SOPHOS
Cybersecurity evolved.

The State of Ransomware in Financial Services 2021

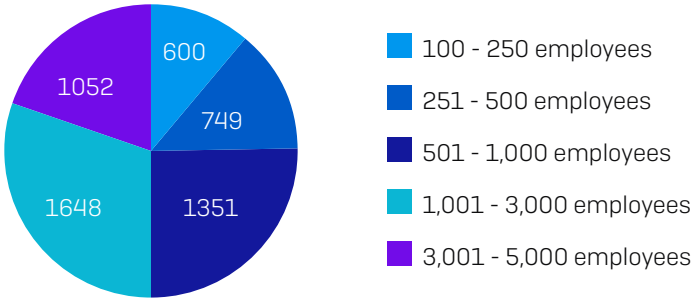
Based on an independent survey of 550 IT decision makers, this report shares new insights into the current state of ransomware in the financial services sector. It provides a deep dive into the prevalence of ransomware in financial services, the impact of those attacks on victims, the cost of ransomware remediation, as well as how the sector stacks up in terms of its future expectations and readiness against these attacks.

A Sophos Whitepaper. September 2021

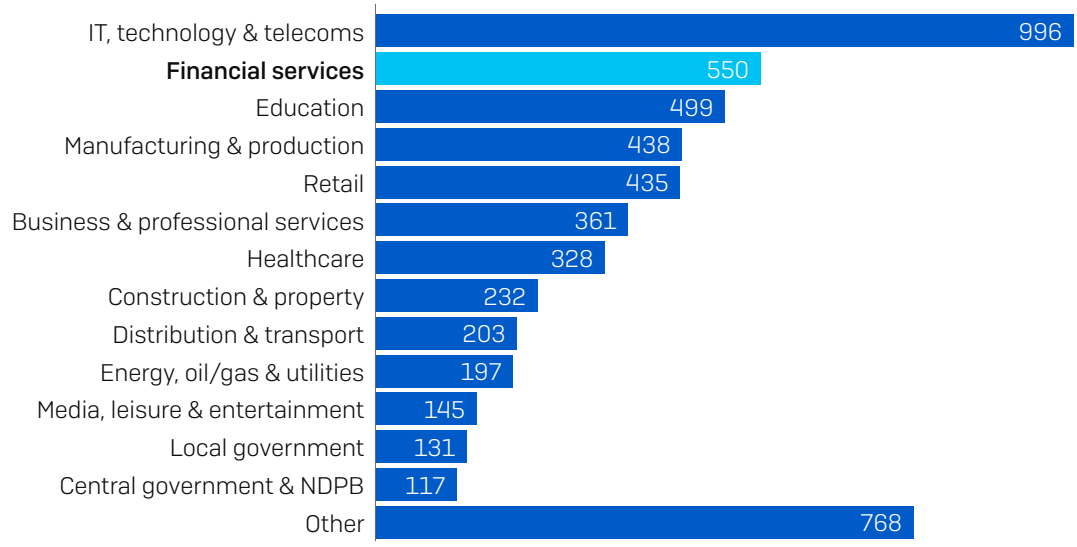
About the survey

Sophos commissioned a global survey of 5,400 IT managers across 30 countries by the independent research house Vanson Bourne. Respondents came from a wide range of sectors, including 550 respondents from the financial services sector. The survey was conducted in January and February of 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 550 financial services IT decision makers came from all geographic regions surveyed: the Americas, Europe, the Middle East, Africa, and Asia Pacific.

Region	# Respondents
Americas	146
Europe	197
Middle East and Africa	78
Asia Pacific	129

550 IT decision makers in financial services

Key findings in financial services

- **34%** of financial services organizations **were hit by ransomware in the last year**
- **51%** of organizations hit by ransomware said the **cybercriminals succeeded in encrypting their data** in the most significant attack
- **25%** of those whose data was encrypted **paid the ransom to get their data back** in the most significant ransomware attack
- **62%** of those whose data was encrypted **used backups to restore data**
- **63% of data was restored**, on average, after paying the ransom, leaving over one third inaccessible
- **91%** of financial services organizations **have a malware incident recovery plan**
- **The average bill for rectifying a ransomware attack** in the financial services sector, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, **was US$2.10 million**

Ransomware is very much a reality for the financial services industry. Approximately a third (34%) of organizations were hit by ransomware in the last year; while this is lower than the global average of 37%, it's still a major concern.

A quarter (25%) of financial services organizations whose data was encrypted paid the ransom to get their data back; again, this is lower than the cross-sector average of 32%, and likely a result of the sector's above average ability to restore data from backups. It appears that financial services are reaping the benefits of having Business Continuity and Disaster Recovery (BC-DR) plans which prepare them for situations like a ransomware attack. Given that organizations that paid the ransom got back just 63% of their data on average, financial institutions are wise to focus on backups as their primary recovery method.

Overall, the financial services sector stands out as the only sector where all organizations whose data was encrypted managed to get at least some of it back. Again, it's likely that financial organizations' disaster recovery work has prepared them well for a ransomware attack.

Financial services also come in below average when it comes to the actual ransoms paid, with an average payment of US$69,369 compared to the cross-sector average of US$170,404 (Note: The base number of respondents in financial services sector is not high enough to make robust conclusions.)

The good news stops there, however. The overall ransomware recovery cost for financial services is around a quarter of a million dollars higher than the global average (US$2.10 million vs. US$1.85 million). This is likely due to high spending on remediation measures to keep operations running at all costs, and the high costs of data breach notification, reputational damage, and regulatory fines that all impact this sector.

Furthermore, two thirds (68%) of IT teams in financial services said their cybersecurity workload increased over 2020, likely due to the need to support the rapid shift to working from home driven by the pandemic. While this would have impacted IT teams' abilities to spot and respond quickly to cybersecurity issues, the silver lining is that 70% of IT teams said their ability to develop cybersecurity knowledge and skills increased over the course of the year, putting them in good stead for the future.

Financial services organizations should continue to invest in backups and their disaster recovery efforts to minimize the impact of an attack. They should also look to extend their anti-ransomware defenses by combining technology with human-led threat hunting to neutralize today's advanced human-led attacks.

The prevalence of ransomware in financial services

Financial services hit by ransomware last year

Of the 550 financial services respondents that were surveyed, 34% were hit by ransomware in the last year, defined as *multiple computers being impacted by a ransomware attack, but not necessarily encrypted.*

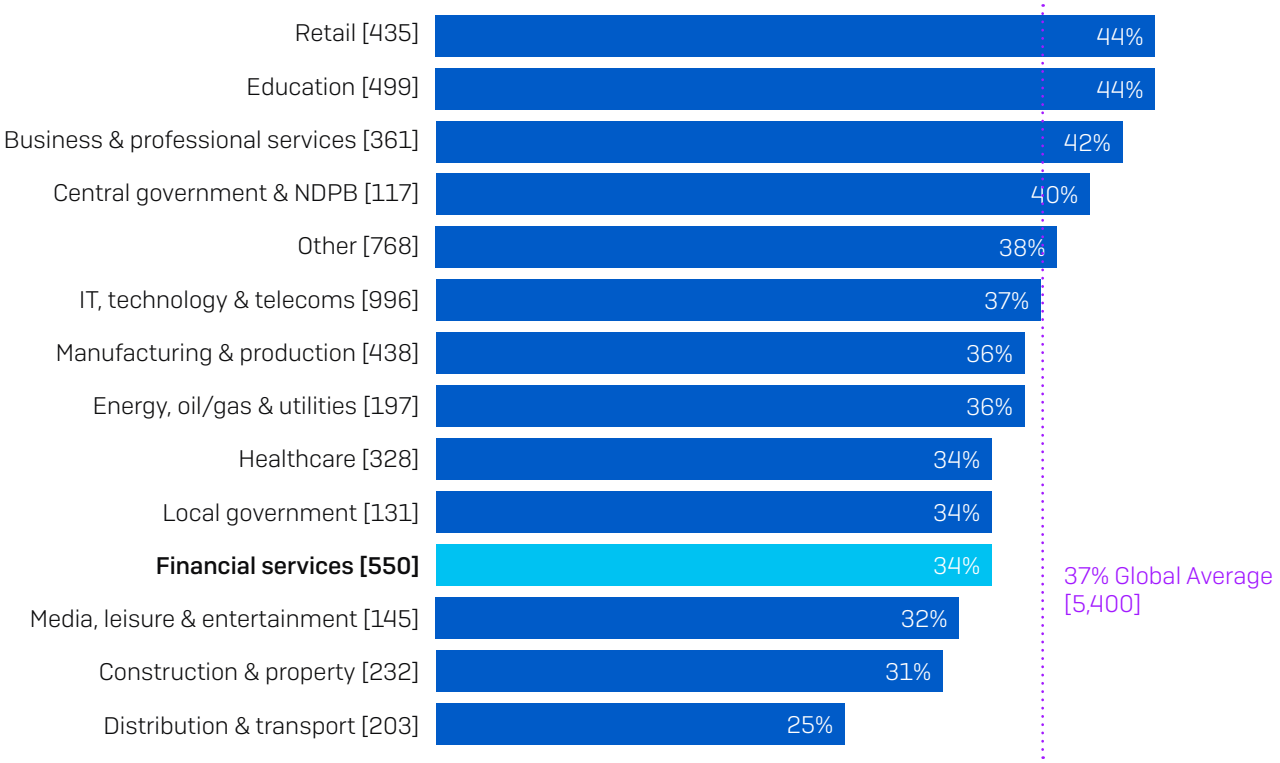
In the last year, has your organization been hit by ransomware? [550 financial services respondents]

Among the organizations not hit last year, 42% said they expected to be hit by ransomware in the future while 22% were confident that they are safe from future attacks. We'll dive deeper into the reasons behind expecting to be hit in the future as well as what gives others confidence in the face of future attacks later in the report.

Financial services below the global average for ransomware

When we compare finance with other sectors, we see that it actually experienced a below-average level of attacks. Retail and education experienced the highest level of ransomware attacks, with 44% of respondents in these sectors reporting being hit compared to the global average of 37%.

% respondents hit by ransomware in the last year



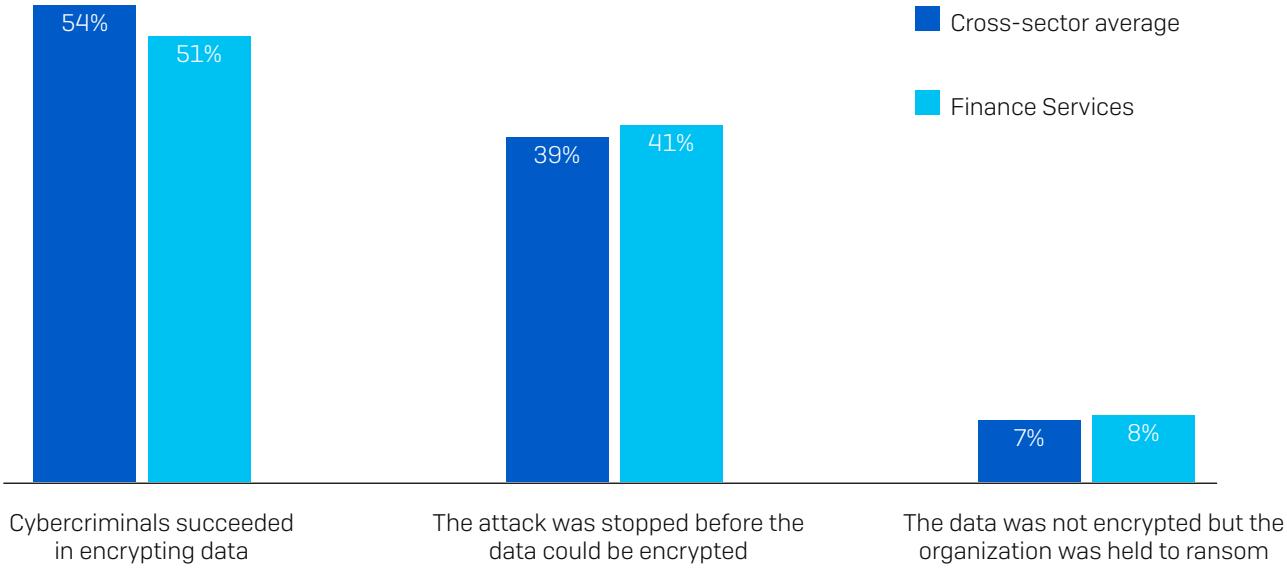
In the last year, has your organization been hit by ransomware? Yes [base numbers in chart] omitting some answer options, split by sector

Globally across all sectors, the percentage of organizations hit by ransomware in the last year has dropped considerably from last year, when 51% admitted being hit. While the drop is welcome news, it's likely due in part to evolving attacker behaviors 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

Ability of financial services to stop data encryption

We asked respondents whose organization had been hit by ransomware in the last year whether the cybercriminals succeeded in encrypting their data. 51% of financial services respondents said yes, slightly below the global average of 54%.



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2006/185 financial services organizations that were hit by ransomware in the last year]

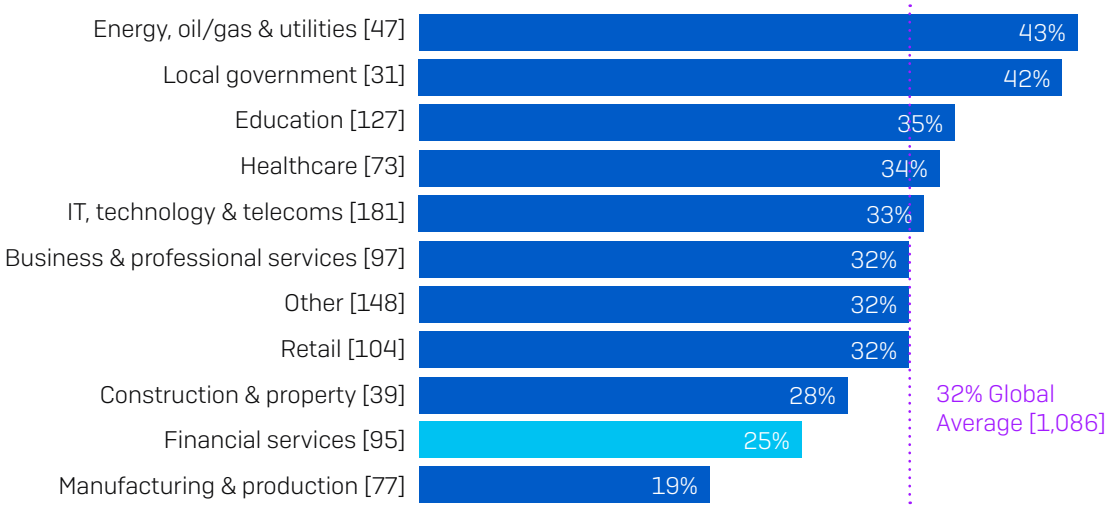
While the finance services sector was more successful at stopping encryption than the global average (41% of attacks were stopped vs. an average of 39%) this sector was vulnerable to a small but growing new trend: extortion-only attacks, where the ransomware operators don't encrypt files but threaten to leak stolen information online if a ransom demand isn't paid. In fact, 8% of financial services organizations that were hit by ransomware experienced an extortion attack.

SophosLabs has seen an increase in this style of attack over the last year. They require less effort on the part of the attackers as no encryption or decryption is needed, and 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

The survey revealed that financial services have a much lower propensity to pay the ransom than most other industries. One in four financial services organizations (25%) whose data was encrypted submitted to the ransom demand, compared to a global average of 32%. A likely reason for this, as we will discuss below, is the sector's impressive ability to restore the encrypted data using backups.

% 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

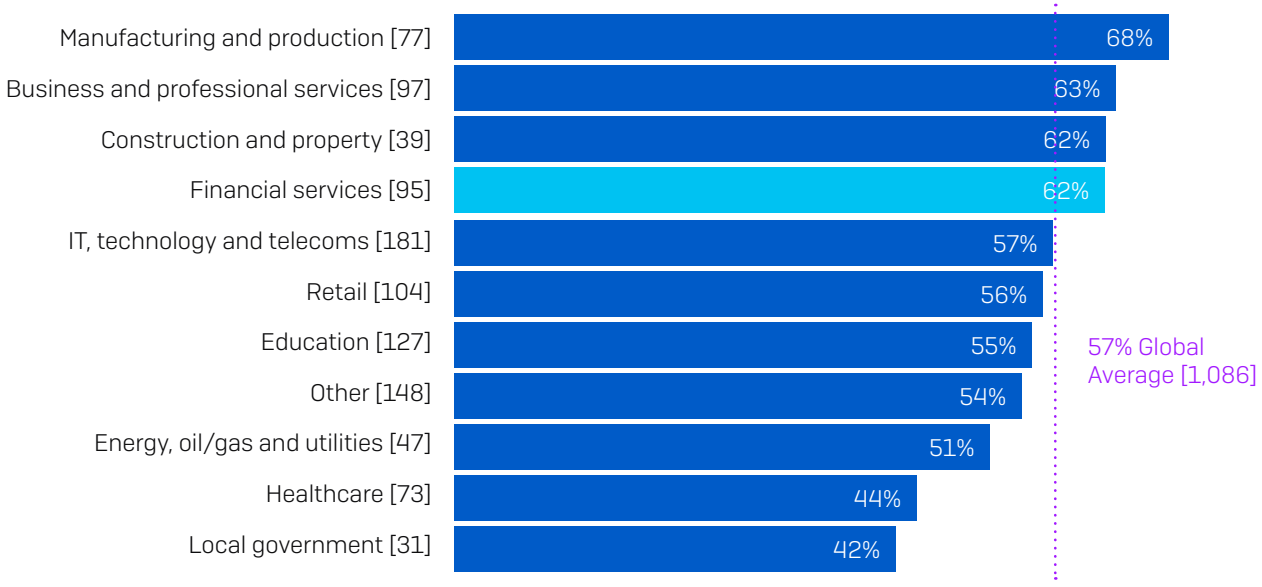
Across sectors, **energy, oil/gas, and utilities** is most likely to pay the ransom, with 43% submitting to the ransom demand. This sector typically has a lot of legacy infrastructure that cannot be easily updated, so victims may feel compelled to pay the ransom to enable continuation of services.

Local government reports the second-highest level of ransom payments (42%). This is also the sector most likely 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

When we compare this section with the previous one, the correlation between ability to restore data from backups and propensity to pay the ransom is clearly visible, with those sectors most able to use backups also the least likely to pay up.

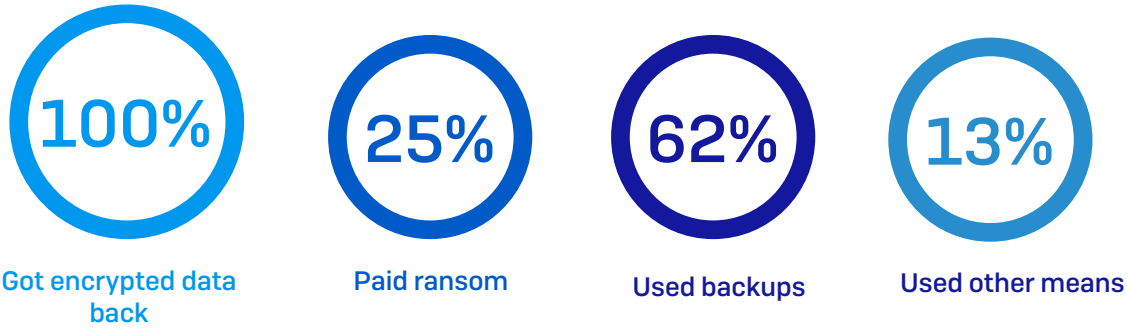
% that used backups to restore encrypted data



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

Financial services respondents (62%) were among the most capable at restoring encrypted data using backups. This is likely because banks and many other financial services organizations are required to have Business Continuity and Disaster Recovery (BC-DR) plans in order to prevent huge losses in the event of a disaster or a data breach. Not having a plan can lead to fines and/or hikes in their FDIC. Creating backups and practicing restoring data from them will be an integral part of any good plan.

Everyone in Financial Services Got Their Encrypted Data Back



Did your organization get the data back in the most significant ransomware attack? [95] financial services organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack.

The good news for financial services is that it is the only sector where every organization whose data was encrypted could get it back. As we've seen, 25% paid the ransom, 62% used backups, and 13% used other means to get their data back.

Paying the ransom only gets you some of your data

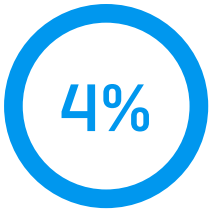
Those who paid the ransom, however, didn't get all their data back. What attackers omit to say when issuing ransom demands is that even if you pay, your chances of getting all your data back are slim.

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

Percentage of data restored after paying the ransom
FINANCIAL SERVICES AVERAGE

Average amount of data organizations got back in the most significant ransomware attack. [344/24] organizations that paid the ransom to get their data back

The base number of respondents in the financial services sector is not high enough to draw robust conclusions. However, anecdotally, financial services respondents reported getting back on average just 63% of their data after paying the ransom, leaving more than a third inaccessible. This is slightly below the global average (65%). It is likely that this is not a deliberate ploy by the attackers, but rather a reflection that adversaries focus more time and effort on developing strong encryption tools than their decryption counterparts.



Got ALL their data back

Got half or less of their data back

Amount of data organizations got back in the most significant ransomware attack. [24] financial services organizations that paid the ransom to get their data back

Further emphasizing this point, just 4% of financial services organizations that paid the ransom got back **all** their data, and 33% got back **half or less** of their data. Clearly paying up doesn't pay off. Again, the financial services base number is slightly low so should be considered indicative only.

The cost of ransomware

Revealed: the ransom payments

Of the 357 respondents across sectors who reported that their organization paid the ransom, 282 also shared the exact amount paid.

$ 170,404

Average GLOBAL ransom payment

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

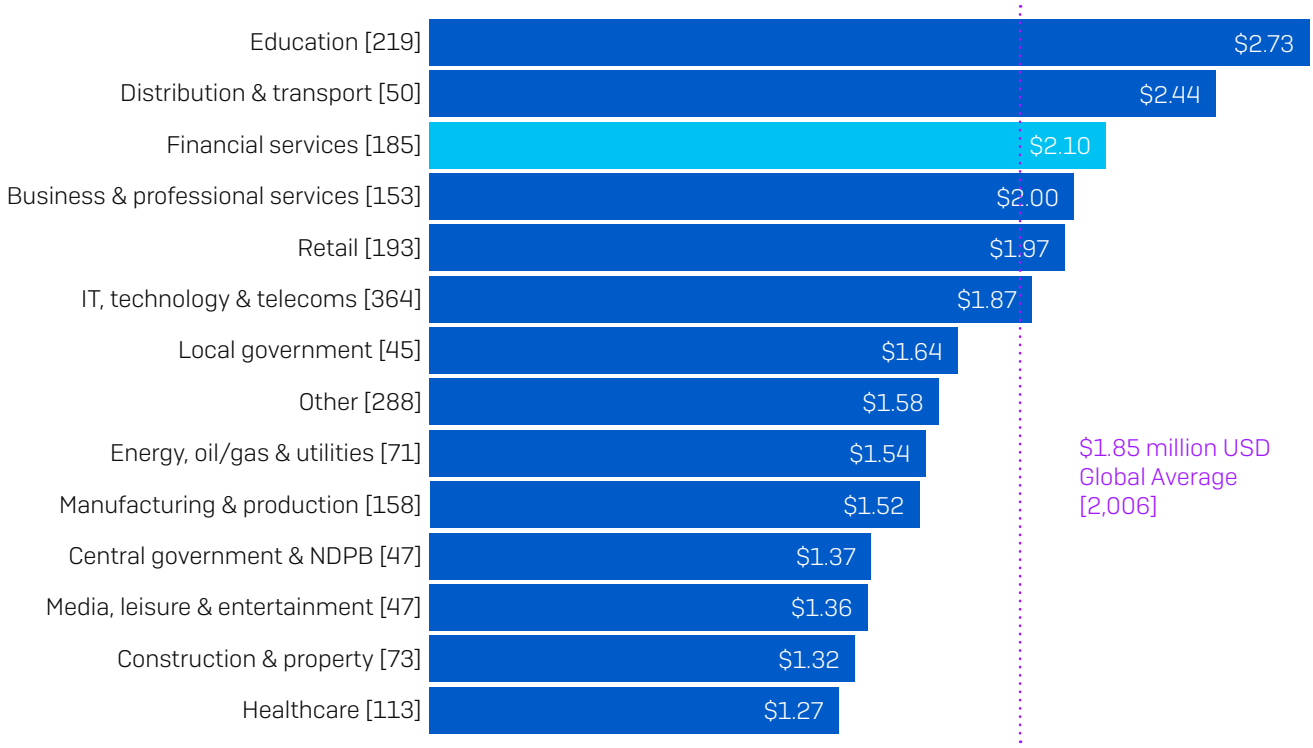
Globally **across all sectors**, the average ransom payment was US$170,404. 13 respondents in **financial services** organizations shared their actual ransom payments, with the average ransom payout coming in at US69,369, a full US$100,000 below the global average. This low payment level is likely due, in part, to the significant ability of this sector to restore data using backups. Furthermore, paying a ransom can expose financial services organizations to increased legal and compliance risk, including contravention of anti-money laundering (AMC) and Combatting Financing of Terrorism (CFT) laws.

These numbers vary greatly from the eight-figure dollar 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 companies. 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).

Ransomware recovery cost in financial services

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

The survey revealed that the financial services sector experiences an average ransomware remediation cost of US$ 2.10 million (considering downtime, hours lost, device cost, network cost, lost opportunity, ransom paid, legal and regulatory fines, and so on), which is considerably higher than the global average of US$ 1.85 million.

There are several likely factors behind this. Firstly, financial services organizations hold a large amount of highly sensitive data on individuals, businesses, and public organizations so incur high data breach notification costs as part of their remediation efforts. Secondly, disruption to the operations of financial services organizations can cause havoc around the globe. This puts huge pressure on businesses to get up and running again as quickly as possible, whatever the cost.

Additionally, financial services is among the most highly regulated industries in the world. Organizations must adhere to myriad regulations including SOX, GDPR, and PCI DSS that all have huge penalties for non-compliance. Punitive fines for data breaches incurred as part of a ransomware attack add to the overall recovery costs.

And lastly, with clients often able to switch providers easily, financial services organizations are fully exposed to business impact of reputational damage including lost customers and cancelled accounts.

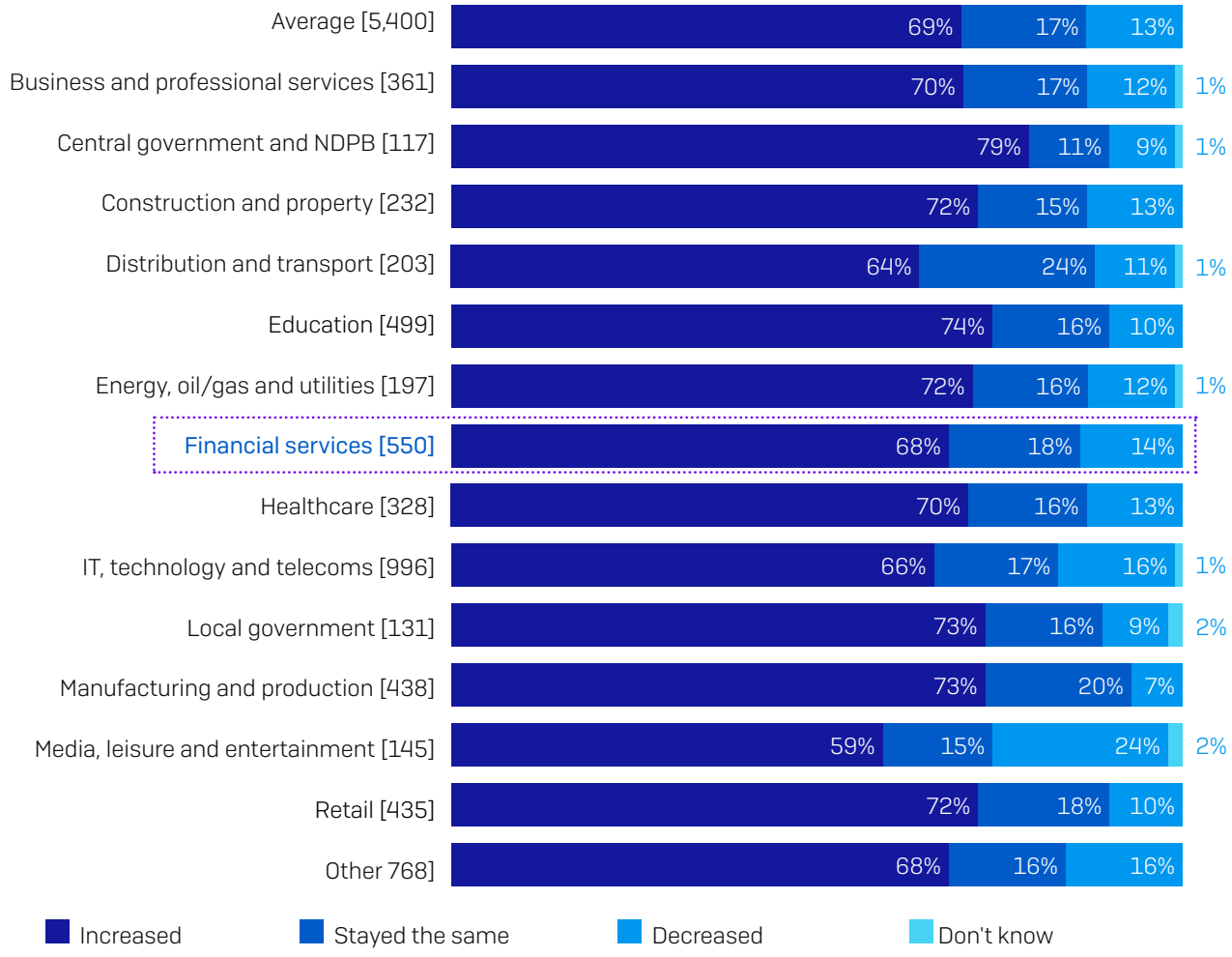
Ransomware is just a part of the cybersecurity challenge

Ransomware is a major cybersecurity issue for financial services 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

IT teams in the financial services sector were heavily impacted by the pandemic, with 68% experiencing an increase in cybersecurity workload over the course of 2020. While the majority of respondents in all sectors reported an increase, central government saw the most increase in growth in workload.

How cybersecurity workload changed over the course of 2020



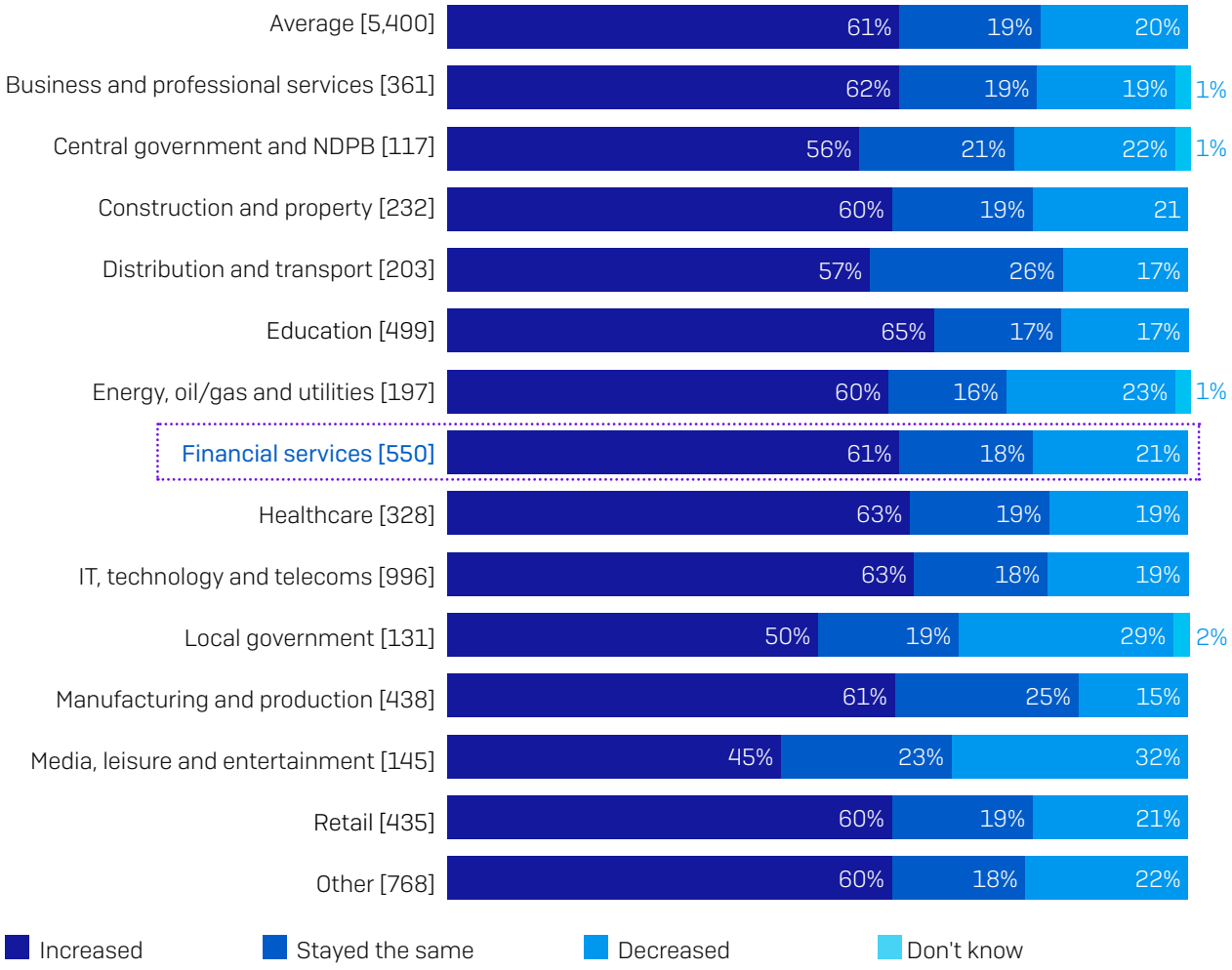
Over the course of 2020, our cybersecurity workload has decreased/increased/stayed the same [base sizes in chart], split by sector

The rapid move to remote working and the need to roll out additional services and solutions for employees as well as the customers in order to remain operational was likely a major factor behind the increased workload with IT teams. The heavy focus on securing new online platforms 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 slow-down in response time to IT cases. The financial services sector was considerably affected, with 61% respondents reporting that response time increased over last year.

Changes in response time to IT cases over the course of 2020



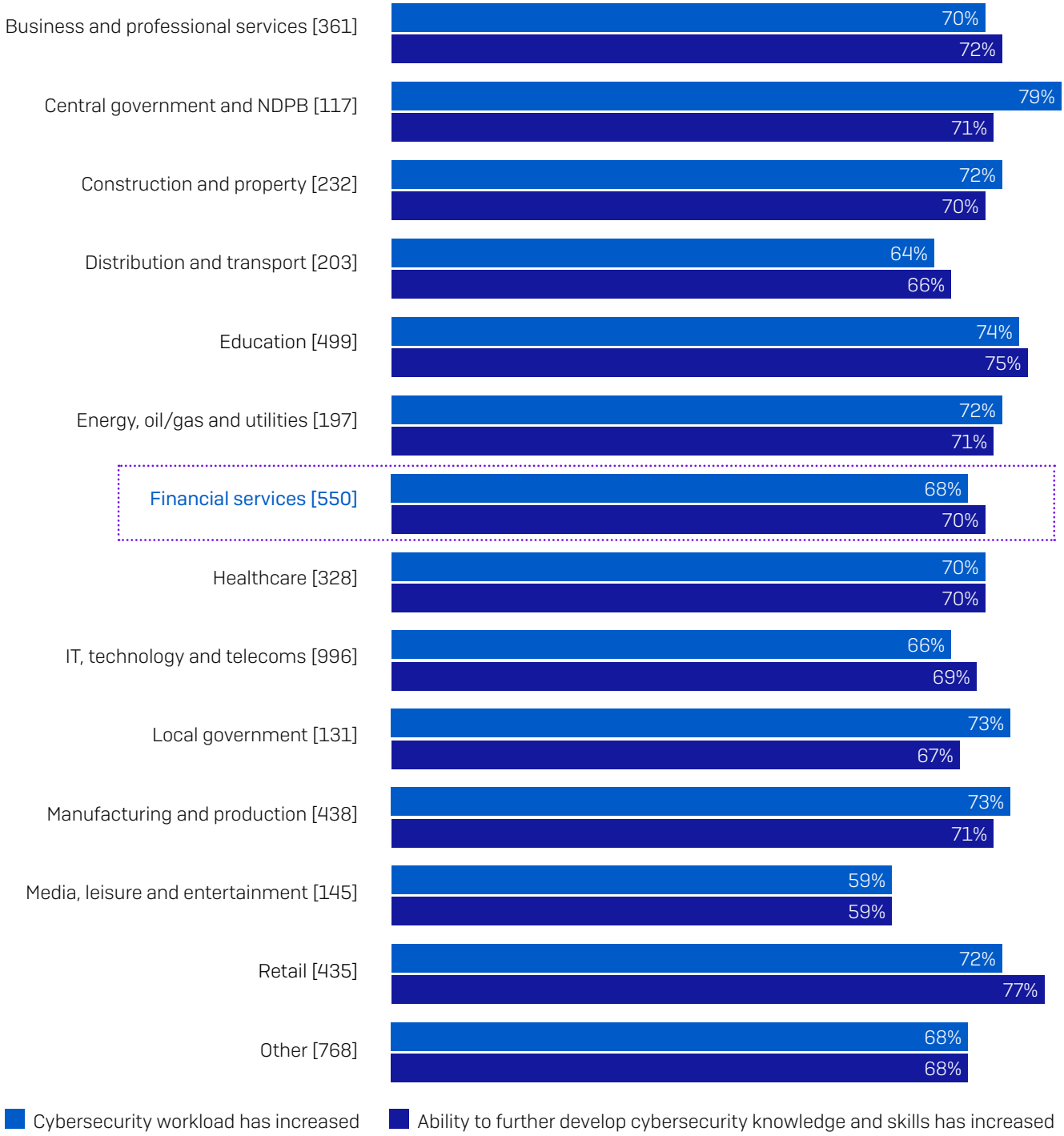
Over the course of 2020, our response time to IT cases has decreased/increased/stayed the same. [base sizes in chart], split by sector

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 slow-down 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 clear correlation 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

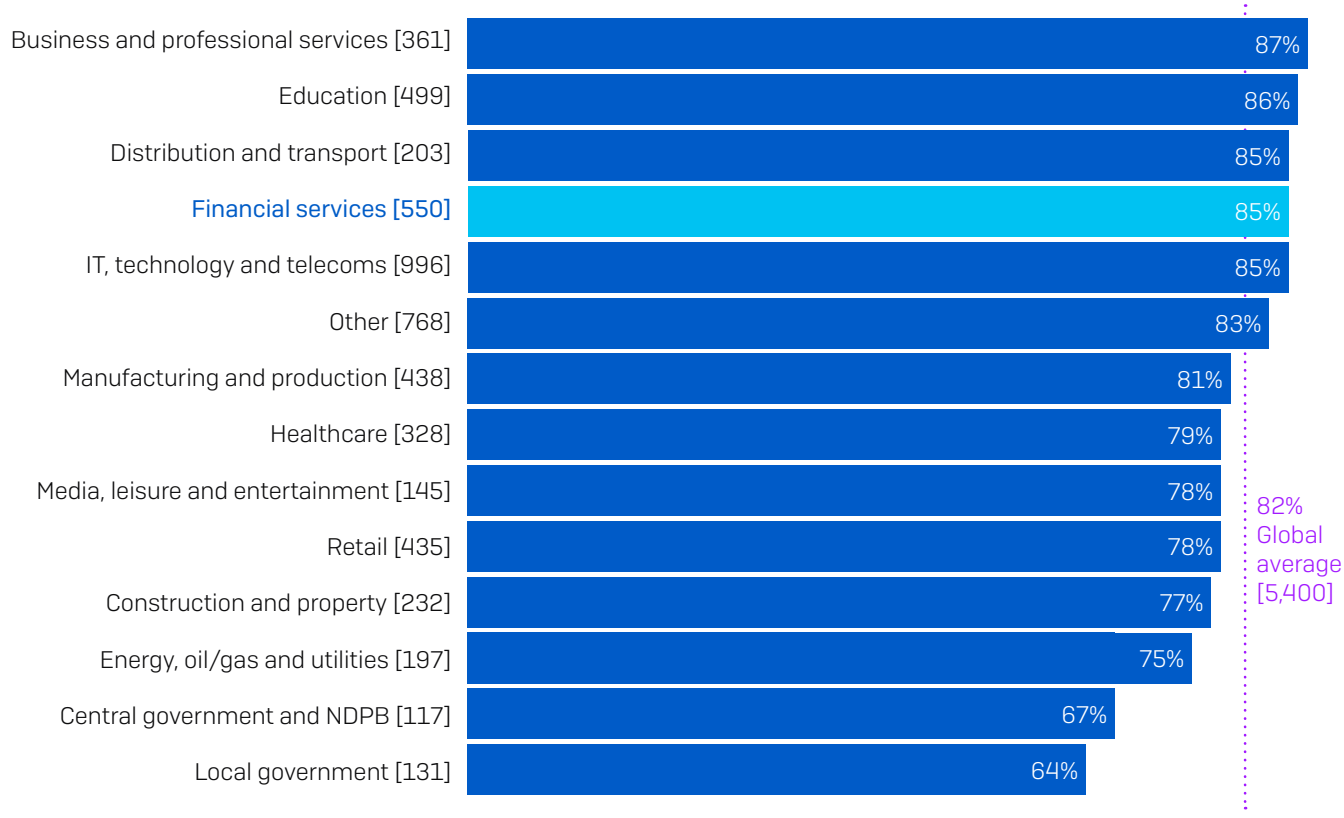
70% of IT teams in financial services said their ability to develop cybersecurity knowledge and skills increased over the course of 2020.

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

Readiness to take on future challenges

85% of respondents in financial services agree that if they detect suspicious activities in their organization, they have the tools and knowledge they need to investigate fully – higher than the global average (82%). This is great news for this sector given the increased cybersecurity workload in this sector. 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

The future

Financial services's expectations of future attacks

Expect to be hit
by ransomware in future

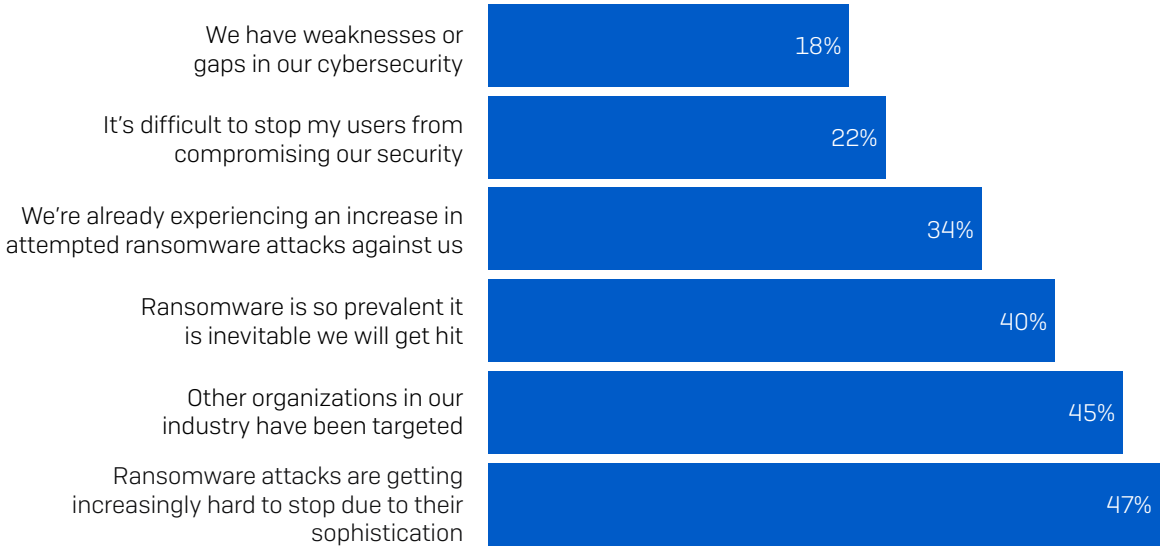
Don't expect to be hit
by ransomware in future

[550] Financial services respondents who answered "No" to the question "In the last year, has your organization been hit by ransomware?"

We saw earlier in this report that 63% of respondents in the financial services sector were not hit by ransomware last year. 42% expect to be hit by ransomware in the future. Conversely, 22% don't anticipate an attack.

Why the financial services sector expects to be hit

Among the financial services organizations that weren't hit by ransomware but expect to be in the future, the most common reason (47%) is that ransomware attacks are getting increasingly hard to stop due to their sophistication. 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 them being able to successfully block any potential ransomware attack last year.



Why do you expect your organization to be hit by ransomware in the future? [229 financial services organizations that haven't been hit by ransomware in the last year but expect to be in the future, omitting some answer options]

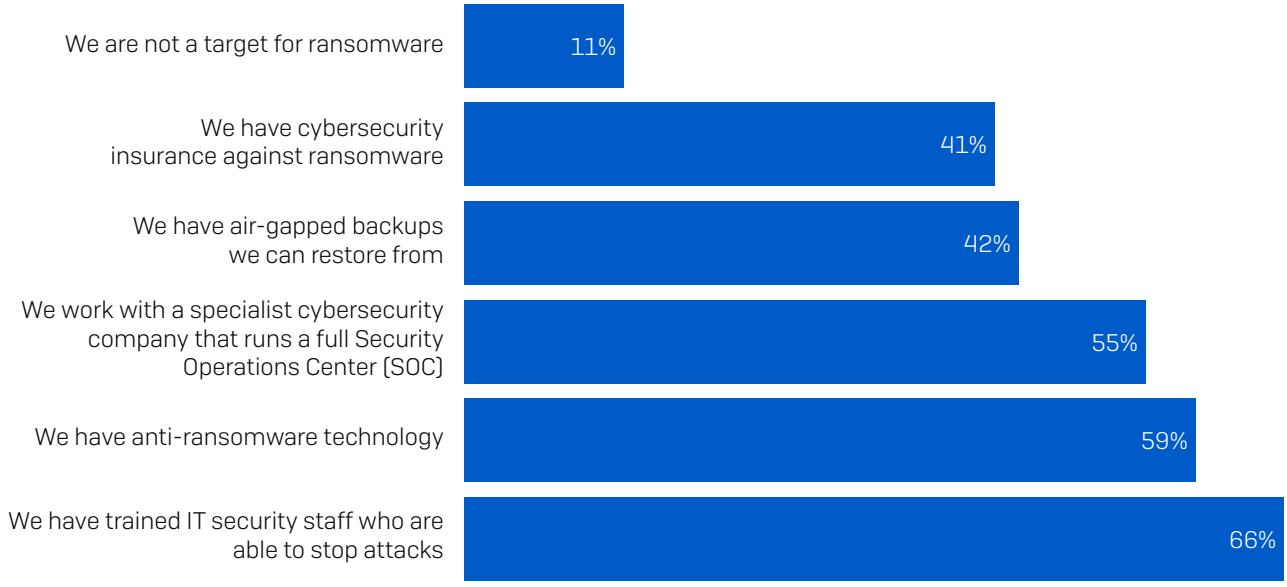
In addition, 45% of respondents said other organizations in their industry have been targeted, increasing their probability to be hit.

22% 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, 18% of financial services 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 the financial services sector doesn't expect to be hit by ransomware

119 financial services 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 do you not expect your organization to be hit by ransomware in the future? [119] financial services 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 number one reason for this confidence is having trained IT staff who are able to stop attacks (66%), followed by the use of anti-ransomware technology (59%). 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.

55% of financial services respondents who don't expect to be hit by ransomware work with a specialist cybersecurity company that runs a full Security Operations Center (SOC). It is encouraging to see that organizations are outsourcing cybersecurity expertise when needed, extending their protection.

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

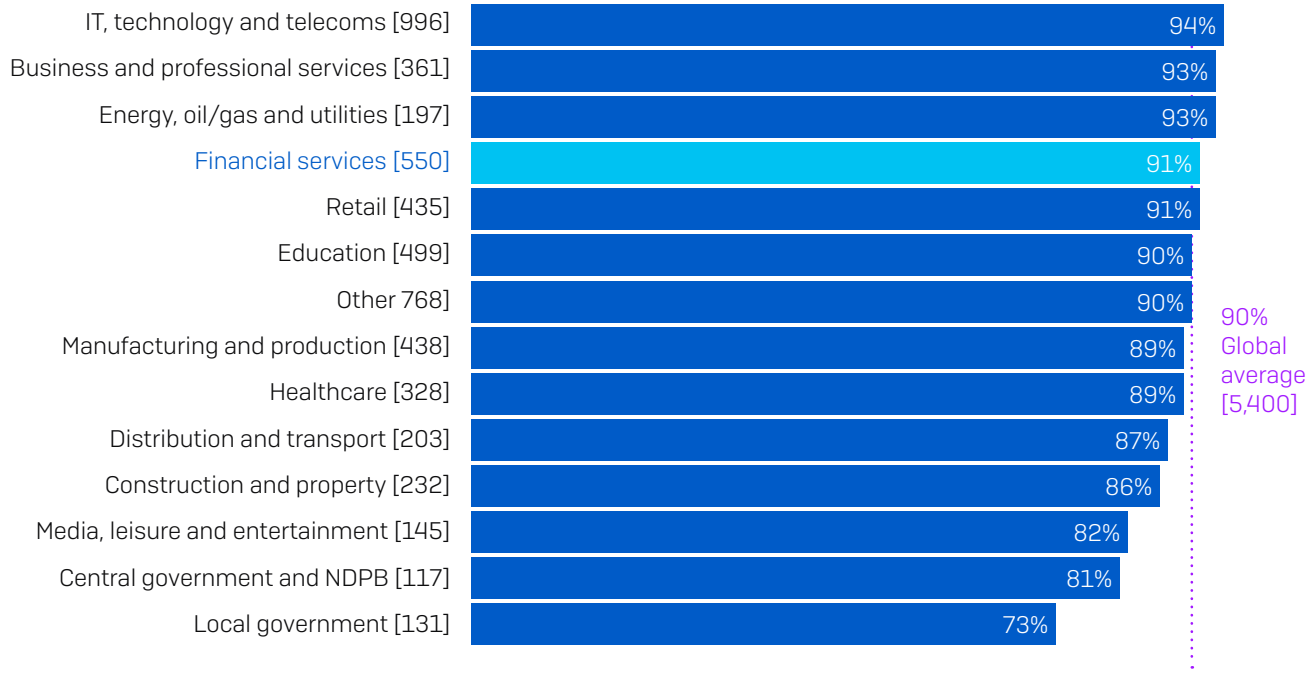
- 61% of financial services respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware.
  - 41% cited cybersecurity insurance against ransomware. Insurance helps cover the cost of dealing with an attack, but doesn't stop the attack itself.
  - 42% 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 61% selecting at least one of these two options.
- 11% believe that they are not a target of ransomware. Sadly, this is not true. No organization is safe.

Financial services organizations 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.

% who 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 91% of financial services organizations have a malware incident recovery plan, with just over half (51%) having a full and detailed plan and 40% having a partially developed plan. These statistics are aligned with the cross-sector average numbers (90%).

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**. The 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 when 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.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2021-09-1 (SB-MP)

SOPHOS