THE STATE OF RANSOMWARE 2020

Results of an independent Sophos study of 5,000 IT managers across 26 countries.

We're pleased to share this research report conducted and written by our partner, Sophos

A Sophos white paper July 2020

Introduction

Stories of organizations crippled by ransomware regularly dominate the IT news headlines, and accounts of six- and seven-figure ransom demands are commonplace. But do the news stories tell the full story?

To understand the reality behind the headlines, Sophos commissioned an independent survey of 5,000 IT managers across 26 countries. The findings provide brand new insight into what actually happens once ransomware hits. It reveals the percentage of attacks that successfully encrypt data; how many victims pay the ransom; how paying the ransom impacts the overall clean-up costs; and the role of cybersecurity insurance. Be prepared to be surprised.

About the survey

Sophos commissioned specialist research house Vanson Bourne to survey 5,000 IT managers on their experiences of ransomware. Sophos had no role in the selection of respondents and all responses were provided anonymously. The survey was conducted during January and February 2020.

Respondents came from 26 countries across six continents:

COUNTRY	# RESPONDENTS
Australia	200
Belgium	100
Brazil	200
Canada	200
China	200
Colombia	200
Czech Republic	100
France	300
Germany	300
India	300
Italy	200
Japan	200
Malaysia	100

COUNTRY	# RESPONDENTS
Mexico	200
Netherlands	200
Nigeria	100
Philippines	100
Poland	100
Singapore	200
South Africa	200
Spain	200
Sweden	100
Turkey	100
UAE	100
UK	300
U.S.	500

Within each country, 50% of respondents were from organizations of between 100 and 1,000 employees, while 50% were from organizations of between 1,001 and 5,000 employees. Respondents came from a range of sectors, both public and private.

SECTOR	# RESPONDENTS	% RESPONDENTS
IT, technology and telecoms	979	20%
Retail, distribution and transport	666	13%
Manufacturing and production	648	13%
Financial services	547	11%
Public sector	498	10%
Business and professional services	480	10%
Construction and property	272	5%
Energy, oil/gas and utilities	204	4%
Media, leisure and entertainment	164	3%
Other	542	11%

Executive summary

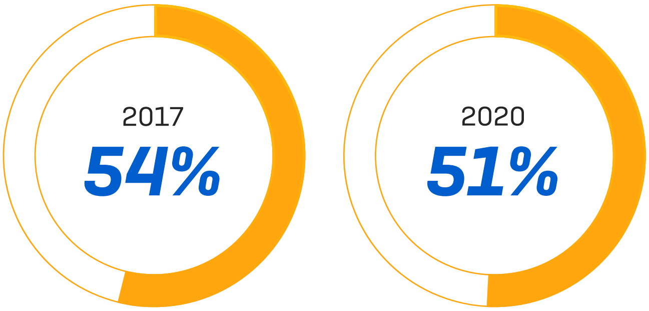
The survey provides fresh new insight into the experiences of organizations hit by ransomware, including:

- **Almost three quarters of ransomware attacks result in the data being encrypted.** 51% of organizations were hit by ransomware in the last year. The criminals succeeded in encrypting the data in 73% of these attacks.
- **26% of ransomware victims whose data was encrypted got their data back by paying the ransom.** A further 1% paid the ransom but didn't get their data back.
- **94% of organizations whose data was encrypted got it back.** More than twice as many got it back via backups (56%) than by paying the ransom (26%).
- **Paying the ransom doubles the cost of dealing with a ransomware attack.** The average cost to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) is US$732,520 for organizations that don't pay the ransom, rising to US$1,448,458 for organizations that do pay.
- **Despite the headlines, the public sector is less affected by ransomware than the private sector.** 45% of public sector organizations were hit by ransomware last year, compared to a global average of 51%, and a high of 60% in the media, leisure, and entertainment industries.
- **One in five organizations has a major hole in their cybersecurity insurance.** 84% of respondents have cybersecurity insurance, but only 64% have insurance that covers ransomware.
- **Cybersecurity insurance pays the ransom.** For those organizations that have insurance against ransomware, 94% of the time when the ransom is paid to get the data back, it's the insurance company that pays.
- **Most successful ransomware attacks include data in the public cloud.** 59% of attacks where the data was encrypted involved data in the public cloud. While it's likely that respondents took a broad interpretation of public cloud, including cloud-based services such as Google Drive and Dropbox and cloud backup such as Veeam, it's clear that cybercriminals are targeting data wherever it stored.

Part 1: The prevalence of ransomware

Half of organizations were hit by ransomware last year

51% of respondents said they had been hit by ransomware in the last year. Organizations did report a slight drop in attacks compared with previous years. An earlier Sophos-commissioned survey published in 2017 (sample size 1,700 organizations) revealed that 54% of respondents had been hit by ransomware in the prior year.



In the last year, has your organization been hit by ransomware? Base: 5,000 respondents (2020), 1,700 respondents (2017).

This drop, while welcome, is likely due to a change in tactics from the ransomware actors rather than a reduced focus on this type of attack. In 2017 mass market 'spray and pray' desktop ransomware was very common based on insights from SophosLabs. These attacks were spread widely and indiscriminately, resulting in a high number of organizations being hit.

Now, in 2020, the trend is for server-based attacks. These are highly-targeted, sophisticated attacks that take more effort to deploy – hence the reduction in the number of attacks. However, they are typically far more deadly due to the higher value of assets encrypted and can cripple organizations with multi-million dollar ransom requests.

For subsequent survey questions, if the organization reported multiple ransomware attacks in the last year, we asked them to respond for *the most significant attack in the last year only.*

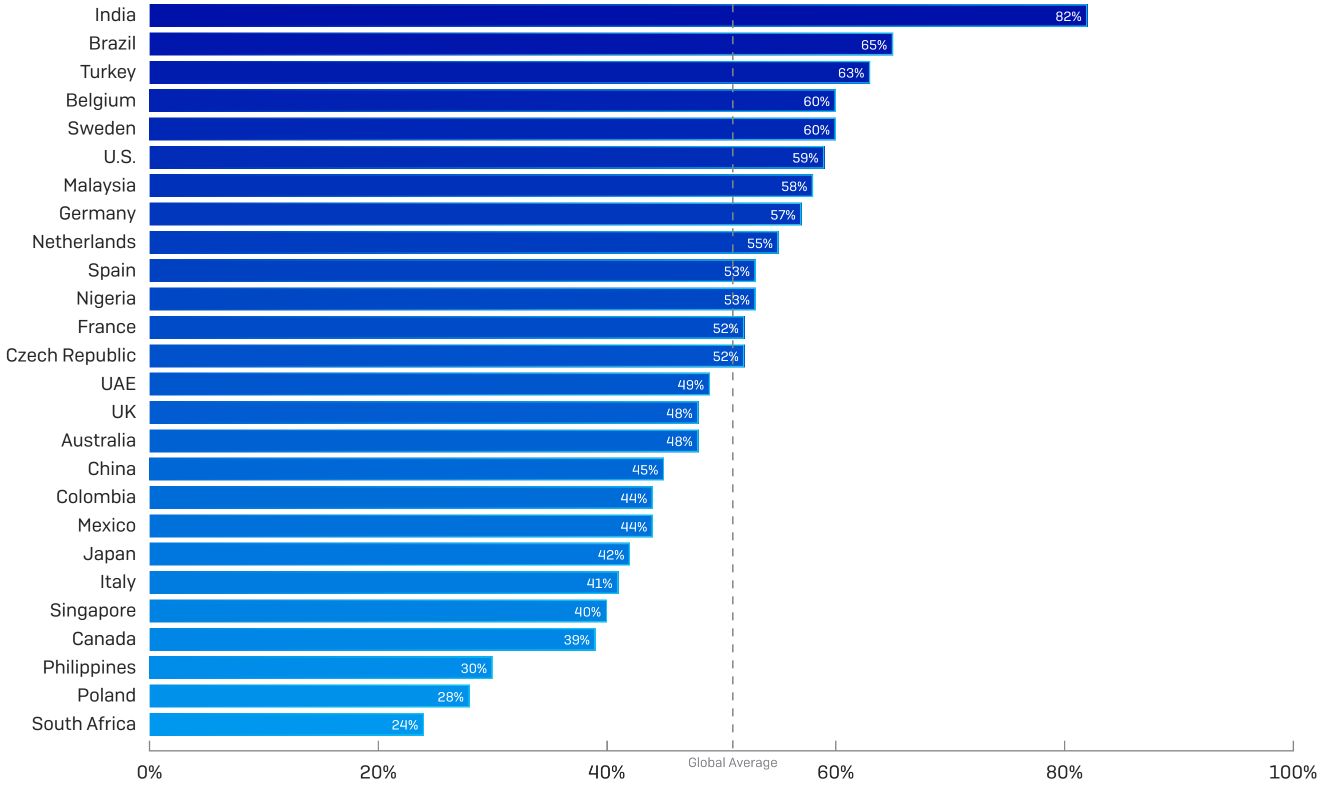
Size doesn't matter

There was a small difference in ransomware attack rates based on organization size. While just under half of the smaller organizations (100-1000 employees) were hit (47%), just over half (54%) of larger organizations (1001-5000 employees) were hit.

Attack levels vary across the globe

Looking at the level of ransomware attacks across the globe reveals interesting variations. This is likely due to criminals focusing their efforts where they see greatest opportunity for return, and also differing countries having differing levels of ransomware defenses.

Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Base: 5,000 respondents.

- **India** (300 respondents) tops the list with 82% of organizations reporting being hit by ransomware in the last year. This is not a huge surprise. Cyber hygiene is generally poor in India, and pirated technology abounds, creating weaknesses in cyber defenses and making organizations more vulnerable to attack.

- **The Philippines, Poland, and South Africa** report the lowest levels of cyberattacks. As we discussed earlier, cybercriminals have moved from 'spray and pray' desktop ransomware attacks to more targeted server-based attacks that affect fewer organizations but with higher ransom demands. They geo-target their attacks to go after the most lucrative opportunities. The three countries at the bottom of the attack scale also have lower GDP than many of the other countries higher up the list which may be why they receive less focus from the cybercriminals.

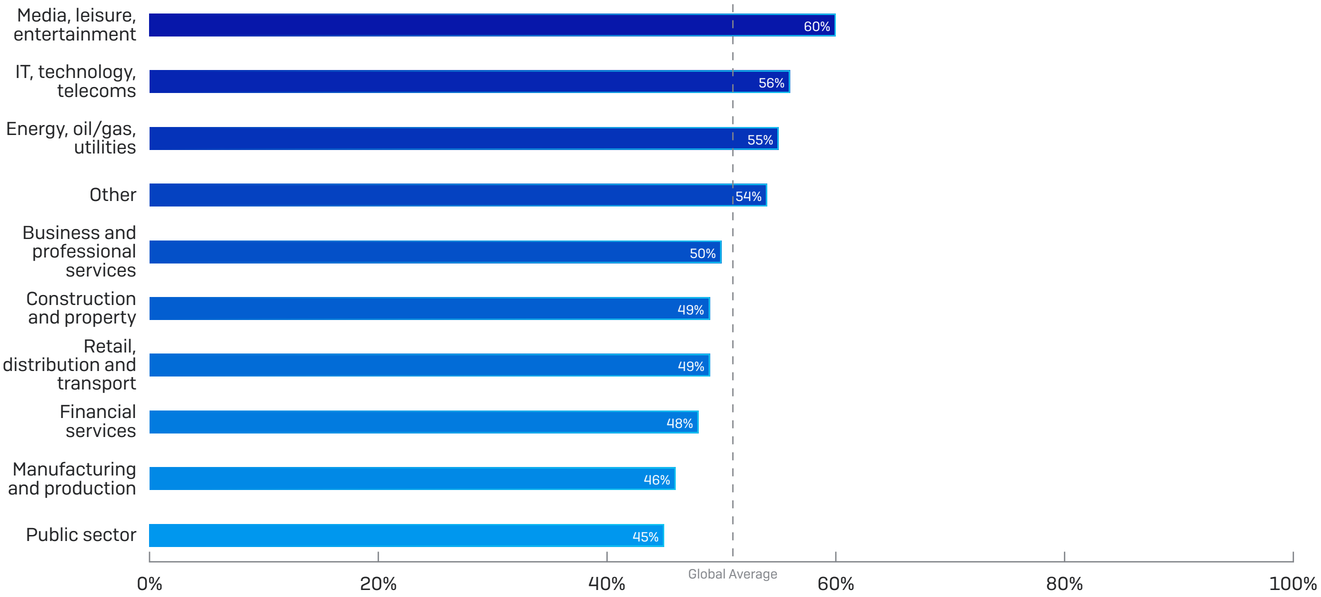
- The move from 'spray and pray' to targeted attacks focused on the most lucrative targets likely contributed to the noticeable reduction in ransomware in **South Africa**. In our previous survey (2017) 54% of respondents reported being hit by ransomware in the last year, but this is now down to 24%, a drop of over 50%.

- **Canada** (200 respondents) reports surprisingly few ransomware attacks. As an advanced, Western country it would be considered a lucrative target, yet only 39% of respondents report being hit by ransomware. This is a full 20 percentage points lower than neighboring U.S., where 59% reported ransomware. It may be that it benefits from being in the attack shadow of the U.S. At the same time, the Canadian respondents were very alert to the issue and expect it to come their way; 68% of the organizations not hit by ransomware anticipate being in the future.

Public sector suffers fewest ransomware attacks

Yes, you read that correctly – the public sector reported fewer attacks than all other sectors. The media, leisure, and entertainment industries actually report the highest levels of attack (60%), closely followed by IT, technology, and telecoms (56%).

Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Base: 5,000 respondents.

At first glance this is surprising: the news is full of stories of hospitals and government organizations that have been held to ransom. However, the survey reveals that those headlines are creating a skewed picture of reality.

In many countries, public sector organizations are obliged to report ransomware attacks. However, the private sector often has no such requirements and so can choose to keep the attack quiet – perhaps to avoid creating concern among customers, reputation damage, or being perceived as an easy target by other attackers.

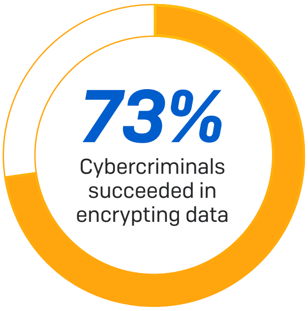
These findings are backed up by Sophos' own research into SamSam ransomware. Working with cryptocurrency monitoring organization Neutrino, Sophos followed the money and identified many ransom payments and victims that were previously unknown. Based on the much larger number of victims now known, it seems that the private sector had actually borne the brunt of SamSam.

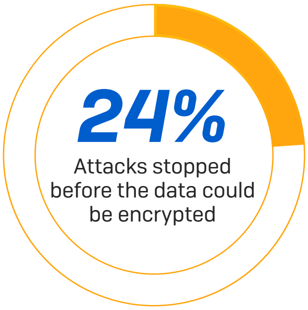
Part 2: The impact of ransomware

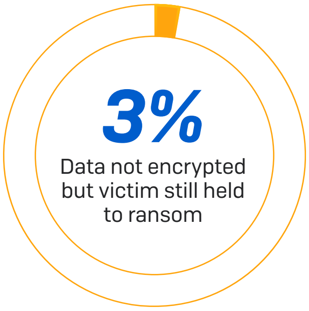
Three quarters of ransomware attacks result in the data being encrypted

Traditionally, there are three main elements to a successful ransomware attack: encrypt the data, get payment, decrypt the data. In almost three quarters of ransomware attacks (73%), the cybercriminals succeeded in encrypting the data.

It is, however, encouraging is that in just under a quarter of cases (24%) the attack was stopped before the data could be encrypted. It seems that anti-ransomware technology is having an impact on the success rate of ransomware attacks.







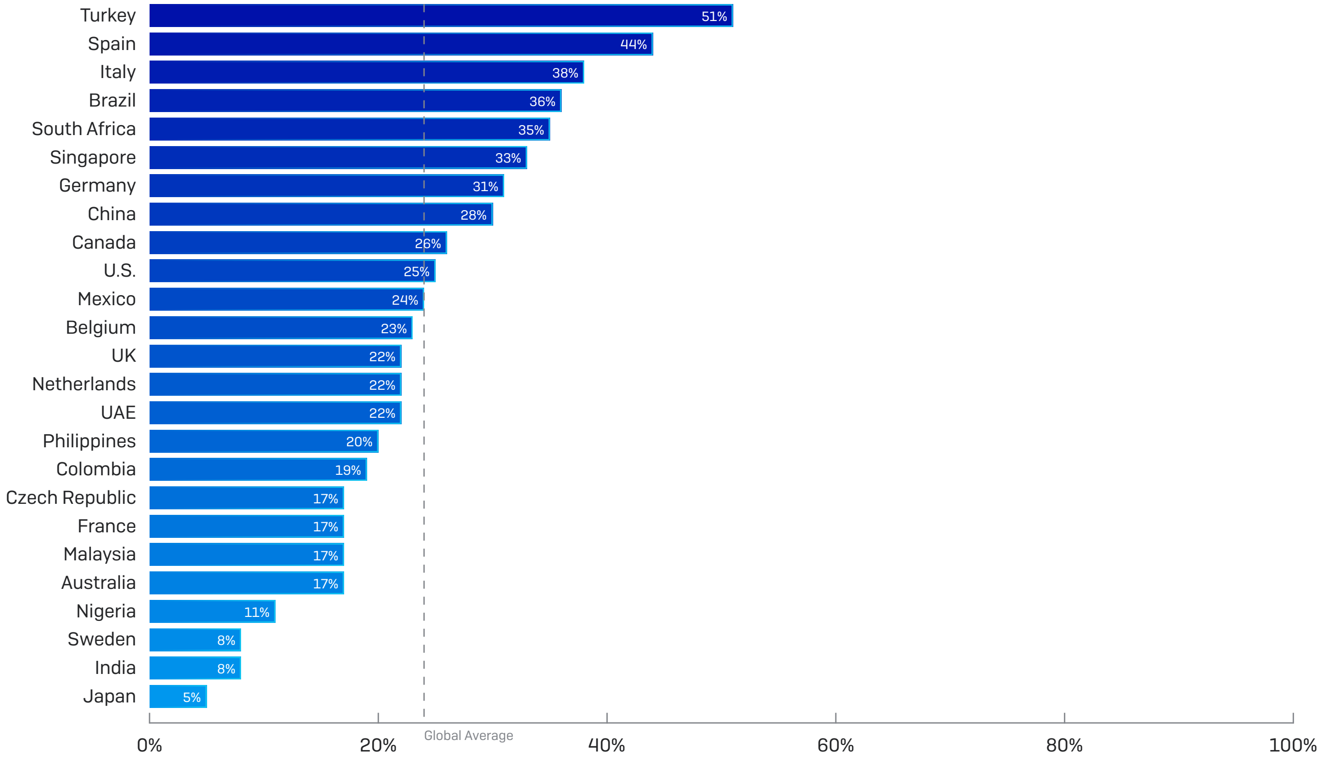
One interesting finding from the survey is that 3% of organizations said their data was not encrypted but they were still held to ransom. This type of attack was particularly dominant in Nigeria, as well as Colombia, South Africa, China, Poland, Belgium and the Philippines.

You could argue that this is extortion rather than ransomware. Semantics aside, the most important take-away is this is an attack vector to be vigilant of as crooks look for ways to make money without the effort of encrypting and decrypting files.

Attacks most likely to succeed in Japan

Looking at a country level, Japan has the least success at stopping attacks with 95% of attacks resulting in the encryption of data. Conversely, in Turkey, half of attacks (51%) were stopped before the data could be encrypted. Reasons for this global variation could include differing levels of awareness of both the prevalence of ransomware and the likelihood of being hit, which in turn could result in differing levels of anti-ransomware specific defenses.

Percentage of attacks stopped before the data was encrypted

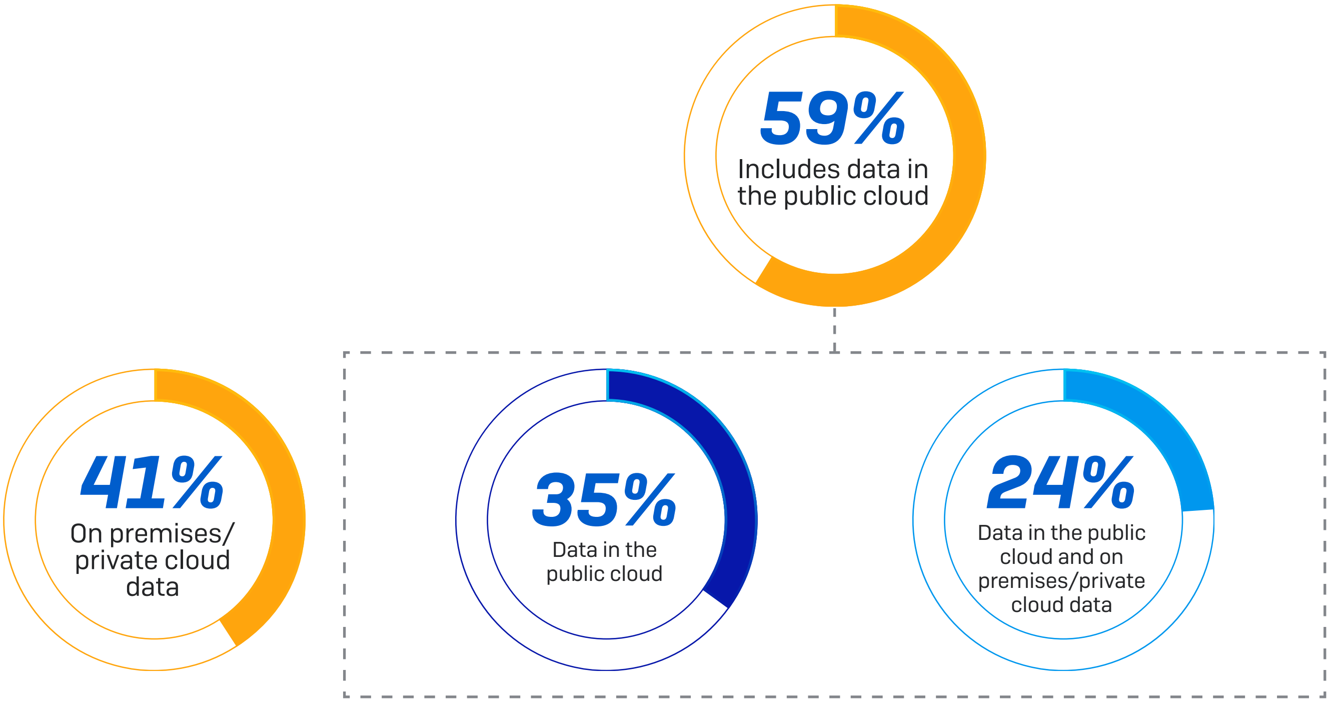


Percentage of respondents that answered 'No, the attack was stopped before the data could be encrypted' to: Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? Question only seen by respondents whose organization had been hit by ransomware in the last year. Base: 2,538 respondents.

Poland has been removed from this chart as it has a base of below 30 respondents, and the Philippines has a base of just 30.

Data in the public cloud is a mainstream target

We asked the 73% of respondents that said their data had been encrypted in the most recent ransomware attack what data was encrypted. 41% said just on-premises data and/or data in the private cloud, while 35% said just data in the public cloud. 24% said a combination of the two. Adding this up, nearly six in 10 successful attacks (59%) include data in the public cloud.



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? Responses from respondents whose organization's data had been encrypted in the most recent ransomware attack. Base: 1,849 respondents.

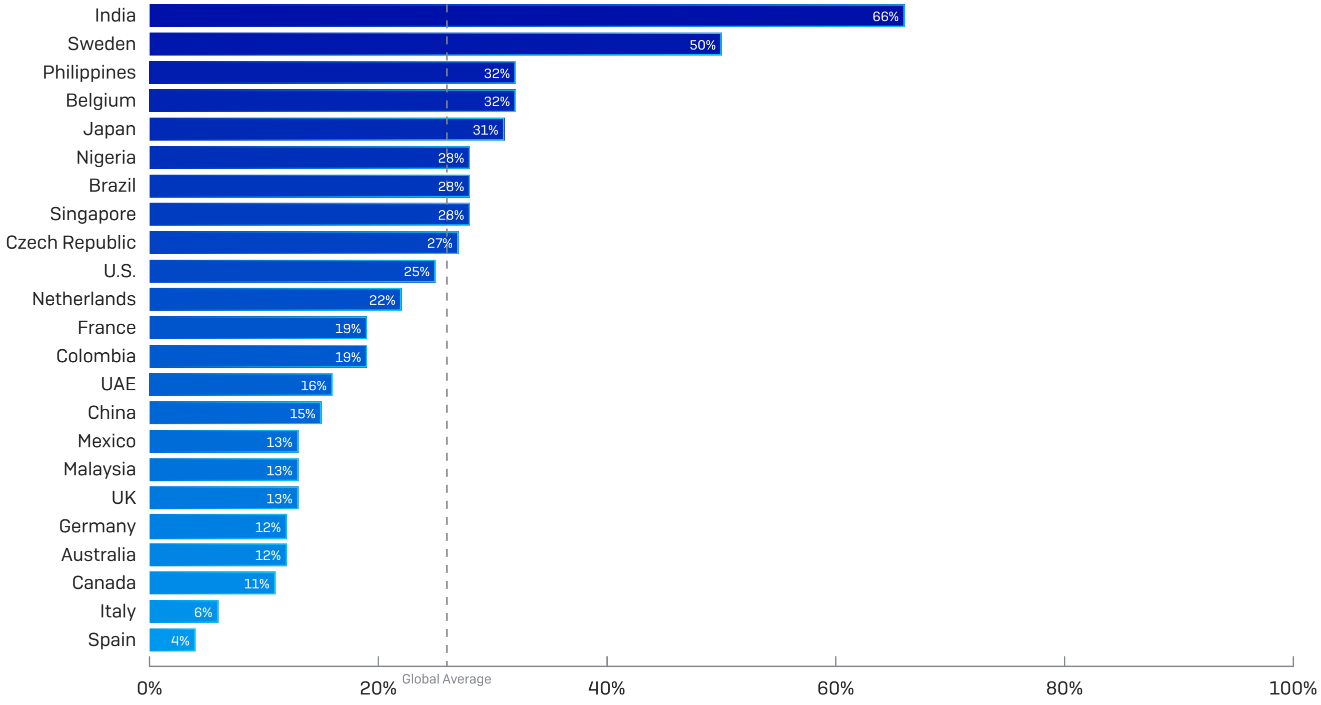
A word of caution here: it is likely that the respondents took a broad interpretation of public cloud, including cloud-based services such as Google Drive and Dropbox and cloud backup such as Veeam, rather than focusing solely on AWS, Azure, and Alibaba Cloud-type services. Nonetheless, there is a clear takeaway: no data is safe, and you should ensure data stored in the cloud is as well protected and backed-up as data stored on premises.

26% of ransomware victims got their data back by paying the ransom

26% of those organizations whose data was encrypted got it back by paying the ransom. A further 1% of organizations whose data was encrypted paid the ransom but didn't get their data back – so overall, 95% of organizations that paid the ransom had their data restored (473 of the 496 organizations that paid the ransom).

When it comes to paying the ransom, we see some noticeable regional variations. In India two out of three (66%) paid the ransom to get the data back, while 29% used backups. Conversely, in Spain just 4% paid the ransom while 72% restored the data from backups.

Percentage of organizations that paid the ransom



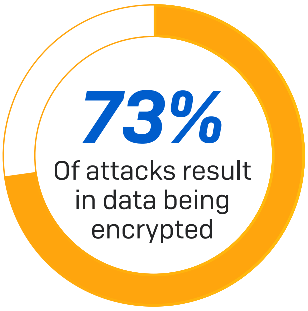
Percentage of respondents that answered "Yes, we paid the ransom" to: Did your organization get the data back in the most significant ransomware attack? Question only seen by respondents whose organization had experienced a ransomware attack where data was encrypted. Base: 1,849 respondents.

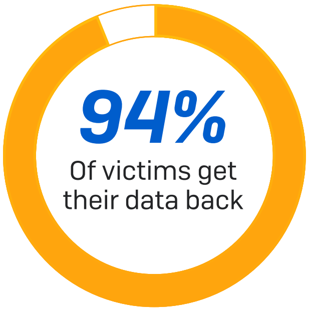
Note, we have removed the Philippines, South Africa, Poland and Turkey from this chart as they all had bases of 30 or fewer for this question.

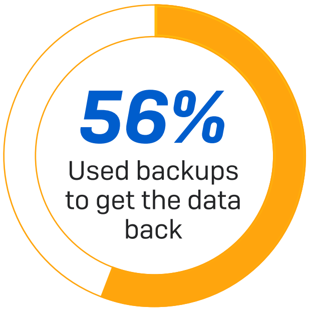
94% of organizations get their data back

While 73% of ransomware attacks succeed in encrypting data, the good news is that 94% of organizations affected managed to get their data back.

As we've seen, 26% got their data back by paying the ransom. However, more than double that (56%) restored their data using backups. The remaining 12% said that they got their data back through other means.







Organization size impacts remediation cost

Unsurprisingly, the survey has confirmed that the cost for remediating a ransomware attack is higher for larger organizations.

Average cost to remediate a ransomware attack

US$761,106
Global average

US$505,827
100–1,000 employees

US$981,140
1,000–5,000 employees

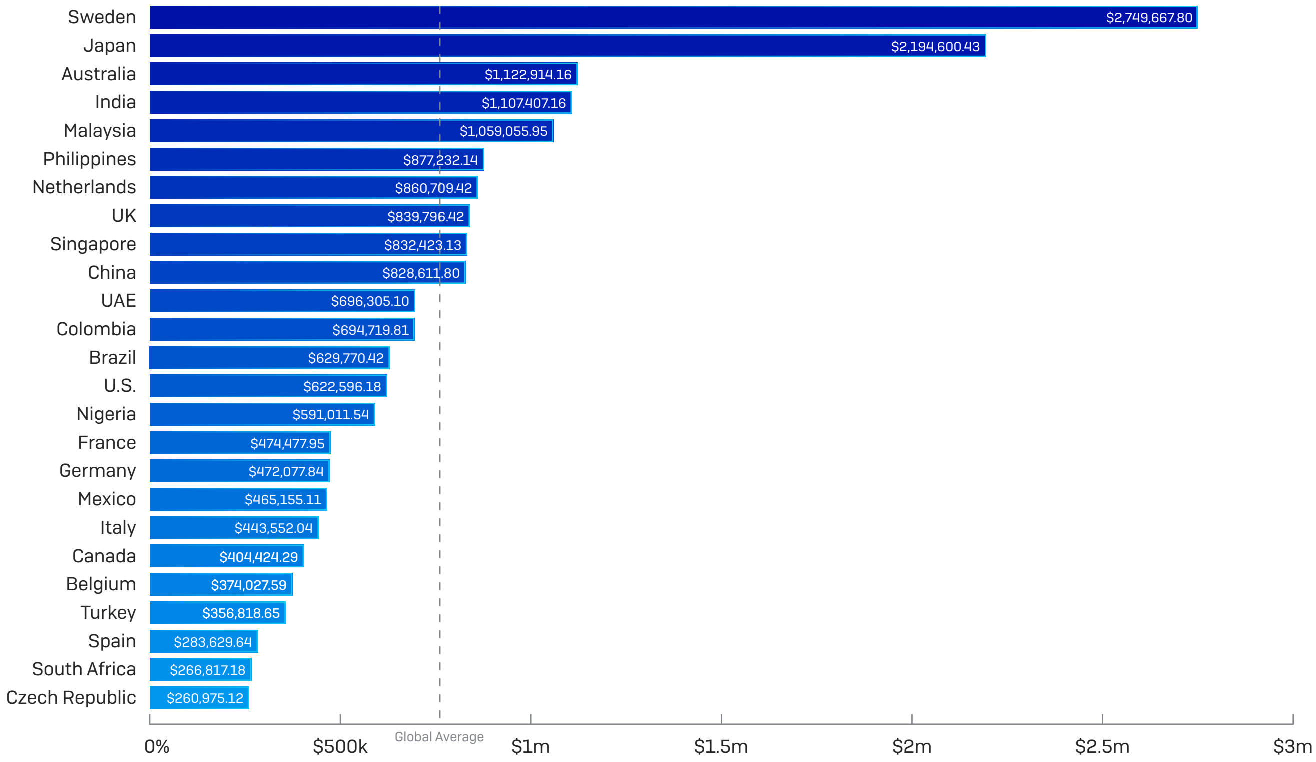
What was the approximate cost to your organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.)? Question only seen by respondents whose organization had been hit by ransomware in the last year. Base: 2,538 respondents.

The average cost to the organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) is US$761,106. For smaller organizations of 100-1,001 employees the average cost was $505,827 and for 1,001 to 5,000 employee organizations the average cost was $981,140.

Ransomware costs vary by country

What is surprising, however, is the variation in remediation cost across the countries surveyed. In particular, Sweden and Japan report considerably higher costs than all other countries. At the other end of the scale, South Africa and the Czech Republic have the lowest remediation costs. We have excluded Poland from this chart as it had a base of below 30 respondents.

Average ransomware remediation cost by country



What was the approximate cost to your organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.)? Question only seen by respondents whose organization had been hit by ransomware in the last year. Base: 2,538 respondents.

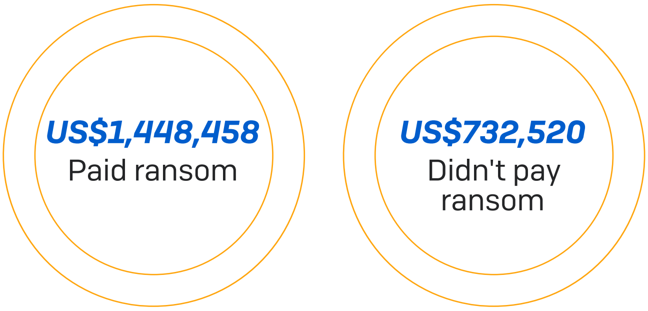
One possible reason for this variation in cost is the labor costs in the different countries. Sweden and Japan are typically higher salary countries, so the cost of the human hours required to remediate the ransomware attack will add up. Conversely, South Africa and the Czech Republic are typically lower labor cost areas.

We have already seen that Sweden has the second highest rate of ransom payment of all countries surveyed, second only to India. However, unlike India, it also has high labor costs which combine to deliver a financial double whammy when it comes to cleaning up after ransomware.

Paying the ransom doubles the cost

One of the most interesting findings from the survey is that paying the ransom almost doubles the overall remediation cost versus not paying or getting the data back via backups or other means. Not only does not paying the ransom generally make you feel better because you haven’t given money to criminals, the good news is that it also saves you money in the long run.

Average cost to remediate a ransomware attack



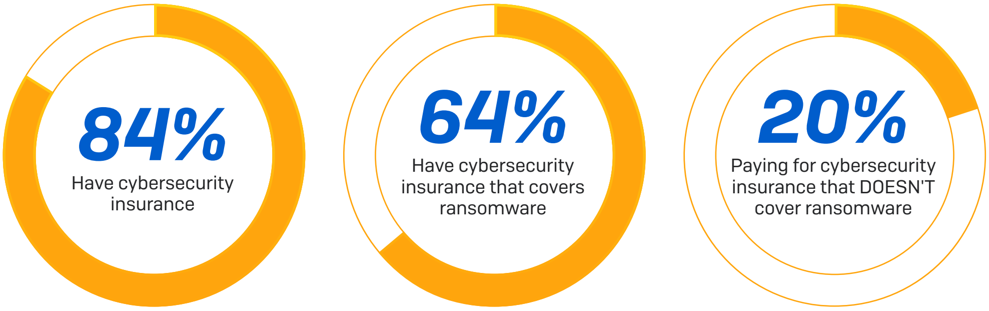
Did your organization get the data back in the most significant ransomware attack? Data only represents respondents whose organization’s data had been encrypted in the most recent ransomware attack. Base: 1,849 respondents. **Paid the ransom** combines responses "Yes, we paid the ransom" and "No, even though we paid the ransom." **Didn’t pay the ransom** combines responses "Yes, we used backups to restore the data," "Yes, we used other means to get our data back," and "No, we didn’t pay the ransom."

This may sound counterintuitive: if you’ve paid the ransom, why does it cost more? Well even if you pay the ransom, you still need to do a lot of work to restore the data. In fact, the costs to recover the data and get things back to normal are likely to be the same whether you get the data back from the criminals or from your backups. But if you pay the ransom, you’ve got another big cost on top.

Part 3: The role of insurance

One in five have holes in their cybersecurity insurance

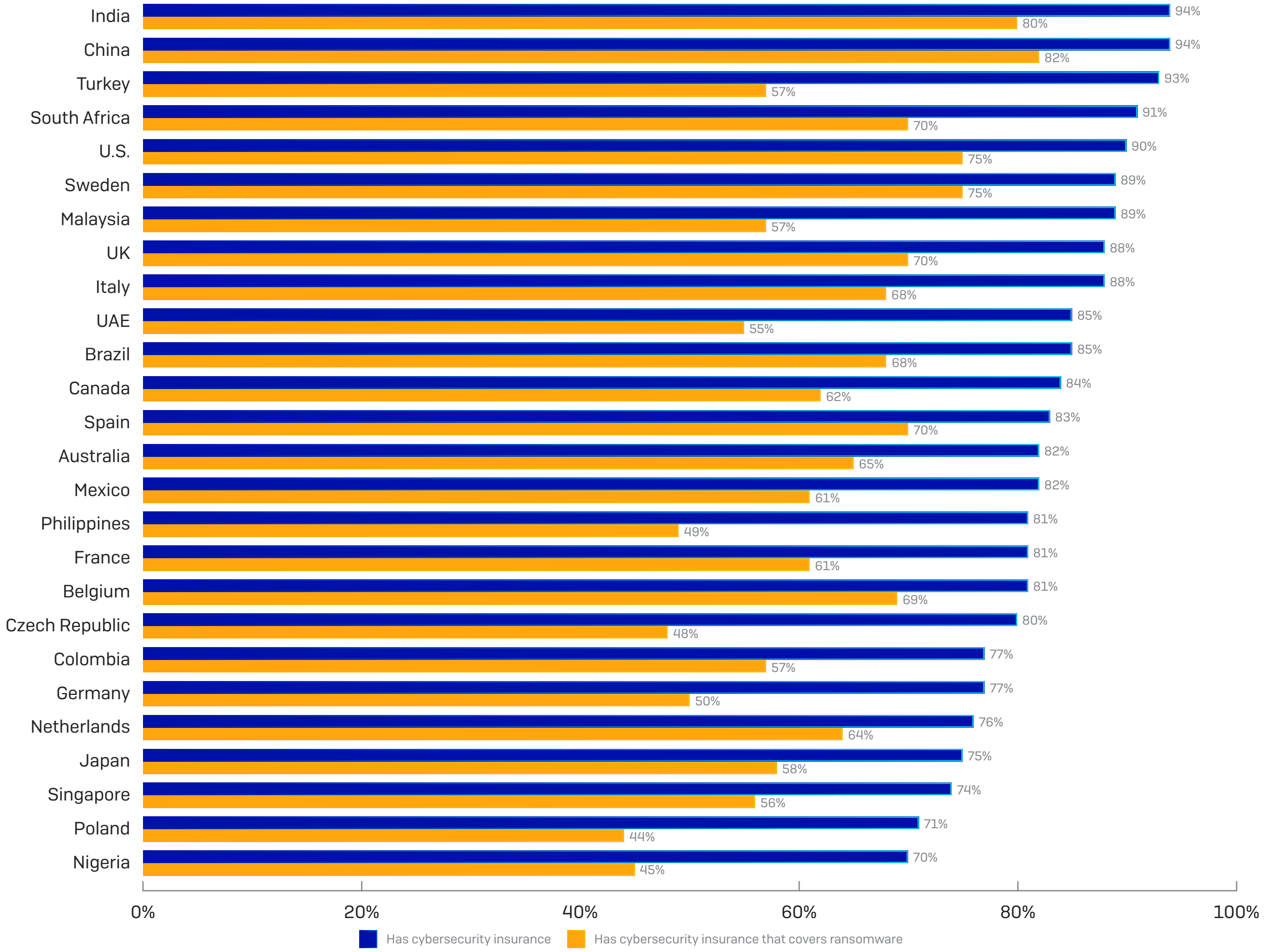
Cybersecurity insurance is now the norm, with 84% of organizations reporting that they have it. However, only 64% have cybersecurity insurance that covers ransomware. This means up to one in five organizations (20%) are paying for cybersecurity insurance that doesn't cover ransomware.



Does your organization have cybersecurity insurance that covers it if it is hit by ransomware? Base: 5,000 respondents.

Given that, as we've seen, 51% of organizations experienced ransomware in the last year, and with average remediation costs of US$761,106, organizations should question the value of insurance that excludes ransomware.

Cybersecurity insurance by country



Does your organization have cybersecurity insurance that covers it if it is hit by ransomware? Base: 5,000 respondents.

This table looks those data points by country. The blue shows the percentage of organizations with cybersecurity insurance and the orange shows the percentage with insurance that covers them for ransomware. What we need to look at here are both the absolute numbers for each column, as well as the gap between the two bars for each country.

India tops the list of organizations with cybersecurity insurance, and has the second-highest level (80%) of organizations with insurance that covers ransomware. Given that India also reported the highest propensity to be hit by ransomware, this is a logical correlation.

Turkey reported the third-highest rate of ransomware attacks. However, while it has the third-highest rate of cybersecurity insurance (93% are covered), it also has one of the biggest gaps between bars with only 57% of organizations covered for ransomware.

Despite China having a below-average rate of ransomware attacks (45% hit in the last year), it has the joint-highest level of cybersecurity insurance (94%) as well the highest level of cybersecurity insurance that covers ransomware (82%). Indeed, it has the smallest gap between columns of all 26 countries surveyed.

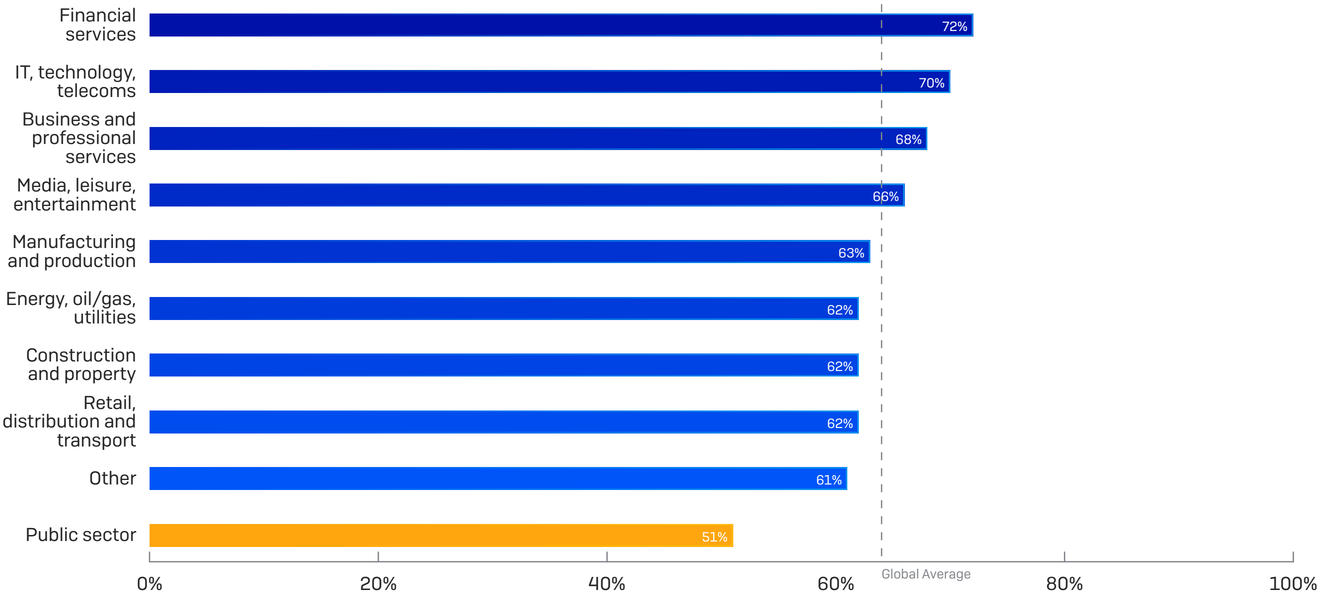
One interesting outlier here is Germany. It is surprising to see a developed economy that has such a low level of insurance (77%), as well as one of the lowest levels of cybersecurity insurance that covers ransomware (50%). Germany reported above-average levels of ransomware (57% of organizations were hit in the last year) which makes the insurance data even more surprising.

The public sector is most exposed to ransomware costs

Although we've seen that the public sector is least exposed to ransomware, it is also – conversely – most exposed to the full cost of an attack.

On average, 64% of organizations have insurance that covers ransomware. The financial services industry has the highest rate of coverage (72%), likely due to the nature of their industry making them a lucrative target for crooks. IT, telecoms, and technology are not far behind on 70%.

Cybersecurity insurance that covers ransomware

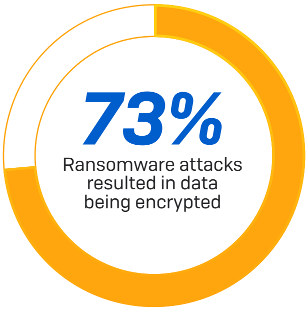


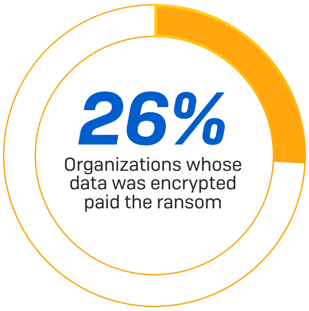
Does your organization have cybersecurity insurance that covers it if it is hit by ransomware? Base: 5,000.

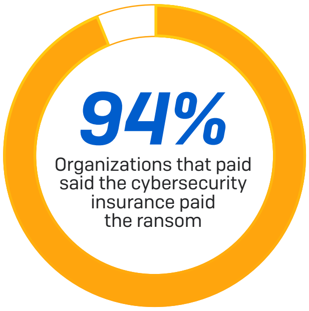
Public sector organizations, however, lag considerably behind their private sector counterparts. Just 51% are covered by insurance for ransomware costs, a full 10 percentage points behind the next sector. This low rate of protection could be due to costs. Tight public sector funding is commonplace across the globe and it may be that budgets don't stretch to insurance. Either way, this is a short term savings if an attack does breach their defenses.

Cybersecurity insurance and ransom payments

Let's now look at the role of cybersecurity in paying the ransom. As we've seen, 73% of ransomware attacks result in the data being encrypted. Of those organizations whose data was encrypted, 26% said they paid the ransom to get the data back.







However, when we dive deeper, we discover that, in almost all of the incidents when the ransom is paid – 94% – it's the cybersecurity insurance that's paying the ransom. And, as we've seen, paying the ransom doubles the overall clean-up costs.

Part 4: Ransomware attack techniques

We asked the organizations that said they had been hit by ransomware in the last year how the attack got into their organization. File download/email with malicious attachments topped the list, accounting for 29% of attacks. Second was remote attacks on servers, accounting for 21% of attacks.

HOW THE RANSOMWARE GOT INTO THE ORGANIZATION	# INCIDENTS	% INCIDENTS
Via a file download/email with malicious link	741	29%
Via remote attack on server	543	21%
Via email with malicious attachment	401	16%
Misconfigured public cloud instances	233	9%
Via our Remote Desktop Protocol (RDP)	221	9%
Via a supplier who works with our organization	218	9%
Via a USB/removable media device	172	7%
Other	0	0%
Don't know	9	0%
Total	2538	100%

How did the ransomware attack get into your organization? Question asked to respondents whose organization had been hit by ransomware in the last year. Base: 2,538 respondents.

What really stands out when we look at this data is that there is no single main attack vector. Rather, attackers are using a range of techniques and whichever defense has a weakness is how they get in. When one technique fails they move on to the next, until they find a weak spot.

This data demonstrates the need for an effective layered defense that covers your endpoints, servers, public cloud instances, email, network gateway, and supply chain. Just focusing on a single technology is a recipe for infection.

Recommendations

The survey has confirmed that ransomware remains a very real threat for organizations today. It's also provided insight into how to minimize your risk of being held hostage:

1. **Start with the assumption that you *will* be hit**. Ransomware it doesn't discriminate: every organization is a target, regardless of size, sector, or geography. Plan your cybersecurity strategy based on the assumption that you will get hit by an attack.
2. **Invest in anti-ransomware technology to stop unauthorized encryption.** 24% of survey respondents that were hit by ransomware were able to stop the attack before the data could be encrypted.
3. **Protect data wherever it's held.** Almost six in 10 ransomware attacks that successfully encrypted data include data in the public cloud. Your strategy should include protecting data in the public cloud, private cloud, and on premises.
4. **Make regular backups and store offsite and offline.** 56% of organizations whose data was encrypted restored their data using backups last year. Using backups to restore your data considerably lowers the costs of dealing with the attack compared with paying the ransom.
5. **Ensure your cyber insurance covers ransomware.** Make sure that you're fully covered if the worst does happen.
6. **Deploy a layered defense.** Ransomware actors use a wide range of techniques to get around your defenses; when one is blocked, they move on to the next one until they find the chink in your armor. You need to defend against all vectors of attack.

Introducing Sophos Intercept X Endpoint

Ransomware actors combine sophisticated attack techniques with hands-on hacking. Sophos Intercept X Endpoint gives you the advanced protection technologies you need to disrupt the whole attack chain, including:

- **Encryption rollback** - CryptoGuard blocks the unauthorized encryption of files and rolls them back to their safe state in seconds.
- **Exploit protection** - Detects and blocks more than three dozen exploit techniques used to download and install malware, preventing attackers getting on your network.
- **AI-powered threat protection** - Sophos' own deep learning engine predictively prevent more attacks and has lower false positives than any other security software.
- **Credential theft** - Stops hackers getting your credentials, blocking unauthorized system access and admin privilege escalation.

Published in June 2020. All information is correct at time of publication. Telefónica UK Limited Registered in England no.1743099.
Registered Office: 260 Bath Road, Slough, SL1 4DX