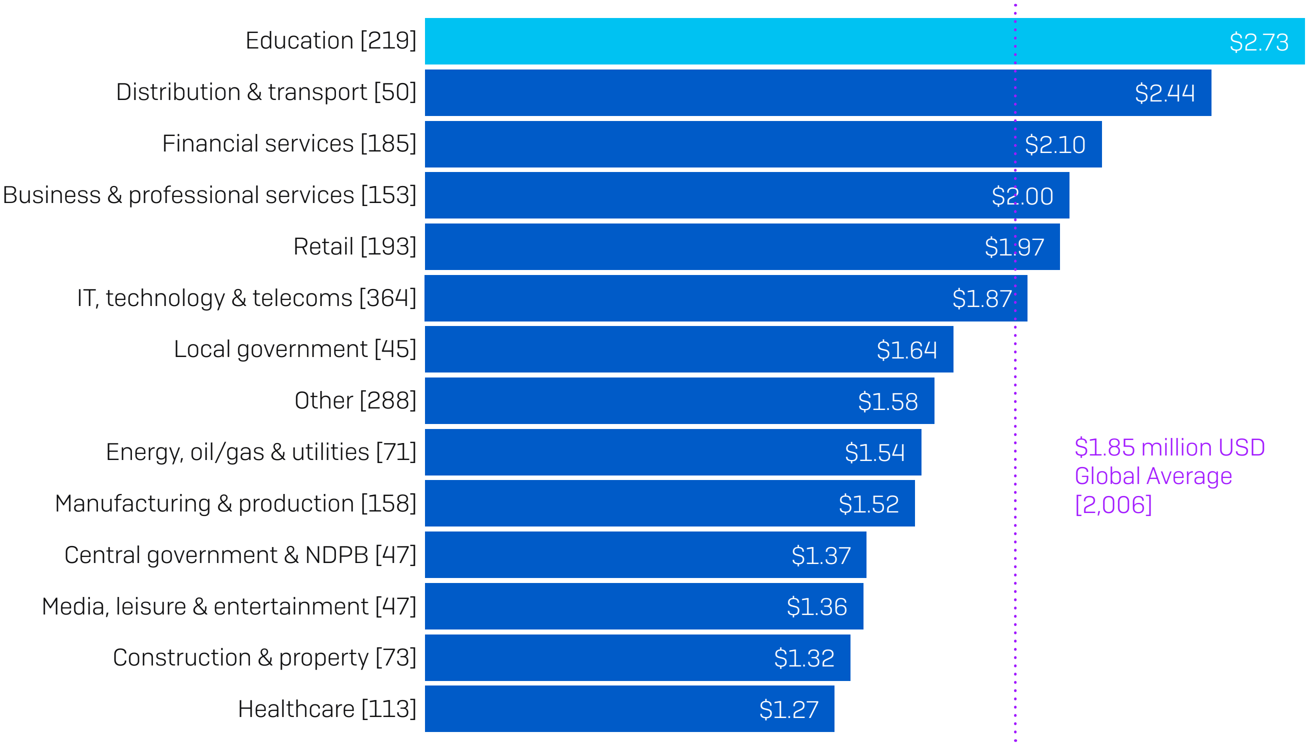
1. **Organization size.** Our respondents are from mid-sized organizations between 100 and 5,000 users who, in general, have fewer financial resources than larger organizations. Ransomware actors adjust their ransom demand to reflect their victim's ability to pay, typically accepting lower payments from smaller organizations. The data backs this up, with the average ransom payment for 100-1,000 employee organizations coming in at US$107,694, while the average ransom paid by 1,001 to 5,000 employee organizations is US$225,588.

2. **The nature of the attack.** There are many ransomware actors, and many types of ransomware attacks, ranging from highly skilled attackers who use sophisticated tactics, techniques, and procedures (TTPs) focused on individual targets, to lower skilled operators who use 'off the shelf' ransomware and a general 'spray and pray' approach. Attackers who invest heavily in a targeted attack will be looking for high ransom payments in return for their effort, while operators behind generic attacks often accept lower return on investment (ROI).

3. **Location.** As we saw at the start, this survey covers 30 countries across the globe, with varying levels of GDP. Attackers target their highest ransom demands on developed Western economies, motivated by their perceived ability to pay larger sums. The two highest ransom payments were both reported by respondents in Italy. Conversely, in India, the average ransom payment was US$76,619, less than half the global number (base: 86 respondents).

Education has the highest ransomware recovery costs

The ransom is just a small part of the overall cost of recovering from a ransomware attack. Victims face a wide range of additional expenses including the cost to rebuild and secure their IT systems, PR, and forensic analysis.



Average approximate cost to organizations to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) [base numbers in chart] respondents whose organization had been hit by ransomware in the last year, split by sector, Millions of US$

The survey revealed that the education sector experiences the highest ransomware recovery cost of all sectors, with an average remediation cost from their most recent ransomware attack of US$2.73 million (considering downtime, hours lost, device cost, network cost, lost opportunity, ransom paid, and so on). This is a massive 48% higher than the global average (US$1.85 million). The weak state of education IT infrastructure likely is a major contributor to the high cost, with organizations often needing to rebuild their IT systems from the ground up in the wake of an attack.

This learning validates the importance of investing in upgrading IT systems and cybersecurity technologies before rather than after an attack.

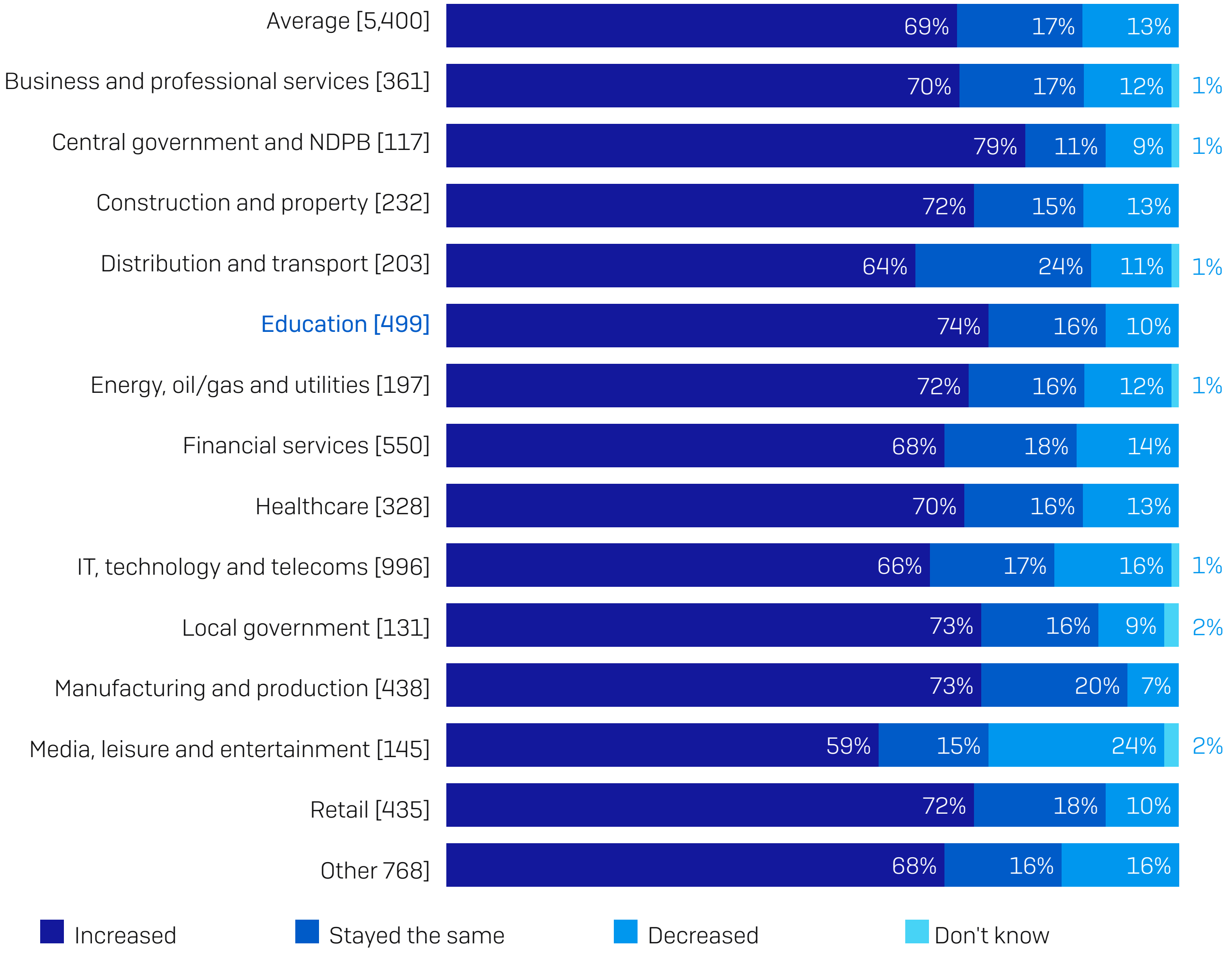
Ransomware is just a part of the cybersecurity challenge

Ransomware is a major cybersecurity issue for education organizations, but not the only one. IT teams are juggling multiple cybersecurity demands, and their challenge has been exacerbated by the pandemic.

Cybersecurity workload increased in 2020

We asked the survey respondents how their cybersecurity workload had changed over the course of 2020.

How cybersecurity workload changed over the course of 2020



Over the course of 2020, our cybersecurity workload has decreased/increased/stayed the same [base sizes in chart], split by sector.

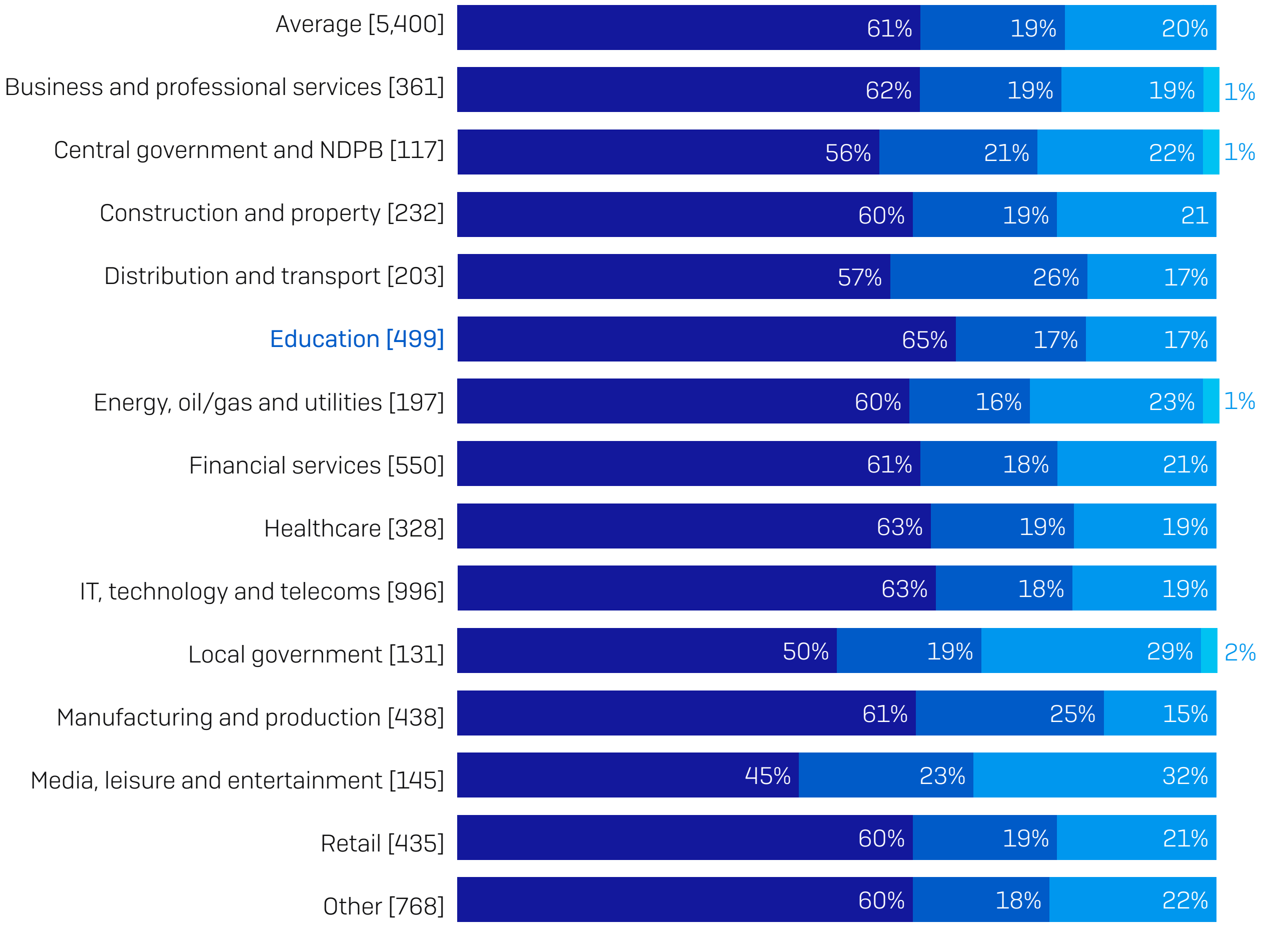
IT teams in the education sector were among the most heavily impacted by the pandemic, with 74% experiencing an increase in cybersecurity workload over the course of 2020. While the majority of respondents in all sectors reported an increase, only central government saw a greater growth in workload than the education sector.

The switch to online learning was likely a major factor behind the increased workload. IT teams needed to secure new learning platforms as well as the devices used by students and educators. The increased use of personal devices for teaching and learning further added to the challenge, with IT teams required to mitigate the risk of unpatched or risky applications that could otherwise provide an entry point to attackers.

The heavy focus on securing online teaching and learning would have likely reduced IT teams' capacity to monitor for and respond to ransomware threats.

Increased workload slowed response times

One of the consequences of the increase in cybersecurity workload over 2020 was a slowdown in response time to IT cases.



Over the course of 2020, our response time to IT cases has decreased/increased/stayed the same. [base sizes in chart], split by sector. N.B. Due to rounding, some totals are greater than 100%

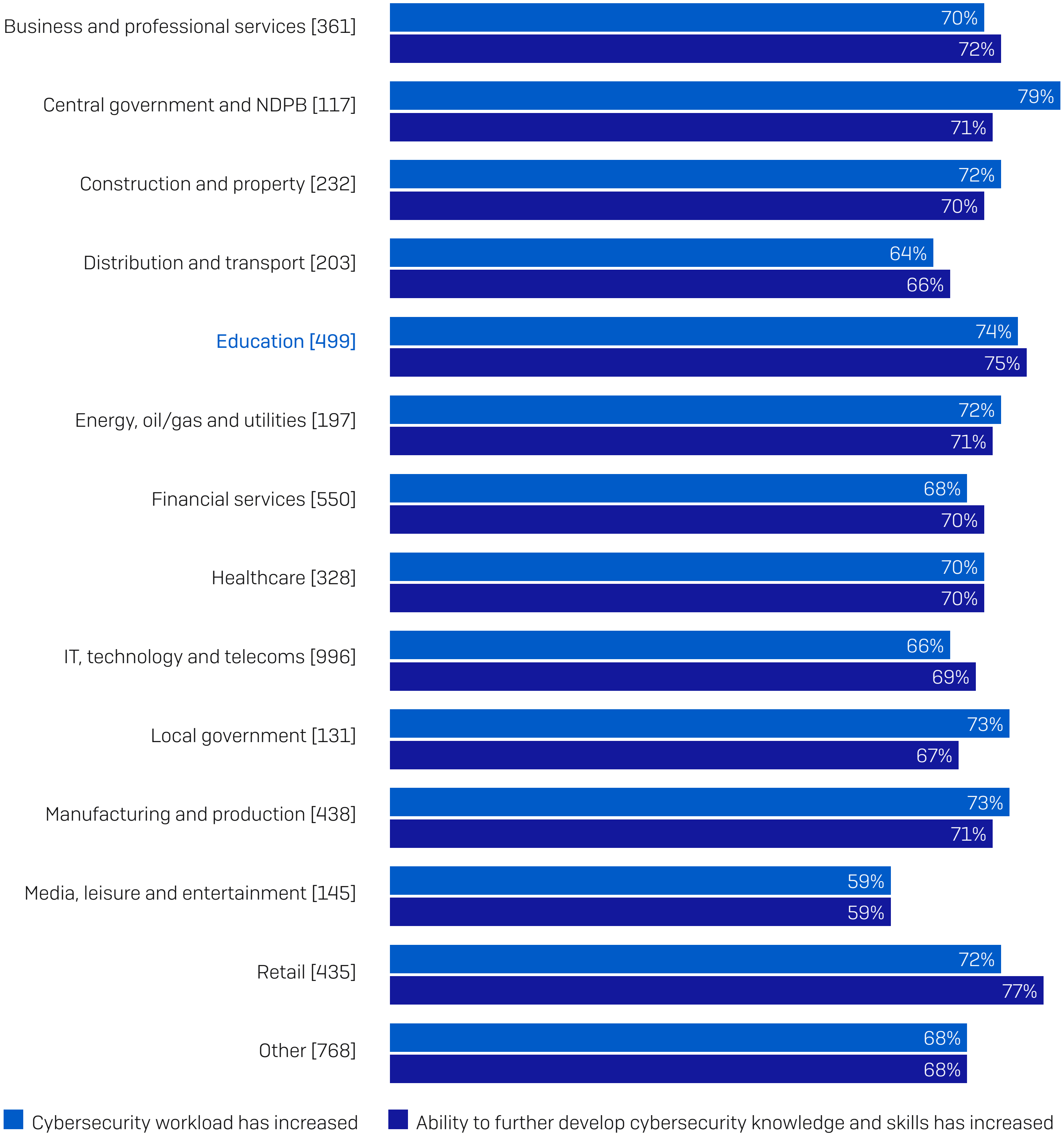
The education sector was most affected, with almost two-thirds (65%) reporting that response time increased over last year – the highest of all sectors.

When an adversary is in your environment, it's imperative to stop them as early as possible. The longer they are allowed to explore your network and access your data, the greater the financial and operational impact of the attack. The slowdown in response time is therefore a cause for alarm.

Increased workload increased knowledge and skills

Every cloud has a silver lining. There is also a link between increase in cybersecurity workload and increased ability to develop cybersecurity knowledge and skills.

Increase in cybersecurity workload and increase in ability to develop cybersecurity knowledge and skills



Over the course of 2020, our cybersecurity workload/our ability to further develop our cybersecurity knowledge and skills has increased [base sizes in chart], split by sector

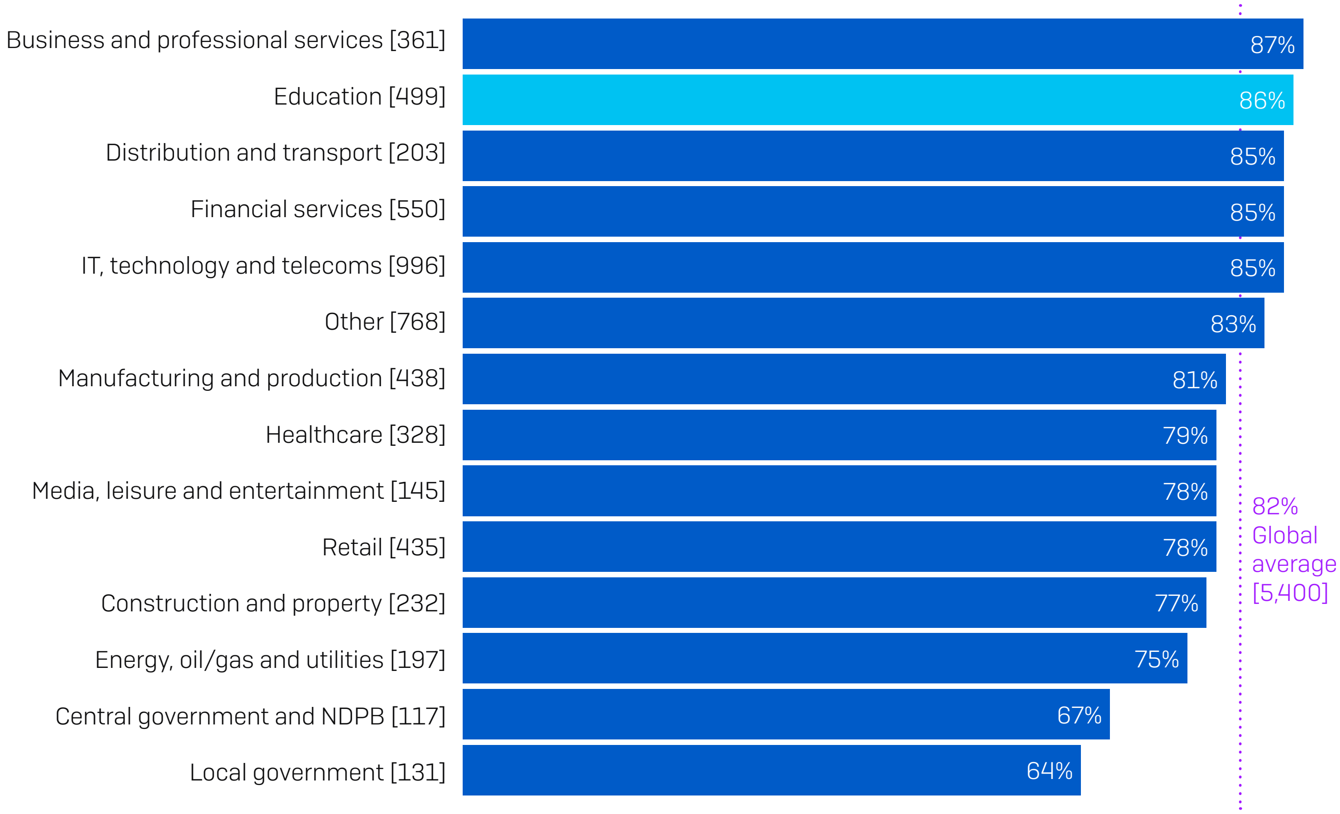
75% of IT teams in education said their ability to develop cybersecurity knowledge and skills increased over the course of 2020, the second highest after retail (77%).

While increased workload adds pressure, it also provides more opportunities to learn new things. In addition, it's likely that the unique circumstances of the pandemic also required IT teams to deliver outputs that they had never been asked for before.

Readiness to take on future challenges

Having the right tools and knowledge is key to being able to investigate and address cyberthreats.

Have the tools and knowledge to investigate suspicious activity



If I detect suspicious activities in my organization, I have the tools and knowledge I need to investigate fully: Strongly agree, Agree. Omitting some answer options [base sizes in chart], split by sector

In the face of the high level of ransomware attacks experienced by the education sector and increased cybersecurity workload, it's encouraging that 86% of education respondents say they have the tools and knowledge they need to investigate fully suspicious activities. This is a notch higher than the global average (82%) and second only to **business and professional services (87%)**.

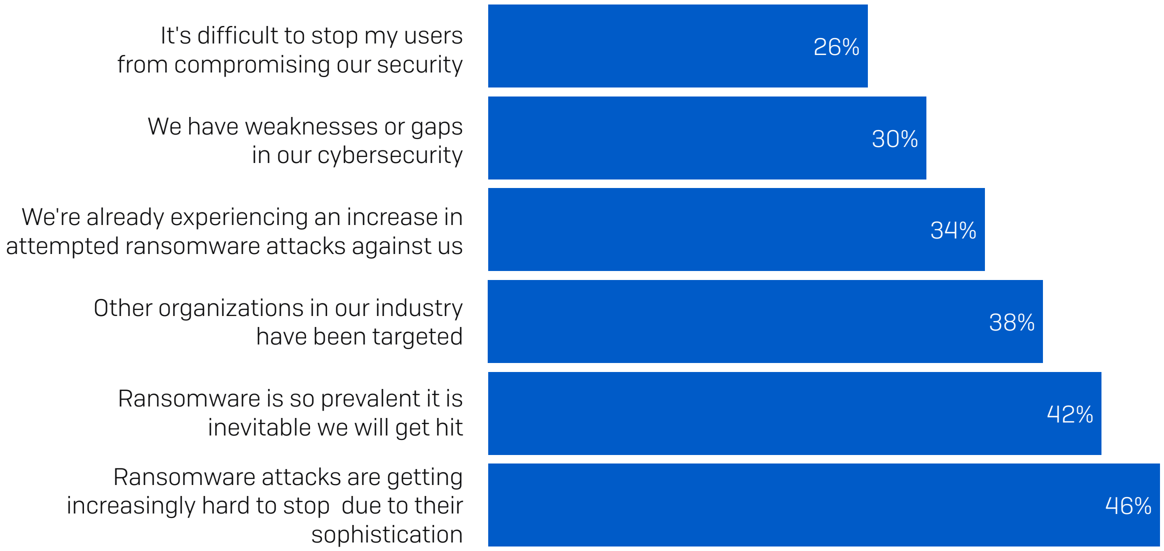
The future

Education's expectations of the future attacks

We saw at the start that 55% of respondents in the education sector were not hit by ransomware last year. Almost two-thirds (61%) expect to be hit by ransomware in the future. Conversely, 39% don't anticipate an attack.

Why the education sector expects to be hit

Among the educational establishments that weren't hit by ransomware but expect to be in the future, the most common reason (46%) is that ransomware attacks are getting increasingly hard to stop due to their sophistication.



Why do you expect your organization to be hit by ransomware in the future? [167 educational organizations that haven't been hit by ransomware in the last year but expect to be in the future, omitting some answer options]

While this is a high number, the fact that these organizations are alert to ransomware becoming ever more advanced is a good thing, and may well be a contributing factor to successfully blocking potential ransomware attacks last year.

In addition, 42% of respondents said that ransomware was too prevalent for them not to get hit.

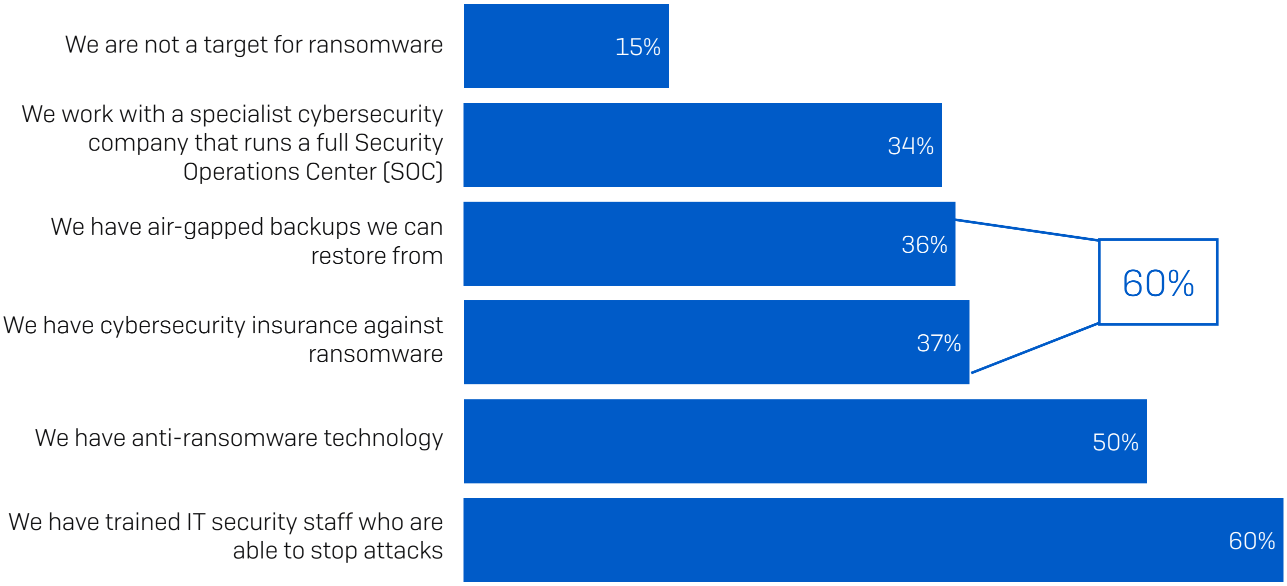
26% of respondents see users compromising security as a major factor behind why they will likely be hit by ransomware in the future. It is encouraging to see that, in the face of sophisticated attackers, most IT teams are not taking the easy option of blaming their users.

Similarly, 30% of education respondents admit to having weaknesses or gaps in their cybersecurity. While it's clearly not a good thing to have security holes, recognizing that these issues exist is an important first step to enhancing your defenses.

Why education doesn't expect to be hit by ransomware

109 education respondents said their organization was not hit by ransomware in the last year and they don't expect to be hit in the future.

Why respondents do not expect to be hit by ransomware in the future



Why do you not expect your organization to be hit by ransomware in the future? [109] Educational establishments that haven't been hit by ransomware in the last year and do not expect to be in the future, omitting some answer options

The most common factor behind this confidence is having trained IT staff who are able to stop attacks (60%), followed by the use of anti-ransomware technology (50%). In addition, 34% of education respondents who don't expect to be hit by ransomware work with a specialist cybersecurity company that runs a full Security Operations Center (SOC).

While advanced and automated technologies are essential elements of an effective anti-ransomware defense, stopping hands-on attackers also requires human monitoring and intervention by skilled professionals. Whether in-house staff or outsourced pros, human experts are uniquely able to identify some of the telltale signs that ransomware attackers have you in their sights. We strongly recommend all organizations build up their human expertise in the face of the ongoing ransomware threat.

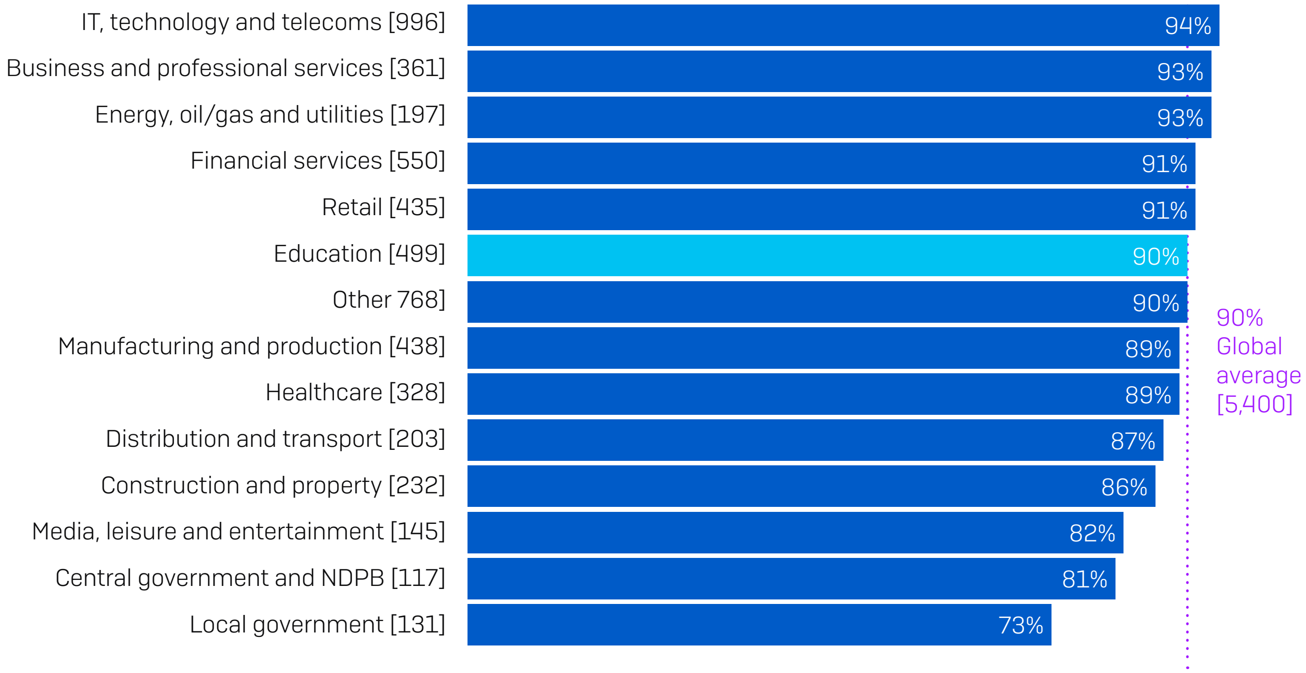
It's not all good news. Some results are cause for concern:

- 60% of education respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware.
  - 37% cited cybersecurity insurance against ransomware. Insurance helps cover the cost of dealing with an attack, but doesn't stop the attack itself.
  - 36% cited air-gapped backups. While backups are valuable tools for restoring data post attack, they don't stop you getting hit.
    N.B. Some respondents selected both the above options, with 60% selecting at least one of these two options.
- 15% believe that they are not a target of ransomware. Sadly, this is not true. No organization is safe.

Educational establishments are well prepared

Responding to a critical cyberattack or incident can be incredibly stressful. While nothing can completely alleviate the stress of dealing with an attack, having an effective incident response plan in place is a surefire way to minimize the impact.

Have a plan to recover from a major malware incident



Does your organization's Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) include plans to recover from a major malware incident? Yes, we have a full and detailed malware incident recovery plan and Yes, we have a partially developed malware incident recovery plan [base numbers in chart], omitting some answer options, split by sector

It's therefore encouraging to discover that 90% of educational establishments have a malware incident recovery plan, with just above half (51%) having a full and detailed plan and 39% having a partially developed plan. These statistics are completely aligned with the cross-sector average numbers.

Recommendations

In light of the survey findings, Sophos experts recommend the following best practices for all organizations across all sectors:

1. **Assume you will be hit**. Ransomware remains highly prevalent. No sector, country, or organization size is immune from the risk. It's better to be prepared but not hit than the other way round.

2. **Make backups**. Backups are the number one method organizations used to get their data back after an attack. And as we've seen, even if you pay the ransom, you rarely get all your data back, so you'll need to rely on backups either way.

A simple memory aid for backups is "3-2-1." You should have at least three different copies (the one you are using now plus two or more spares), using at least two different backup systems (in case one should let you down), and with at least one copy stored offline and preferably offsite (where the crooks can't tamper with it during an attack).

3. **Deploy layered protection.** In the face of the considerable increase in extortion-based attacks, it is more important than ever to keep the adversaries out of your environment in the first place. Use layered protection to block attackers at as many points as possible across your environment.

4. **Combine human experts and anti-ransomware technology.** Key to stopping ransomware is defense in depth that combines dedicated anti-ransomware technology and human-led threat hunting. Technology gives you the scale and automation you need, while human experts are best able to detect the telltale tactics, techniques, and procedures that indicate that a skilled attacker is attempting to get into your environment. If you don't have the skills in-house, look to enlist the support of a specialist cybersecurity company. SOCs are now realistic options for organizations of all sizes.

5. **Don't pay the ransom.** We know this is easy to say, but it's far less easy to do when your organization has ground to a halt due to a ransomware attack. Independent of any ethical considerations, paying the ransom is an ineffective way to get your data back. If you do decide to pay, be sure to include in your cost/benefit analysis the expectation that the adversaries will restore, on average, only two-thirds of your files.

6. **Have a malware recovery plan.** The best way to stop a cyberattack from turning into a full breach is to prepare in advance. Organizations that fall victim to an attack often realize they could have avoided a lot of cost, pain, and disruption if they had an incident response plan in place.

Further resources

The Sophos Incident Response Guide helps organizations define the framework for your cybersecurity incident response plan and explores the 10 main steps your plan should include.

Defenders may also like to review Four Key Tips from Incident Response Experts, which highlights the biggest lessons everyone should learn when it comes to responding to cybersecurity incidents.

Both resources are based on the real-world experience of the Sophos Managed Threat Response and Sophos Rapid Response teams, which have collectively responded to thousands of cybersecurity incidents.

Learn more about ransomware and how Sophos
can help you defend your organization.

2021-07-05 (SB-NP)

SOPHOS