SOPHOS
Cybersecurity evolved.

The State of Ransomware in Manufacturing and Production 2021

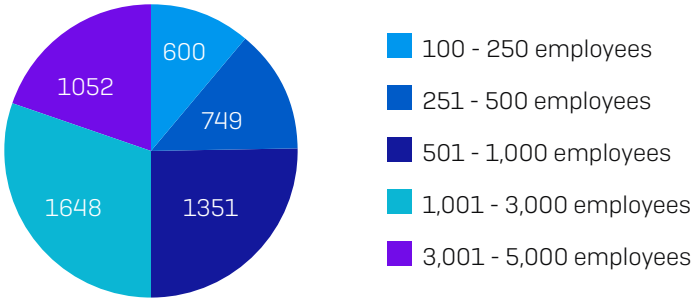
Based on an independent survey of 438 IT decision makers, this report shares new insights into the current state of ransomware in the manufacturing and production sector. It provides a deep dive into the prevalence of ransomware in manufacturing and production, the impact of those attacks on victims, 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

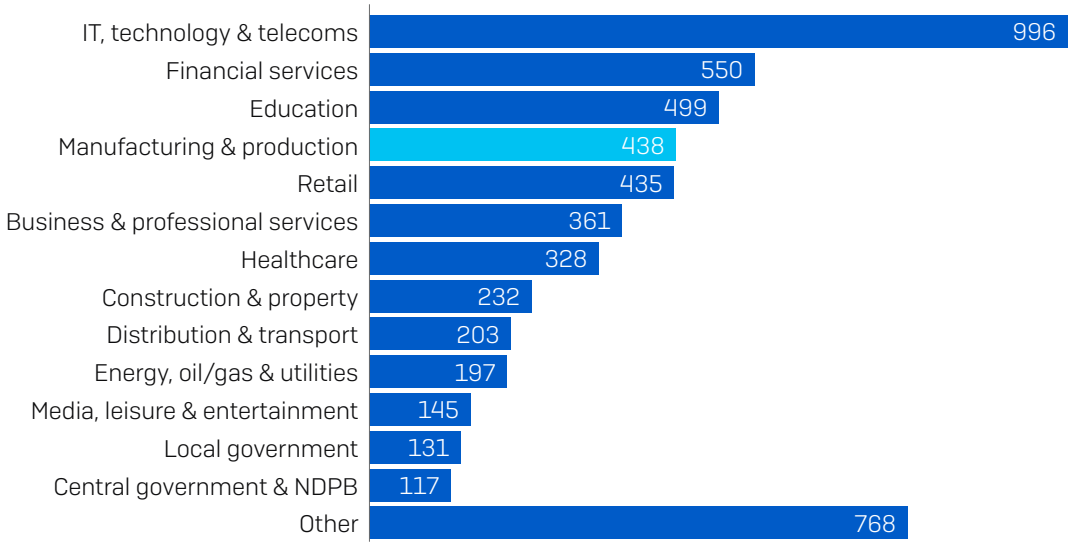
About the survey

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 438 respondents from the manufacturing and production 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 438 manufacturing and production IT decision makers came from all geographic regions surveyed: the Americas, Europe, the Middle East, Africa, and Asia Pacific.

Region	# Respondents
Americas	101
Europe	160
Middle East and Africa	37
Asia Pacific	140

438 IT decision makers in manufacturing and production

Key findings in manufacturing and production

- **36%** of manufacturing and production organizations **were hit by ransomware in the last year**
- **49%** of organizations hit by ransomware said the **cybercriminals succeeded in encrypting their data** in the most significant attack
- **19%** of those whose data was encrypted **paid the ransom to get their data back** in the most significant ransomware attack – the lowest payment rate of all sectors
- **68%** of those whose data was encrypted **used backups to restore data**
- **55% of data was restored**, on average, after paying the ransom, leaving nearly half inaccessible (based on the experiences of 15 respondents)
- **89%** of manufacturing and production organizations **have a malware incident recovery plan**
- **The average bill for rectifying a ransomware attack** in the manufacturing and production sector, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, **was US$1.52 million**

While manufacturing and production experienced an average level of ransomware attacks last year with 36% of organizations hit vs. the global average of 37%, it is the sector that has the highest expectation of experiencing a ransomware attack in the future. Almost half (49%) of the respondents were not hit last year but expect to be hit in the years ahead. This high level of anticipation is driven by awareness of the growing sophistication and prevalence of ransomware: 60% reported that attacks are getting increasingly hard to stop due to their sophistication and 46% stated that ransomware is so prevalent it is inevitable they will get hit.

This sector is by far the most resilient in the face of ransomware. Manufacturing and production was least likely to pay the ransom of all sectors surveyed, with only one in five (19%) organizations whose data was encrypted paying the ransom to get their data back. This is likely thanks to the sector's very high ability to restore data from backups: two thirds (68%) of ransomware victims used backups to restore encrypted data, the highest rate of all sectors. It appears that manufacturing and production are reaping the benefits of having short- and long-term retention of data as required by many government regulations like the GDPR and SOCs, and mandates from the SEC, FDA, and EPA. Given that manufacturing and production organizations that paid the ransom got back just 55% of their data on average, the sector is wise to focus on backups as their primary recovery method.

Manufacturing and production experiences an above-average level of extortion-style attacks where the ransomware operators don't encrypt files but threaten to leak stolen information online if a ransom demand isn't paid, with almost one in ten (9%) organizations hit by ransomware experiencing an extortion-only attack. Cybercriminals are well aware that most manufacturers hold valuable data, such as intellectual property and trade secrets, and they use the threat of selling this data to coerce their victims to pay up. Secondly, this sector's very high ability to restore data from backups is forcing adversaries to move to other approaches that don't rely on the encryption of data.

When it comes to the actual ransoms paid, manufacturing and production comes in below average with an average payment of US$147,917 compared to the cross-sector average of US$170,404 (Note: manufacturing and production has a low response base number, so the figure is not statistically significant.)

The overall ransomware recovery cost for manufacturing and production is almost a quarter of a million dollars lower than the global average: US$1.52 million vs. US$1.85 million average. This lower overall cost is likely thanks to this sector's strong ability to restore encrypted data using backups without relying on ransom payments to get their data back. That said, $1.52 million is still a very high cost and one that will have a major impact on all organizations. Factors that likely contribute to these recovery cost are high spending on remediation measures to keep operations running at all costs, as well as the high costs of reputational damage and regulatory fines that impact this sector.

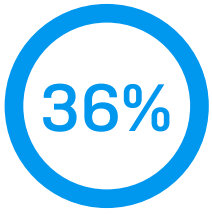
IT teams in manufacturing and production were severely affected by the challenges of 2020. This sector was the least likely to experience a decrease in cybersecurity workload over 2020: just 7% said their cyber workload had decreased, vs. a global average of 13%. It also had the fewest respondents who saw improved response time to IT cases – just 15% said response time to IT cases decreased over 2020, vs. a global average of 20%. As the world went into lockdown, this sector was forced to rapidly move to remote management of production facilities. Organizations faced the challenge of maintaining production output which has traditionally required significant human hands-on involvement. They also needed to work with a highly-impacted supply chain, with shortages of goods regularly hitting the headlines in the first months of the pandemic. The silver lining is that cyber skills also increased, with 71% of respondents saying their team's ability to further develop cybersecurity knowledge and skills increased over 2020.

Manufacturing and production 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.

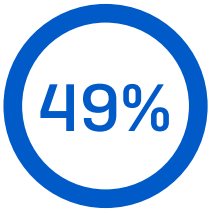
The prevalence of ransomware in manufacturing and production

Manufacturing and production hit by ransomware last year

Of the 438 manufacturing and production respondents that were surveyed, 36% were hit by ransomware in the last year, defined as multiple computers being impacted by a ransomware attack, but not necessarily encrypted.



Hit by ransomware in the last year



Not hit by ransomware in the last year, but expect to be hit in the future – highest across all sectors!

Not hit by ransomware in the last year, and don't expect to be hit in the future

In the last year, has your organization been hit by ransomware? [438 manufacturing and production respondents]

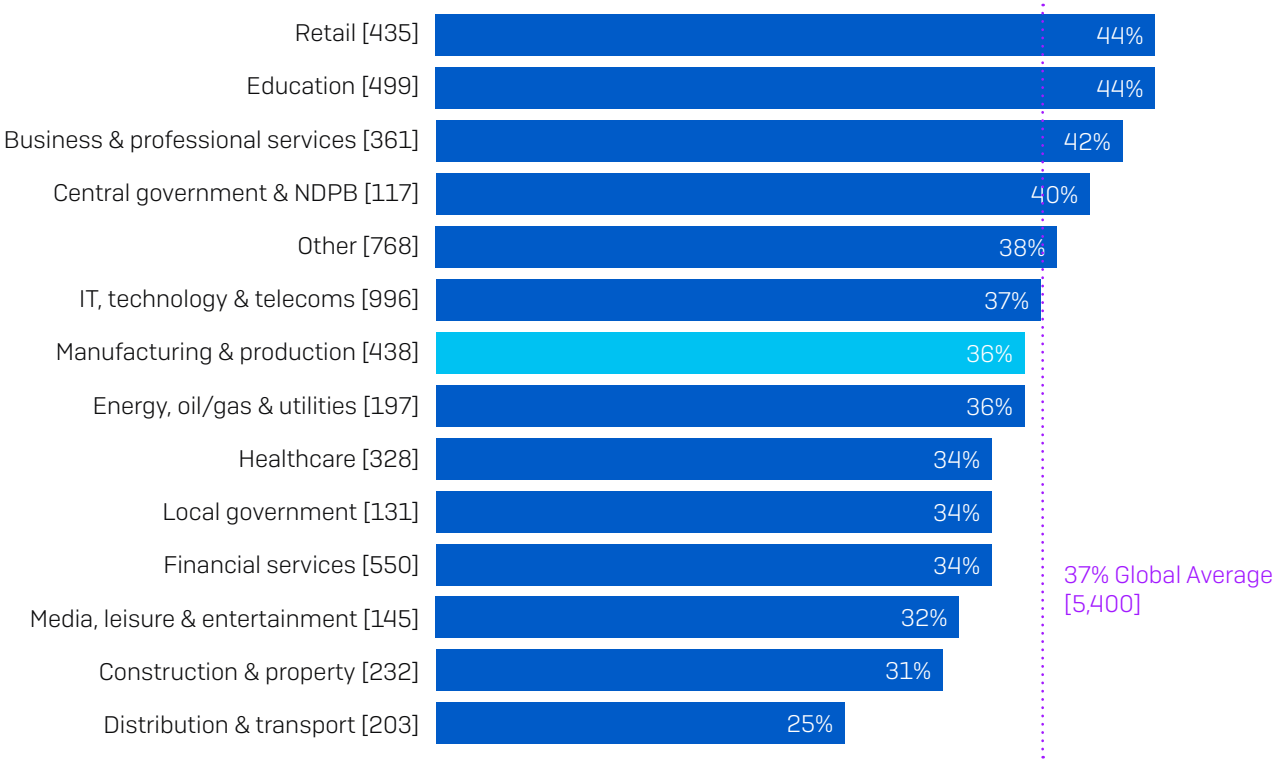
While they didn't experience an attack in the past year, 49% said they expected to be hit by ransomware in the future, which is the highest across all sectors surveyed. As we will see later in this report, this high level of anticipation to be hit in the future is driven by their awareness of the growing sophistication and prevalence of ransomware. At the same time, 15% 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.

Sector with the highest expectation of being hit by ransomware in the future

The number of **manufacturing and production** organizations that reported being hit by ransomware (36%) was slightly less than the cross-sector global average (37%). **Retail** and **education** experienced the highest level of ransomware attacks with 44% of respondents in these sectors reporting being hit.

% respondents hit by ransomware in the last year



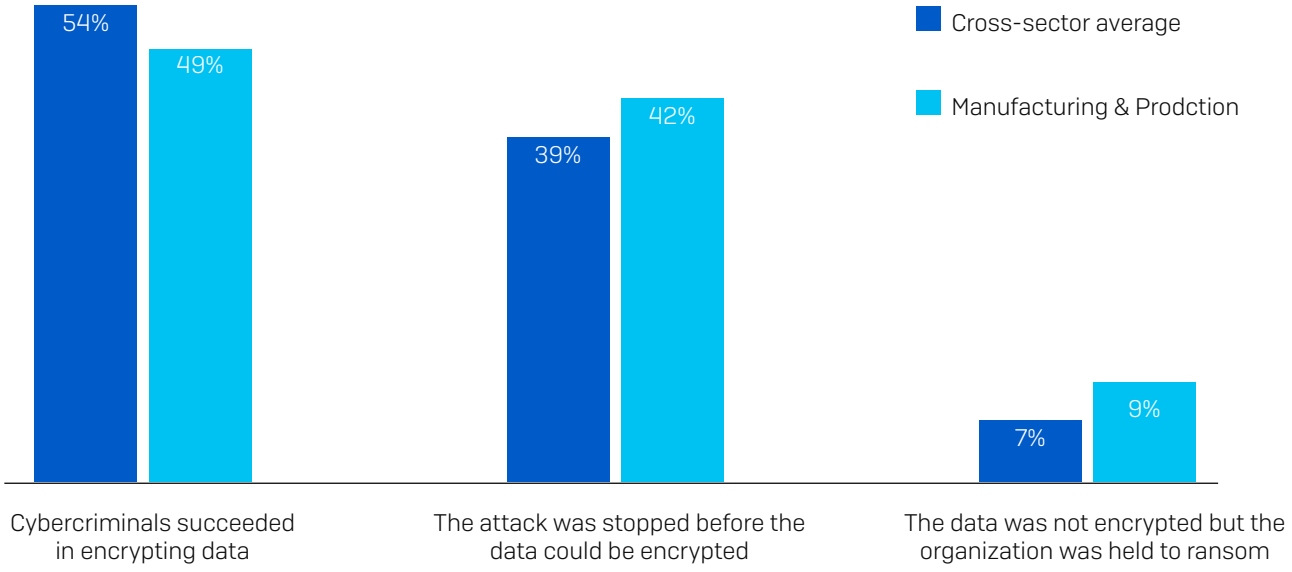
In the last year, has your organization been hit by ransomware? Yes [base numbers in chart] omitting some answer options, split by sector

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 manufacturing and production 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. 49% of manufacturing and production respondents said yes, which is lower than the global average of 54%.



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2006 /158 manufacturing and production organizations that have been hit by ransomware in the last year]

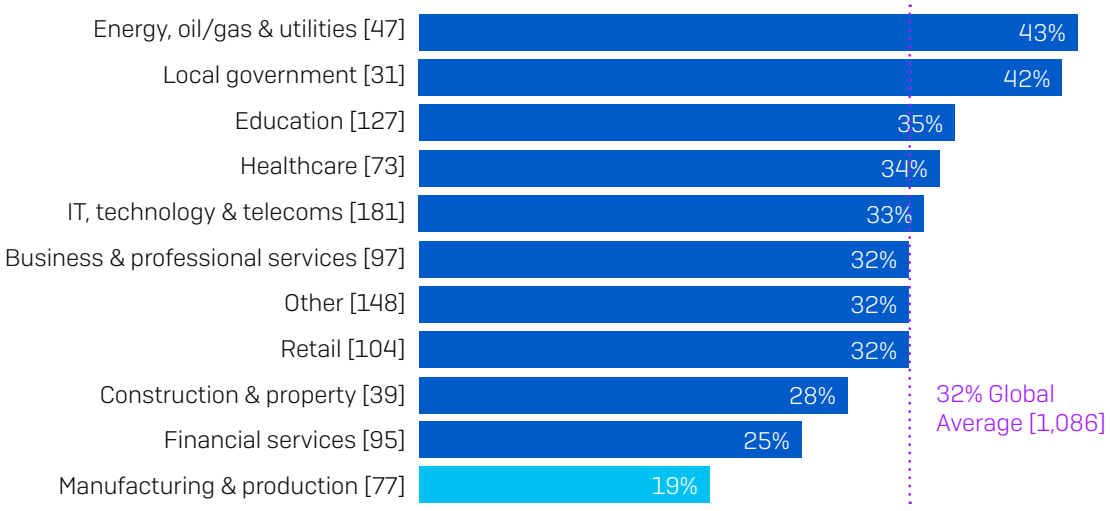
While manufacturing and production was more successful at stopping encryption than the global average (42% of attacks were stopped vs. an average of 39%) this sector was vulnerable to a small but growing new trend: extortion-only attacks, where the ransomware operators don't encrypt files but rather threaten to leak stolen information online if a ransom demand isn't paid. In fact, 9% of manufacturing and production organizations that were hit by ransomware experienced an extortion attack. It is likely that cybercriminals are well aware of the valuable data, such as intellectual property and trade secrets, most manufacturers hold and they use the threat of selling this data to coerce their victims to pay up. Another likely reason is (as we will see later) this sector's very high ability to restore data from backups that pushes adversaries to move to other approaches that don't rely on the encryption of data.

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.

Lowest propensity to pay the ransom

The survey revealed that manufacturing and production organizations had the lowest propensity to pay the ransom of all the sectors surveyed. Just one in five (19%) manufacturing and production organizations whose data was encrypted submitted to the ransom demand, compared to a global average of 32%. A likely reason for this, as we will see shortly, is the sector's impressive ability to restore the encrypted data using backups, which is the highest across all sectors.

% 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

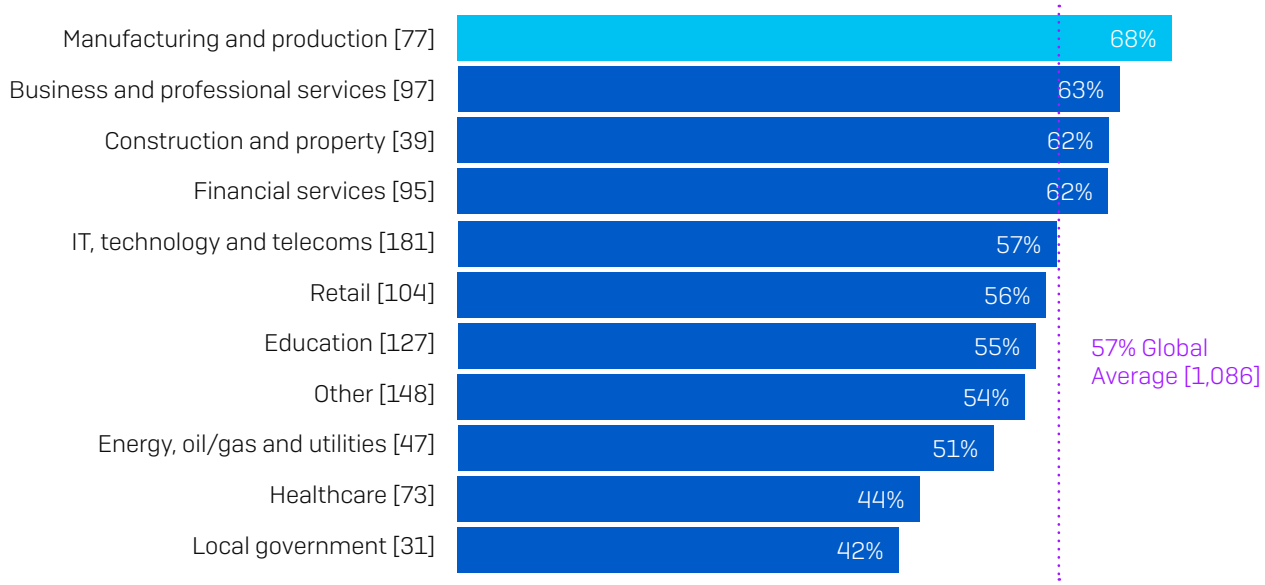
Across sectors, **energy, oil/gas, and utilities** were most likely to pay the ransom, with 43% submitting to the ransom demand. This sector typically has a lot of legacy infrastructure that cannot be easily updated, so victims may feel compelled to pay the ransom to enable continuation of services.

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 chart 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.

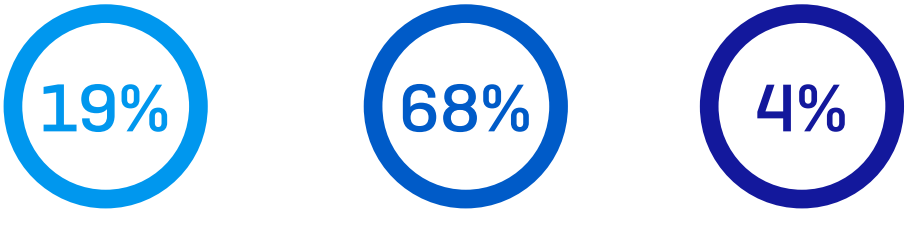
% that used backups to restore encrypted data



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

Manufacturing and production respondents (68%) were the most able to restore encrypted data using backups. This is likely because manufacturing and production organizations require a near-continuous availability of operations, infrastructure, and data to meet the complexities of operating in a global and regulated economy. Industry best practices; government regulations like SOCs, ISO 27001, GDPR; and mandates from the Securities and Exchange Commission (SEC), Food and Drug Administration (FDA), and Environmental Protection Agency (EPA), require the short- and long-term retention of data. Creating backups and practicing restoring data from them will be an integral part of any good plan for this sector.

91% got their encrypted data back



Did your organization get the data back in the most significant ransomware attack? [77] manufacturing and production organizations whre the cybercriminals scceeded in encrypting their data in the most significant ransomware attack.

The good news for manufacturing and production organizations is that 91% of those whose data was encrypted got it back. As we've seen, 19% paid the ransom, 68% used backups, and 4% 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.

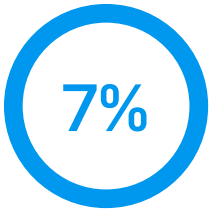
Percentage of data restored after paying the ransom **CROSS-SECTOR AVERAGE**

Percentage of data restored after paying the ransom **MANUFACTURIING & PRODUCTION AVERAGE**

Average amount of data organizations got back in the most significant ransomware attack. [344/15] organizations that paid the ransom to get their data back

The base number of respondents in manufacturing and production sector is not high enough to draw robust conclusions. However, anecdotally, manufacturing and production respondents reported getting back on average just 55% of their data after paying the ransom, leaving nearly half of the data inaccessible. This is considerably less than the global average of 65% of data restored.

It is likely that the partial decryption of data 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. [15] manufacturing and production organizations that paid the ransom to get their data back

Further emphasizing this point, just 7% of manufacturing and production organizations that paid the ransom got back all their data, and 40% got back half or less of their data. Clearly paying up doesn't pay off. Again, the manufacturing and production base number is 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

$ 147,917

Average MANUFACTURING and PRODUCTION ransom payment

How much was the ransom payment your organization paid in the most significant ransomware attack?
[282/12] organizations that paid the ransom to get their data back
Note: Manufacturing and Production sector has a low response base.

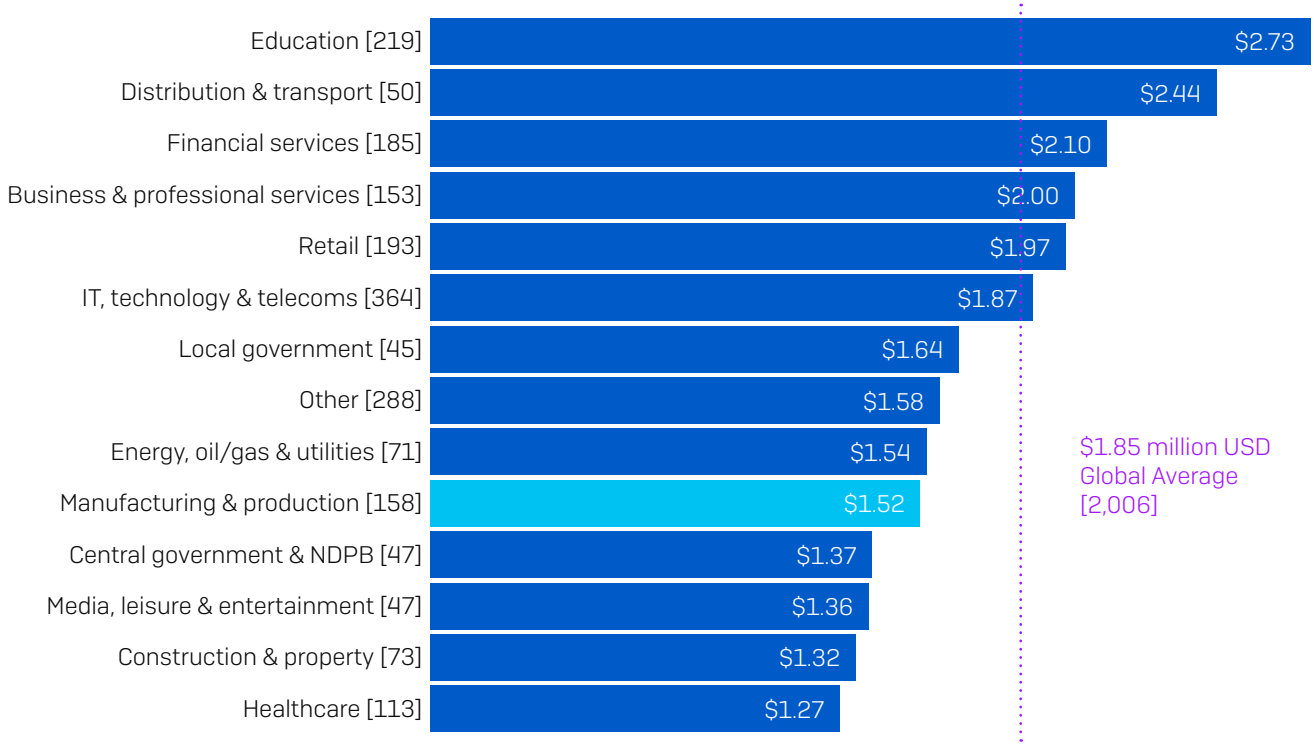
Globally **across all sectors**, the average ransom payment was US$170,404. Anecdotally, the 12 respondents in manufacturing and production organizations paid on average US$147,917. This low payment level is likely due, in part, to the significant ability of this sector to restore data using backups.

Globally, the ransom payment numbers vary greatly from the eight-figure dollar payments that dominate the headlines for multiple reasons.

- **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.
- **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).
- **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 manufacturing and production

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 manufacturing and production sector experiences a below-average ransomware remediation cost of US$ 1.52 million (considering downtime, hours lost, device cost, network cost, lost opportunity, ransom paid, legal and regulatory fines, and so on), which is considerably lower than the global average of US$ 1.85 million. This is likely because of this sector's higher ability to retrieve encrypted data using backups while not relying on ransom payments to get their data back.

While below average, the cost of ransomware is still very considerable for this sector, and likely driven by several factors. In addition to the cost of loss of business due to reputational damage, the cost of being unable to run production when impacted by a ransomware attack can be huge. Often manufacturers form part of a supply chain alongside other manufacturing and production organizations. Disruption to their operations can severely impact the production of other parts of the chain, resulting in large scale business losses. This puts huge pressure on manufacturing and production organizations to get up and running again as quickly as possible, whatever the cost.

Additionally, manufacturing and production organizations must adhere to myriad industry and government regulations including SOCs and GDPR that have huge penalties for non-compliance. Punitive fines for data breaches incurred as part of a ransomware attack add to the overall recovery costs.

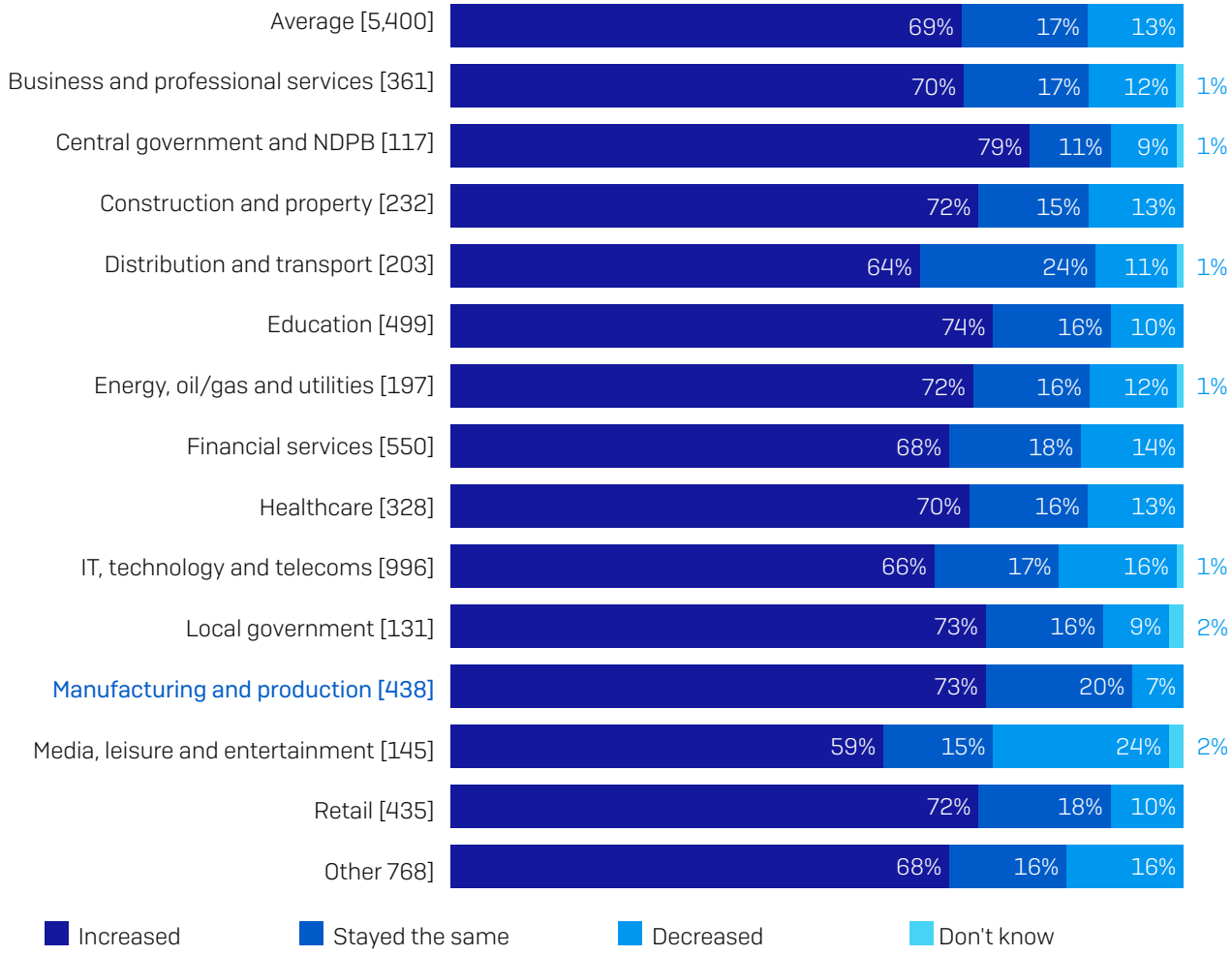
Ransomware is just a part of the cybersecurity challenge

Ransomware is a major cybersecurity issue for manufacturing and production 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 manufacturing and production sector were heavily impacted by the pandemic, with 73% experiencing an increase in cybersecurity workload over the course of 2020. This is also the sector that reported the least incidence of decrease in workload over the year.

How cybersecurity workload changed over the course of 2020



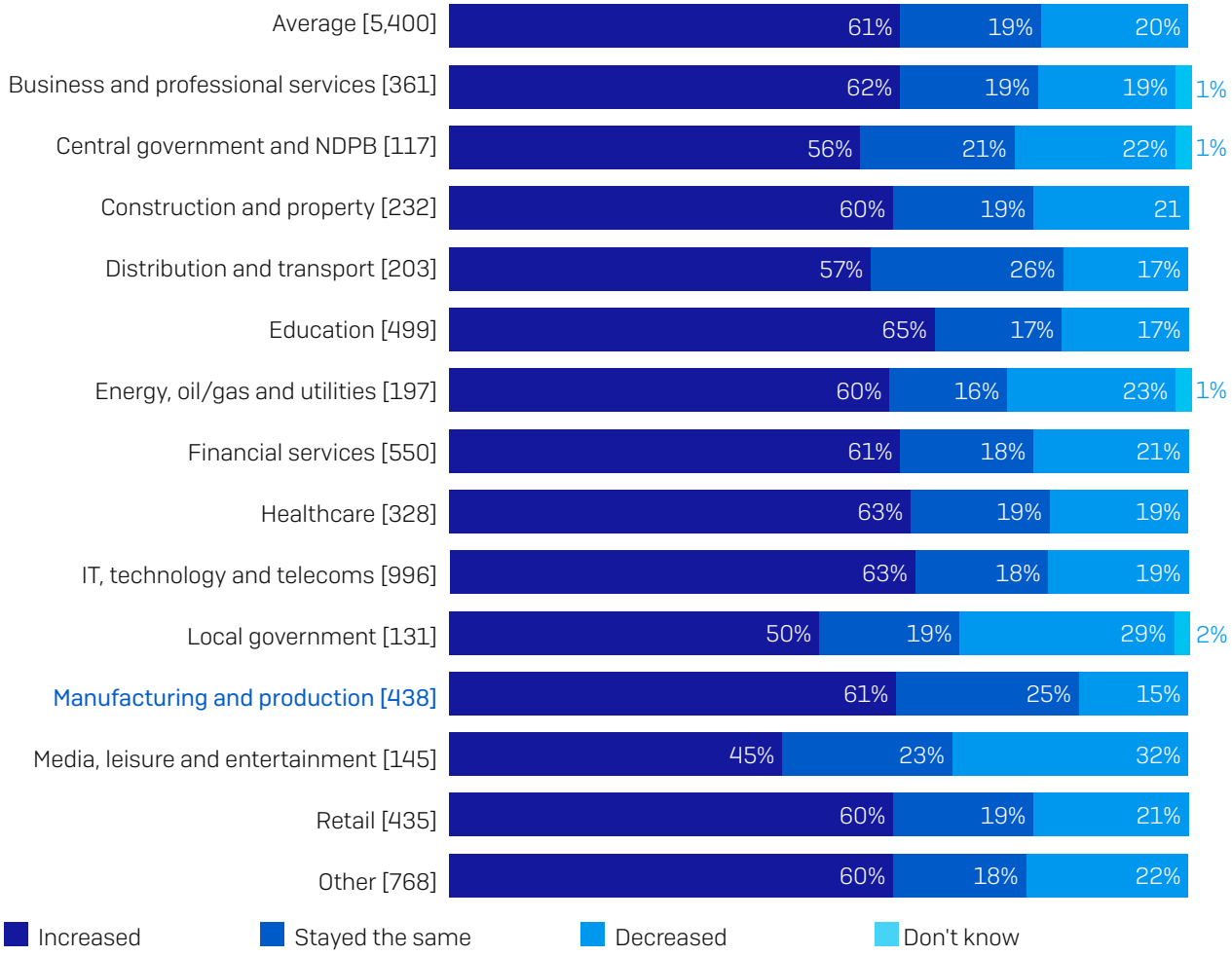
Over the course of 2020, our cybersecurity workload has decreased/increased/stayed the same [base sizes in chart], split by sector.

As the world went into lockdown, this sector was forced to rapidly move to remote management of production facilities. They also needed to work with a highly-impacted supply chain, with shortages of goods regularly hitting the headlines in the first months of the pandemic. Their IT teams faced the challenge of supporting the maintenance of production output which has traditionally involved high levels of human hands-on involvement. The need to facilitate remote access into industrial facilities and secure remote solutions for employees working from home 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 slowdown in response time to IT cases. The manufacturing and production sector was considerably affected, with 61% respondents reporting that response time increased over last year. Again, this sector is least likely to report a decrease in response time to IT cases.

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



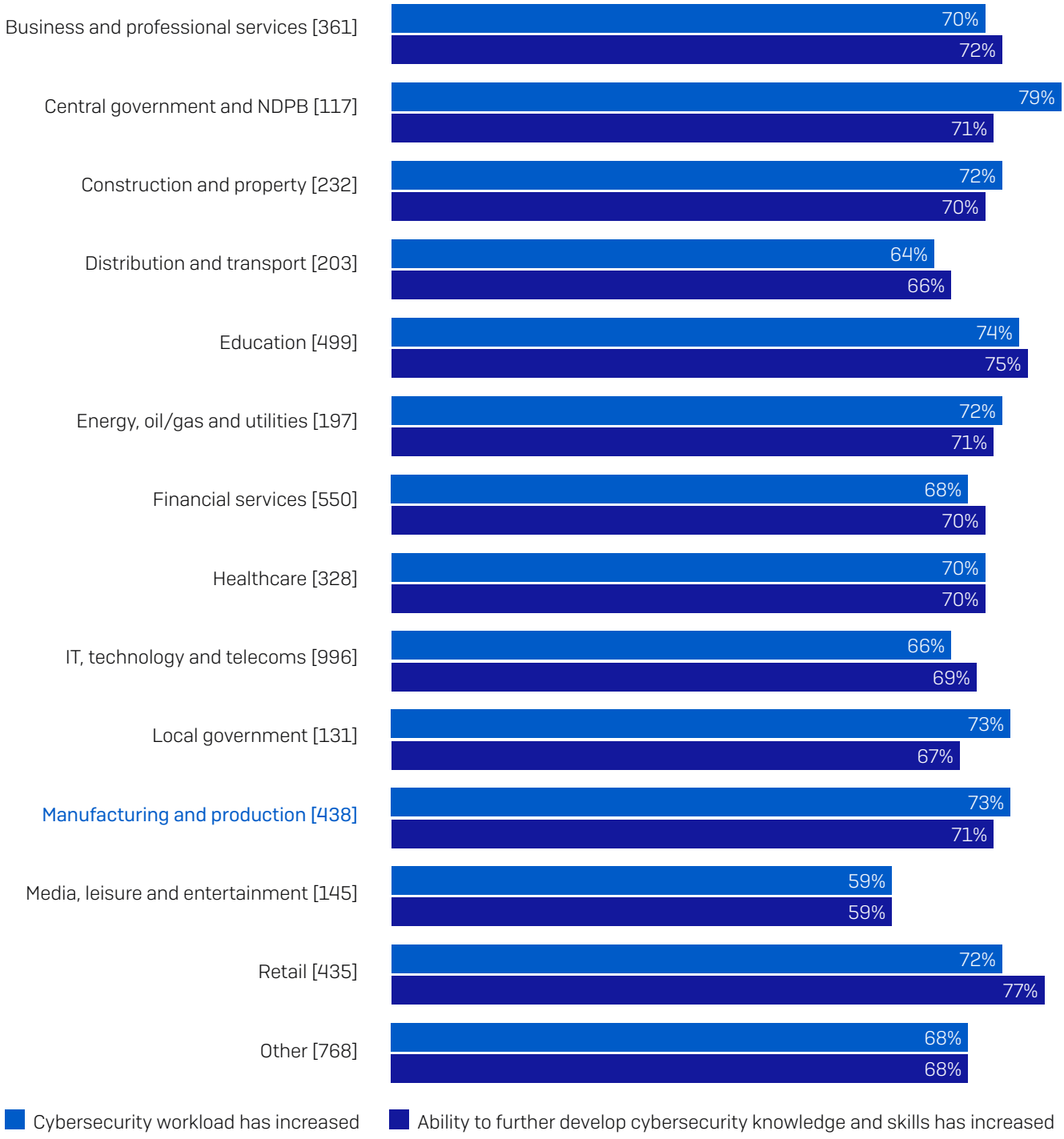
Over the course of 2020, our response time to IT cases has decreased/increased/stayed the same. [base sizes in chart], split by sector. N.B. Due to rounding, some totals are greater than 100%

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

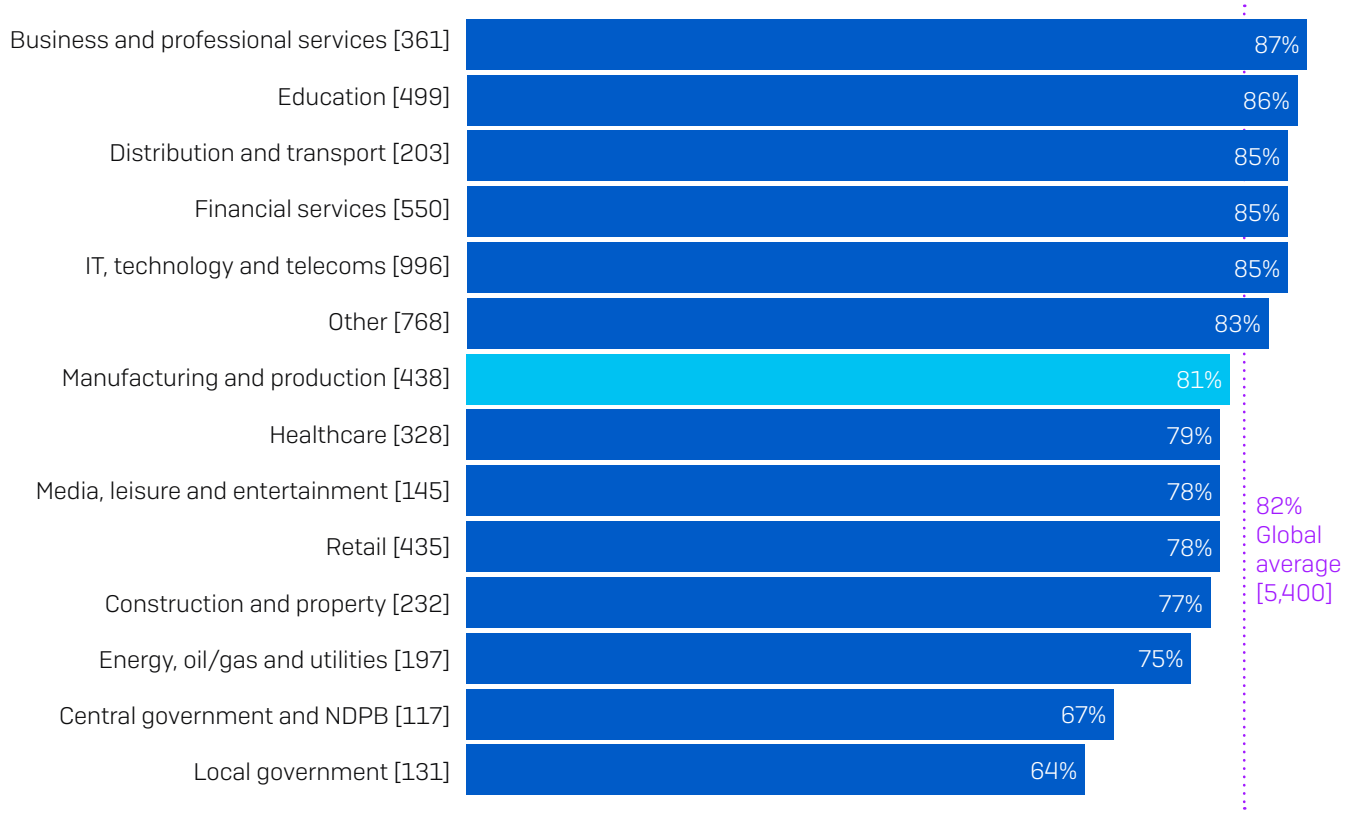
71% of IT teams in manufacturing and production said their ability to develop cybersecurity knowledge and skills increased over the course of 2020.

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 they had never been asked for before.

Readiness to take on future challenges

81% of respondents in manufacturing and production agree that if they detect suspicious activities in their organization, they have the tools and knowledge they need to investigate fully – in line with the global average (82%). This is great news 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

Ransomware expectations in the future

Expect to be hit by ransomware in future

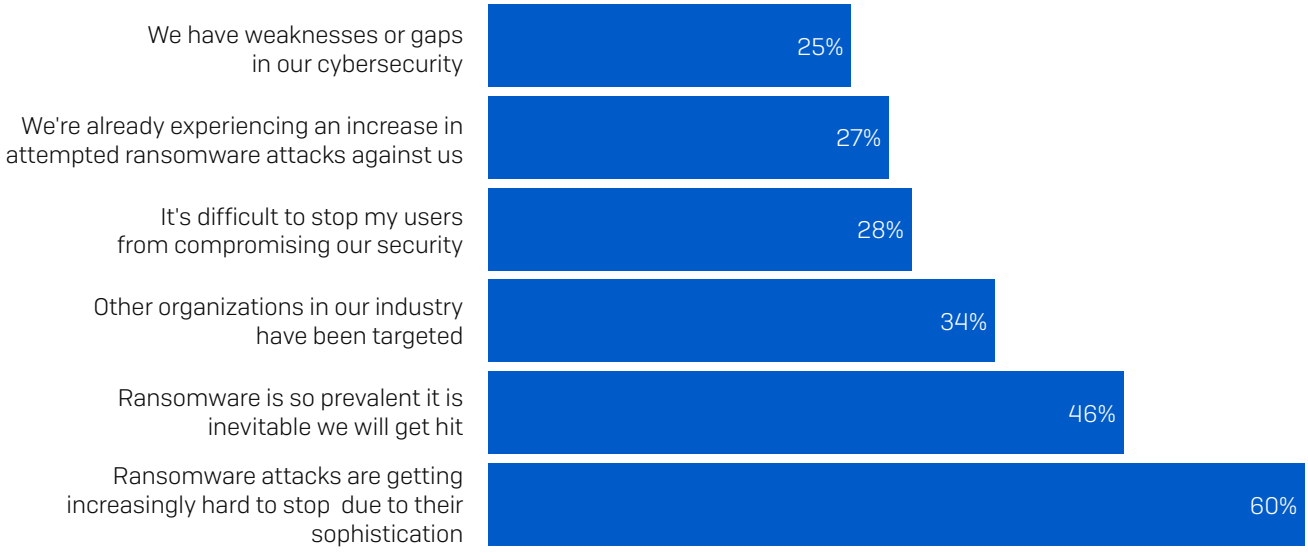
Don't expect to be hit by ransomware in future

[438] Manufacturing and production 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 64% of respondents in the manufacturing and production sector were not hit by ransomware last year. 49% expect to be hit by ransomware in the future. Conversely, 15% don't anticipate an attack.

Why manufacturing and production sector expects to be hit

Among the manufacturing and production organizations that weren't hit by ransomware but expect to be in the future, the most common reason (60%) is that ransomware attacks are growing more sophisticated and therefore increasingly hard to stop. While this is a high number, the fact that these organizations are aware of ransomware becoming ever more advanced is a good thing and may well be a contributing factor to 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? [215 manufacturing and production 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, 46% of respondents said ransomware is so prevalent it is inevitable they will get hit. 34% believed that other organizations in their industry have been targeted, increasing their probability to be hit.

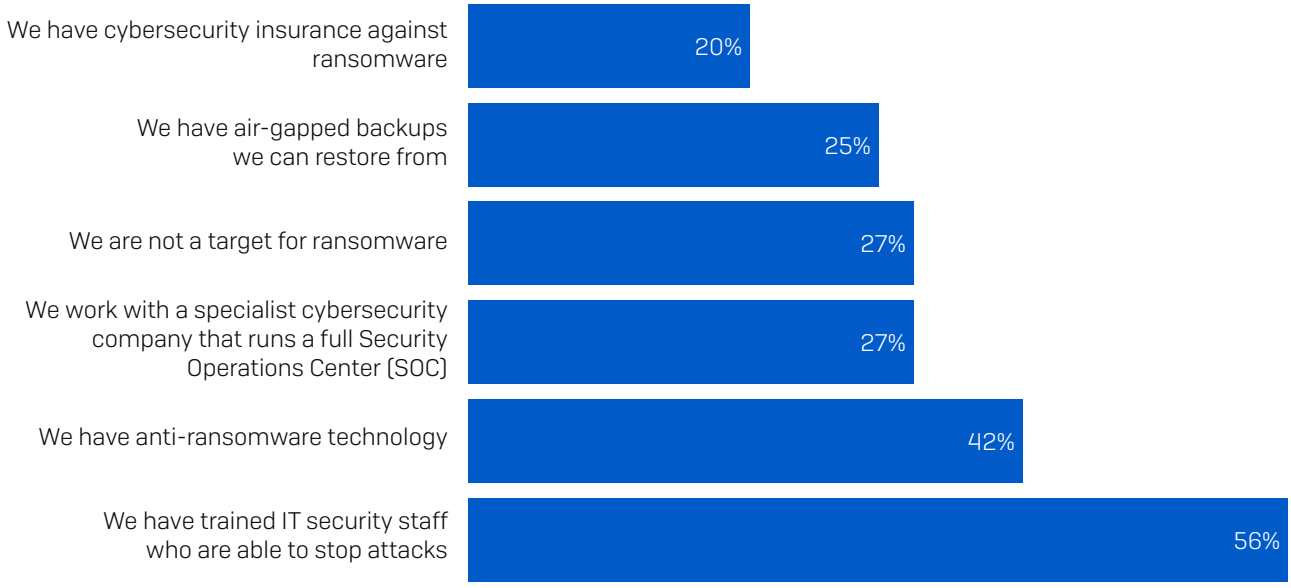
28% of respondents see users compromising security as a major factor behind why they will likely be hit by ransomware in the future. It is encouraging to see that, in the face of sophisticated attackers, most IT teams are not taking the easy option of blaming their users.

Similarly, 25% of manufacturing and production 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 manufacturing and production don't expect to be hit by ransomware

64 manufacturing and production 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? [64] manufacturing and production 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 level of confidence is having trained IT staff who are able to stop attacks (56%), followed by the use of anti-ransomware technology (42%). 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.

27% of manufacturing and production 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:

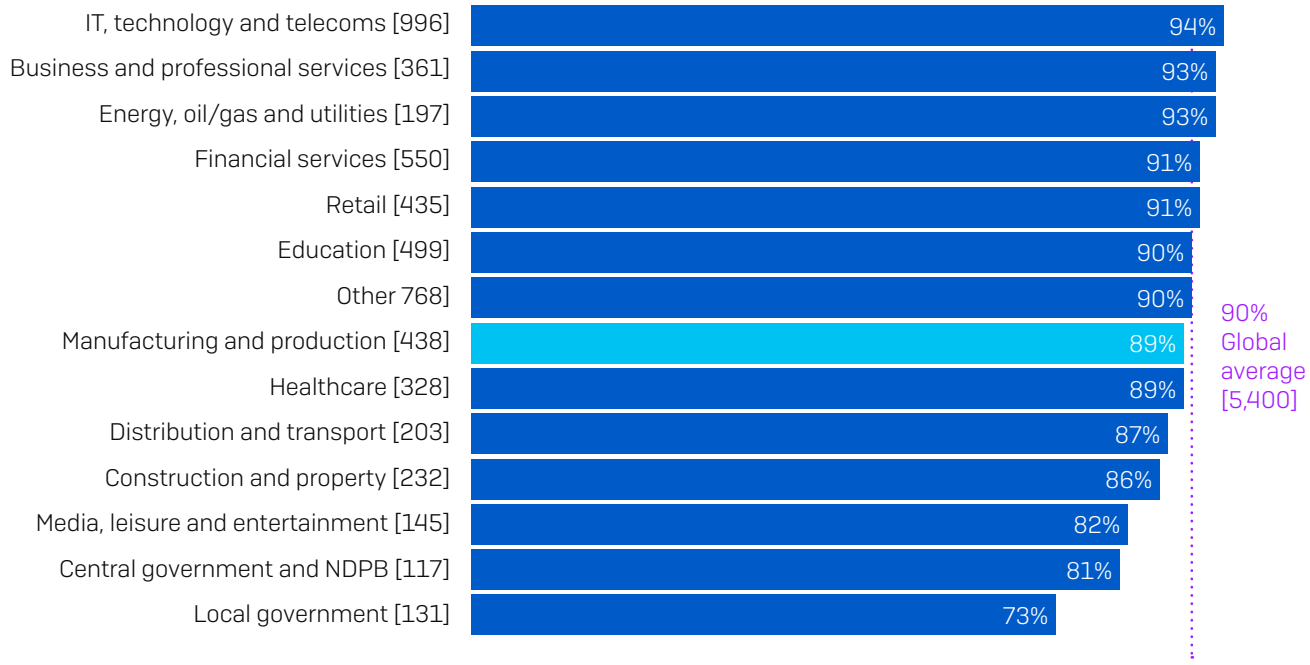
- 38% of manufacturing and production respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware.
  - 20% cited cybersecurity insurance against ransomware. Insurance helps cover the cost of dealing with an attack, but doesn't stop the attack itself.
  - 25% 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 38% selecting at least one of these two options.
- 27% believe that they are not a target of ransomware.
  Sadly, this is not true. No organization is safe.

Manufacturing and production 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.

% 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 89% of manufacturing and production organizations have a malware incident recovery plan, with just under half (49%) having a full and detailed plan and 41% 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.

2021-09-20 (SB-NP)

SOPHOS