THE 2022 HORNETSECURITY RANSOMWARE ATTACKS ANALYSIS

HORNETSECURITY

KEY TAKEAWAYS FROM THE 2022 RANSOMWARE ATTACKS SURVEY BY HORNETSECURITY

1. 1 in 4 (23.9%) IT professionals say their organization has been the victim of a ransomware attack.
2. 21% of these attacks happened in the last 12 months.
3. Organisations targeted by ransomware attacks either lost data (14.1%) or had to pay the ransom to recover the data (6.6%)
4. Nearly 6 in 10 ransomware attacks (58.6%) originated from malicious email or phishing attacks.

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

HORNETSECURITY

ABOUT THE 2022 RANSOMWARE ATTACKS SURVEY

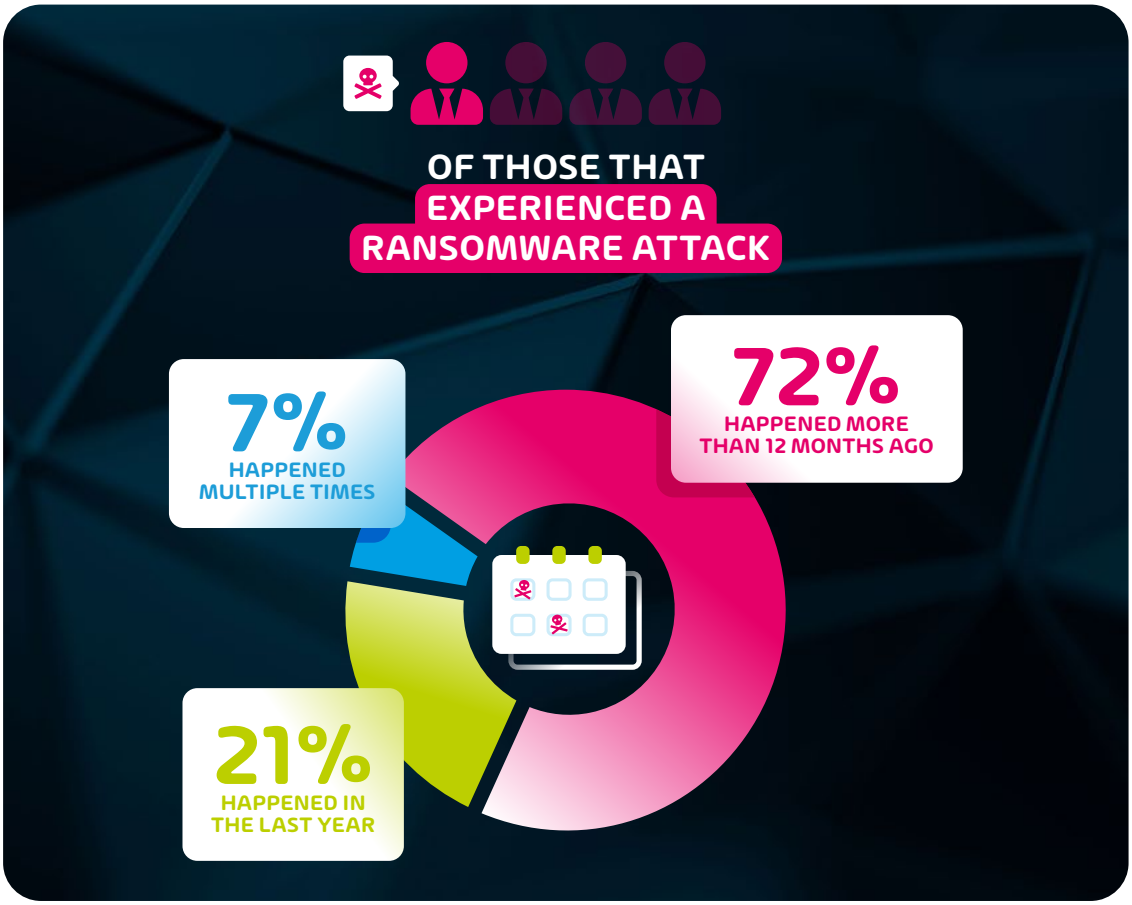
Most IT professionals would agree that ransomware attacks are an IT department's worst nightmare. Successful ransomware attacks bring a company's operation to a grinding halt, making critical data and applications inaccessible. They also expose organizations to huge fines if sensitive information is compromised.

As cybersecurity experts, it is our responsibility to invest time and effort in understanding the latest trends in the industry. Our knowledge base is packed with detailed information about all the current major cybersecurity threats that exist, and as a part of our commitment to staying ahead of the curve, we perform multiple surveys per year to gather data straight from the source: IT professionals around the world.

Last year's ransomware attacks survey found that **1 out of every 5 IT professionals** has experienced a ransomware attack at some point in their career. This year, we wanted to take things a step further by delving deeper into the sources of these attacks and whether the shift towards cloud technologies has influenced the incidence and severity of attacks.

This year's edition of the ransomware attacks survey collected data from over **2,000 IT professionals** across industries and continents. Here are the key takeaways, along with some recommendations on how best to prevent ransomware attacks.

1 IN 4 I.T. PROS EXPERIENCED A RANSOMWARE ATTACK - 21% HAPPENED IN THE LAST YEAR



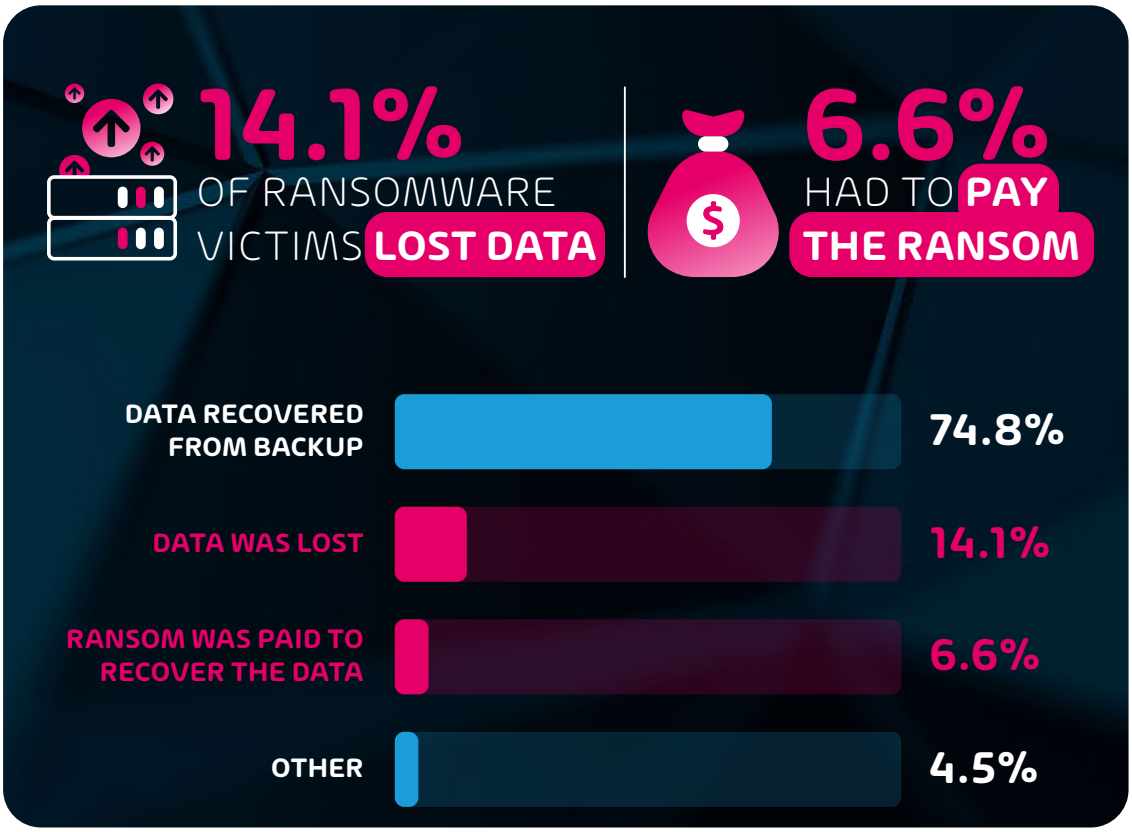
The survey revealed that **23.9% of IT professionals say their organization has been the victim of a ransomware attack.** This indicates that ransomware attacks are steadily rising in comparison to last year where just 21.1% of IT professionals reported such an incident.

We also found that **21%** of all the reported ransomware attacks occurred over the **last 12 months.** This amounts to 5% of surveyed IT professionals having experienced a ransomware attack in the last year alone. While at first glance this might not seem like much, it means that just over the last 12 months, 1 in 20 companies has faced an attack.

We believe that this slight uptick in incidence may be the result of two factors. The first being the fact that these attacks continuously prove to be lucrative for cyber criminals as organizations struggle to keep up. The second is the increasing adoption rate of hybrid cloud technology. According to our own Hybrid Cloud Adoption survey data, organizations have steadily increased their use of cloud technologies. More IT teams are relying on cloud-based platforms such as Microsoft 365 and Google Workspace, thinking that the stock security features will protect them from security threats.

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

14.1% OF RANSOMWARE VICTIMS LOST DATA, 6.6% HAD TO PAY THE RANSOM

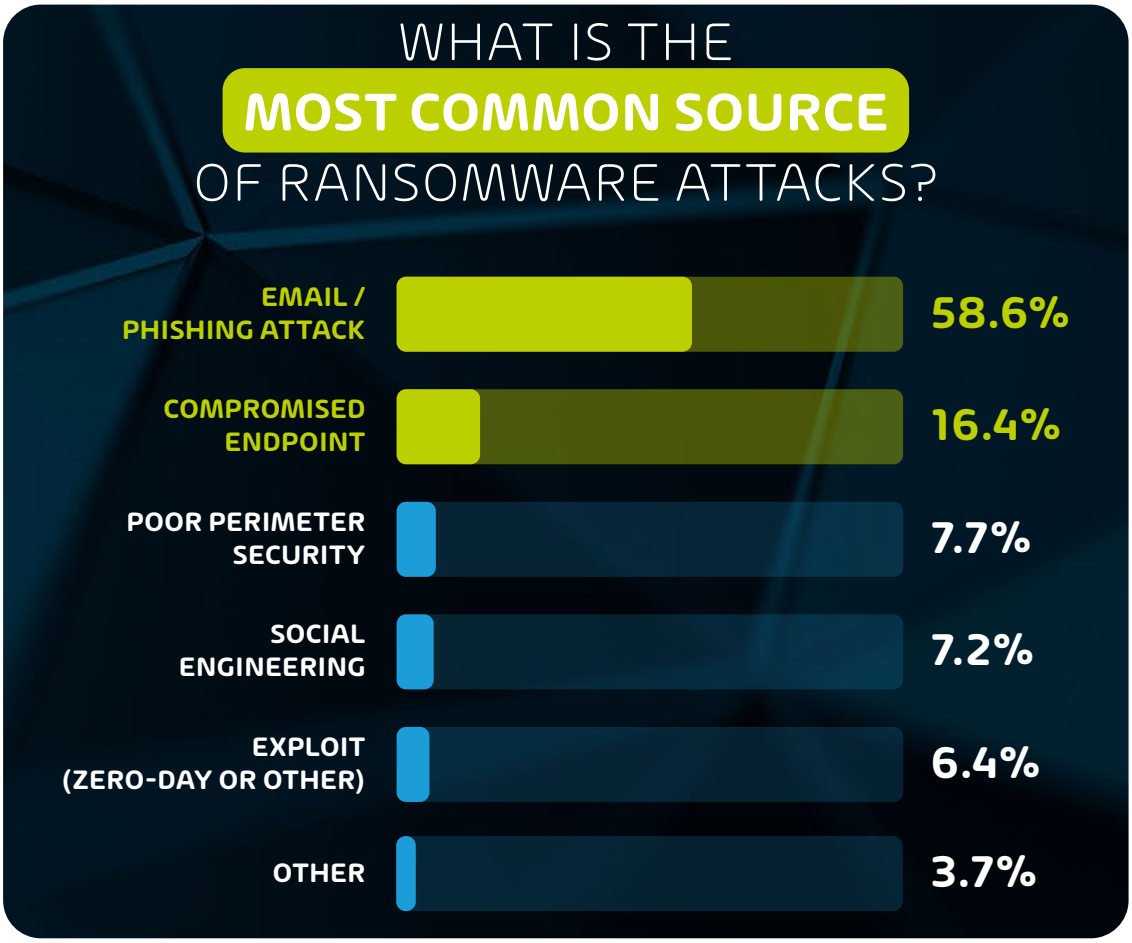


Of all the respondents that reported a ransomware attack, **1 in 7** (14.1%) indicated that their organization decided to either cut their losses and abandon the data that was ransomed, or they managed to recover some - but not all - of the compromised data. A further **6.6%** of respondents said their organization was left with no choice but to **pay the ransom.**

The rest were able to recover all their data from protected backups.

Available industry data from IBM also indicates that data breaches such as ones caused by ransomware attacks are not only more frequent, but more costly. Major data breaches in 2022 cost their victims an average of **$4.35 million**, a **2.6% rise** from the 2021 average of $4.24 million. This takes into account the potential ransoms paid, the cost of the significant down-time that a data breach can cause, and industry fines that can be levied against companies that fail to protect sensitive data.

WHAT IS THE MOST COMMON SOURCE OF RANSOMWARE ATTACKS?



For any of this survey's ransomware data to be actionable, we needed to understand the source of these attacks.

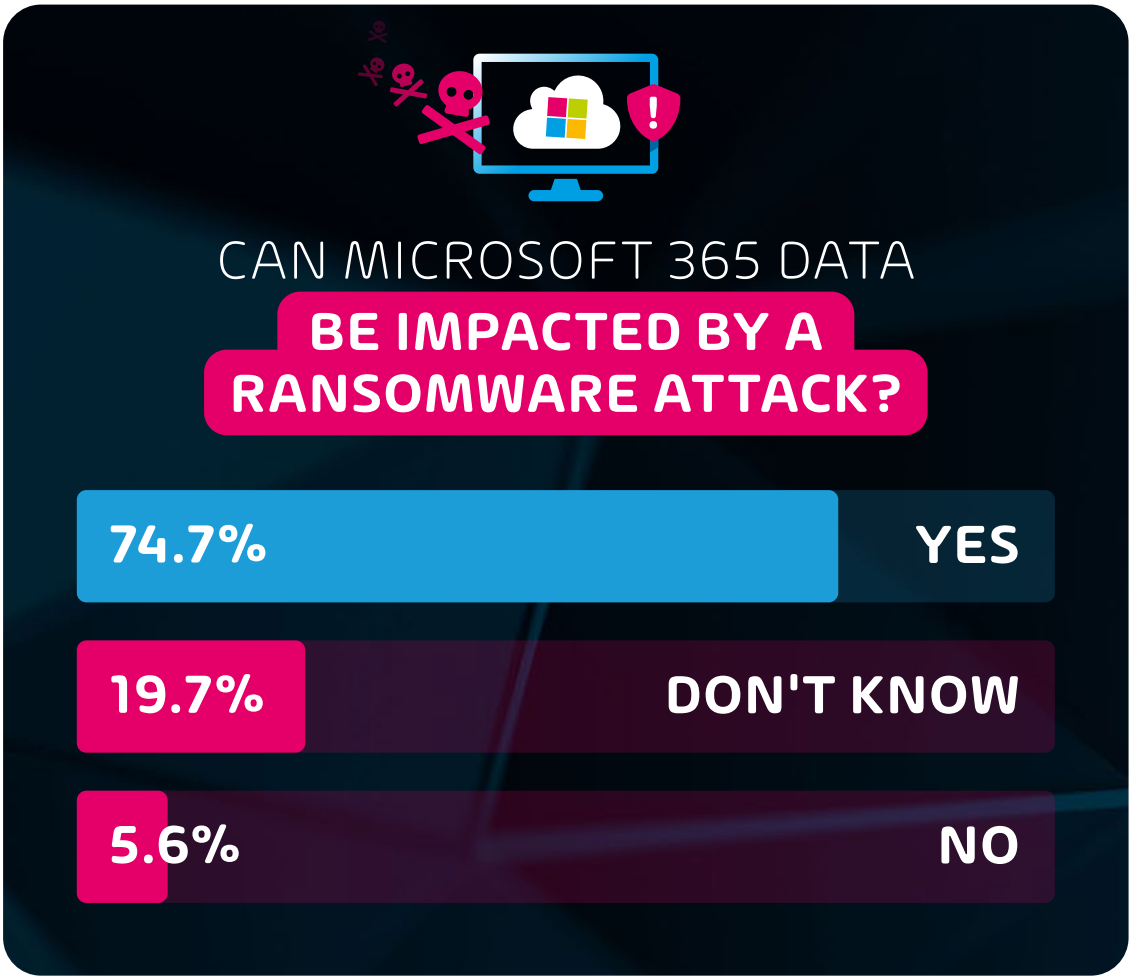
6 in 10 (58.6%) of the reported ransomware attacks were the result of **malicious email or phishing attacks.** This comes as no surprise, considering that the survey also revealed that **27%** of organizations **do not provide end-user training** on how to recognize and flag potential ransomware attacks. Furthermore, only 61.4% of organizations make use of email filtration and threat analysis technology.

Cybercriminals will always target an IT infrastructure's weakest link, and in most cases that link is the end user. Last year, we ran a survey focused on email security that found that 62% of email security breaches were caused by user-compromised passwords and successful phishing attacks. This indicates that when it comes to understanding how to prevent ransomware attacks, IT professionals need to start with the users.

Other sources of ransomware attacks include **'compromised endpoints'** (16.4%), **'poor perimeter security'** (7.7%), **'social engineering'** (7.2%), and **'exploits (zero-day or other)'** (6.4%).

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

CAN MICROSOFT 365 DATA BE IMPACTED BY A RANSOMWARE ATTACK?



As mentioned earlier, organizations are increasingly investing in cloud platforms for their IT infrastructure. In fact, our own Hybrid Cloud Adoption survey from earlier this year indicated that over half of IT professionals (54.8%) predicted their organization's IT infrastructure would either be 'cloud native' or 'mostly in the cloud' within the next 5 years.

However, there seems to be a lack of knowledge surrounding the security systems required by a cloud-based system.

1 in 4 respondents (25.3%) either **don't know** (19.7%) or **don't think** (5.6%) that Microsoft 365 data can be compromised by a ransomware attack. In reality, unsecured cloud-platforms are just as vulnerable, if not more so, than on-premise IT infrastructures.

Third-party security solutions, like Hornetsecurity's own 365 Total Protection suite, are practically a must for organizations to ensure their cloud data is properly protected.

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

4 IN 10 I.T. PROS USING MICROSOFT 365 IN THEIR ORGANIZATION SAY THEY HAVE NO RECOVERY PLAN IN PLACE

To further illustrate the point prior to this one, recovery plans are also more scarce among IT professionals that use cloud platforms such as Microsoft 365. Automatically assuming data is recoverable just because it is being stored within Microsoft 365 is a mistake that could cripple an organization.

While there is no chance of data being lost to hardware failure, cloud data is still **extremely vulnerable** to cyber attacks, especially if there are multiple end-points that are being used on foreign networks that might not be secured. This is usually the case among organizations that have employees that operate remotely. In this case, each employee likely has multiple end-points in their possession that could become compromised, such as a laptop and a phone, with access to **sensitive data** stored on Microsoft 365 services.

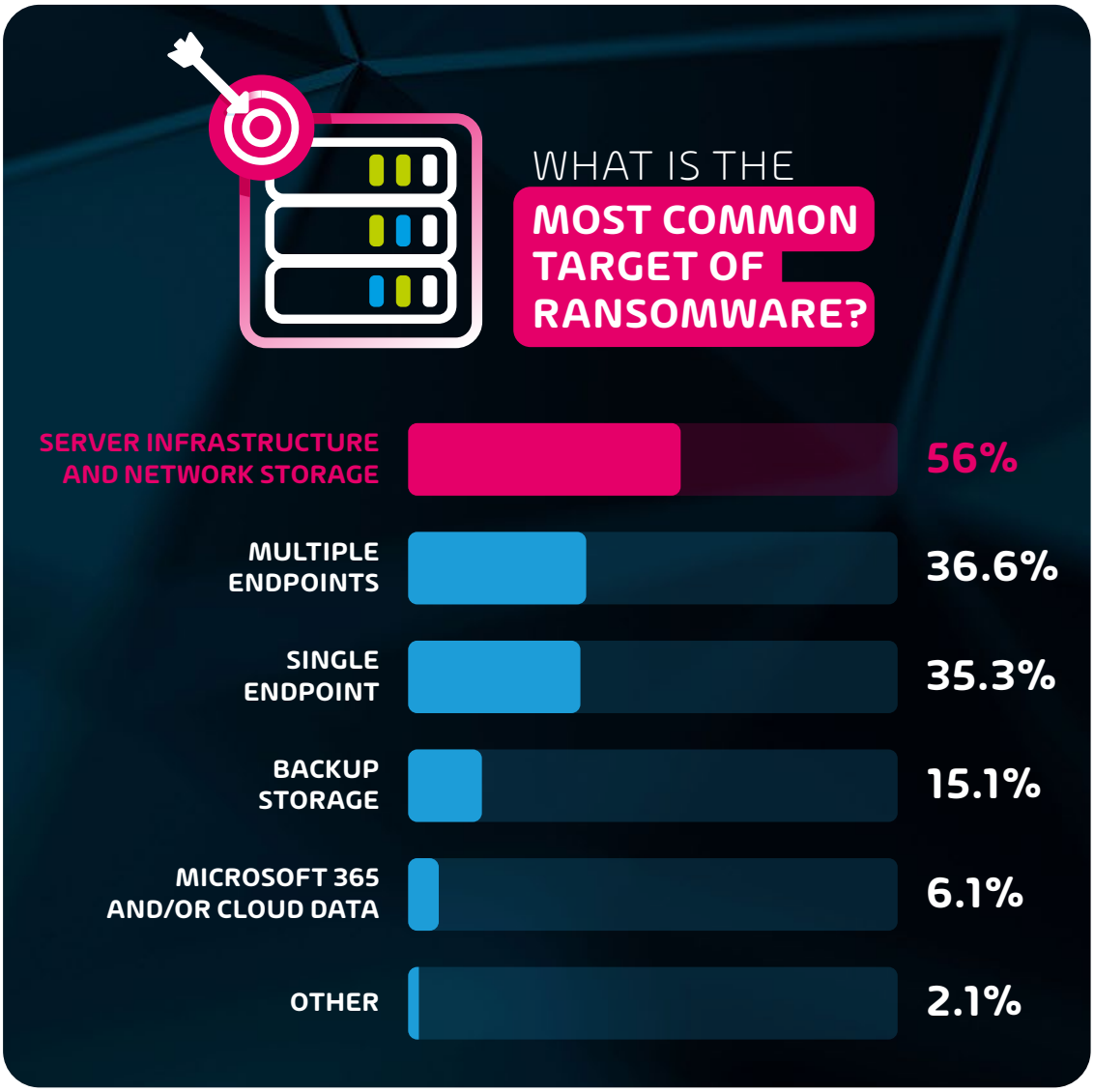
The risk of endpoints being compromised in the context of ransomware attacks is a significant one. As we pointed out earlier, the survey revealed that compromised endpoints were the second most common vector of ransomware attacks at 16.4%. This means that 1 of every 7 ransomware attacks happens due to **compromised unsecured endpoints** with access to critical data.

The counter to this risk would naturally be detection software with anti-ransomware capabilities built into each

endpoint. Our survey respondents agree with this, as this technology is the most commonly used among them, with 7 in 10 (69.2%) making use of it. That said, the fact that **3 in 10 organizations** do not use this **basic**, but effective, method of preventing ransomware attacks is concerning.

If your organization is one of the 4 in 10 that use Microsoft 365 without a recovery plan in place, join 50,000 companies around the world that use our solutions. Our 365 Total Protection Enterprise Backup is the only solution on the market that covers all aspects of security, backup and compliance for Microsoft 365.

WHAT IS THE MOST COMMON TARGET OF RANSOMWARE?



Our ransomware data reveals that **56%** of the nearly 400 respondents that reported having experienced a ransomware attack revealed that **server infrastructure and network storage** were impacted. It's likely that most of these attacks were targeting critical data with the aim of encrypting it. Usually that data takes the form of both operation-critical day-to-day data and backups of that same data.

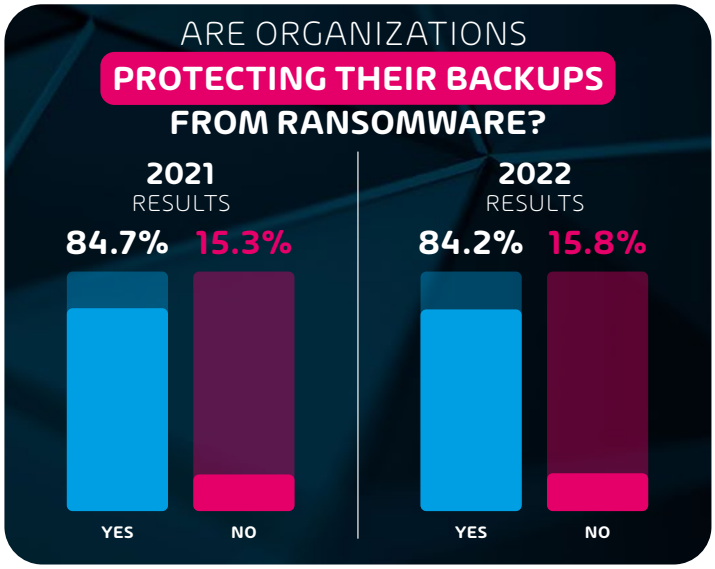
1 in 7 respondents (15.1%) indicated that **back-up storage** was specifically targeted.

The way an organization stores and protects its backups has a huge impact on how vulnerable it is to a ransomware attack. The reason for this is clear - if mission-critical data is consistently backed-up safely, then a ransomware attack can quickly be thwarted by simply replacing the now-encrypted data.

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

HOW ARE COMPANIES PROTECTING THEIR DATA FROM THE THREAT OF RANSOMWARE?

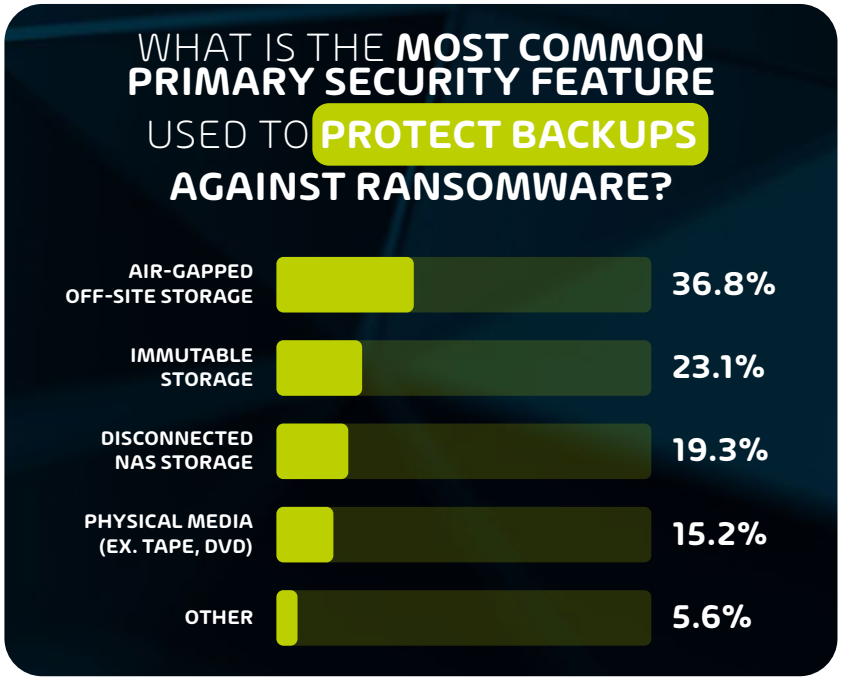
Are organizations protecting their backups from ransomware?



Since regularly keeping **and** protecting back-ups is the primary method of avoiding data loss or ransom payment, we asked respondents whether their organization currently actively protects its data from ransomware.

15.8% of our respondents indicated that they **do not.** This figure remained roughly the same in comparison to last year's survey (15.3%). This means that just over 1 in 7 organizations would be forced into **significant data loss** or have to **pay a ransom** in order to recover its data if a ransomware attack had to occur today.

What is the primary security feature organizations use to protect their backups in the event of a ransomware attack?

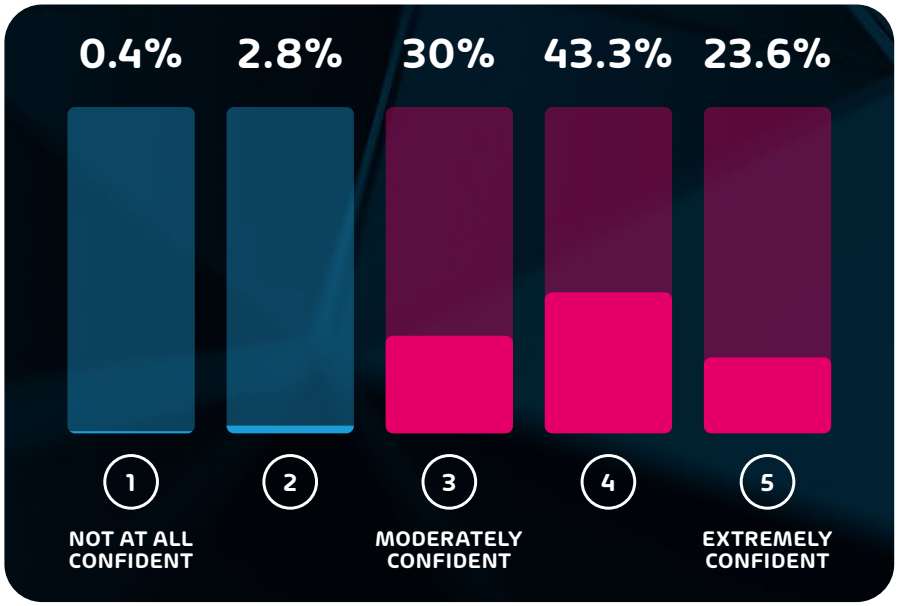


The most popular **primary** security feature used to protect backups from ransomware is air-gapped off-site storage (36.8%). Similar data-protection solutions that were also chosen by respondents include **immutable storage** (23.1%), **disconnected NAS storage** (19.3%), and **physical media** (15.2%). The majority of these solutions focus on separating primary back-up data from networks, making them inaccessible to would-be cybercriminals in the event of a compromised endpoint with access to the system.

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

HORNETSECURITY

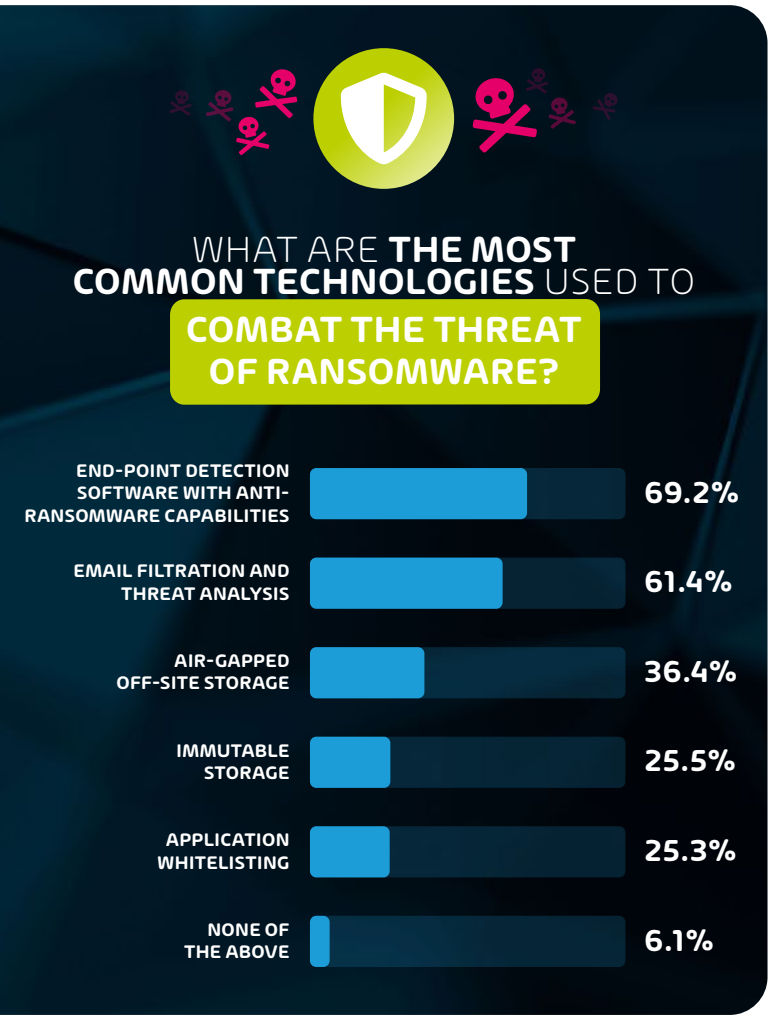
Are IT professionals confident in their primary back-up protection method?



The answer is an overwhelming yes, with **19 in 20** (96.9%) respondents saying they are 'moderately' to 'extremely' confident that their primary security feature would protect their backups from ransomware.

Considering the overwhelming number of reported situations where data was lost in a ransomware attack or a ransom had to be paid despite available security measures, this overconfidence may be misplaced.

What are the most common technologies used to combat the threat of ransomware?



We have an understanding of how organizations **protect** their backups, but what are they doing to **prevent** ransomware attacks from occurring at all? As mentioned earlier, the two most common vectors of attack were 'email/phishing attacks' and 'compromised endpoints'. It therefore makes sense that the most popularly used ransomware prevention technologies are **'end-point detection software with anti-ransomware capabilities'** and **'email filtration and threat analysis'.**

However, they are not quite as commonly used as one would assume, considering they are the most basic and available ways to prevent ransomware attacks. Email filtration and threat analysis is only used by **6 in 10** organizations (61.4%) and 'end-point detection software' only by **7 in 10** organizations (69.2%).

In comparison with 2021's ransomware data, a higher percentage of organizations were using methods of protection. **76.7%** of organizations were using end-point detection software, and **76.2%** used email filtration. These decreases in use could be attributed to our earlier observation that organizations are shifting more towards cloud platforms such as Microsoft 365, and as a result may be **relying upon their baked-in security features** rather than taking a proactive approach to prevent ransomware.

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

DO ORGANIZATIONS BUY INSURANCE THAT COVERS RANSOMWARE ATTACKS?

Our survey data shows that **37.9%** of companies reported having purchased specific insurance cover for ransomware attacks.

Last year, that figure was at **35.7%**, indicating that organizations seem to prefer spending their available budget on security upgrades rather than insurance.

This is a point we agree on. Ransomware insurance is not a bad idea in theory, however covering ransomware cases involves accounting for the entire operation of the company, and may require certain preventative measures to be taken to qualify for the insurance, which could prove an expensive endeavor overall.

FULL 2022 RANSOMWARE ATTACKS SURVEY RESULTS

If you'd like to take a look at the ransomware data, feel free to peruse the survey results here.

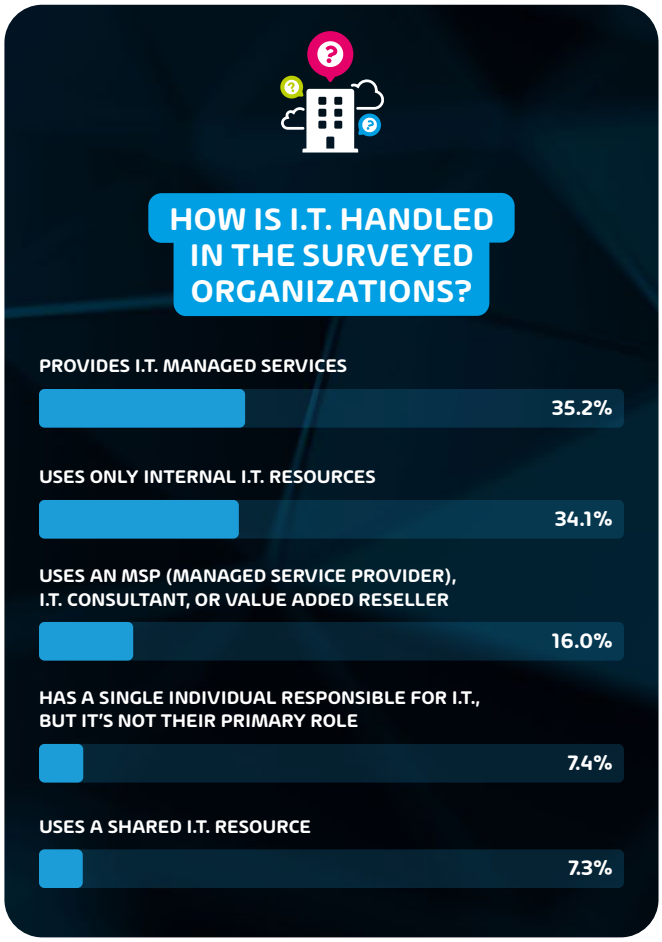
20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

HORNETSECURITY

ABOUT THE 2022 RANSOMWARE ATTACKS SURVEY RESPONDENTS

Here's a full breakdown of the survey respondents.

How is IT handled in the surveyed organizations?



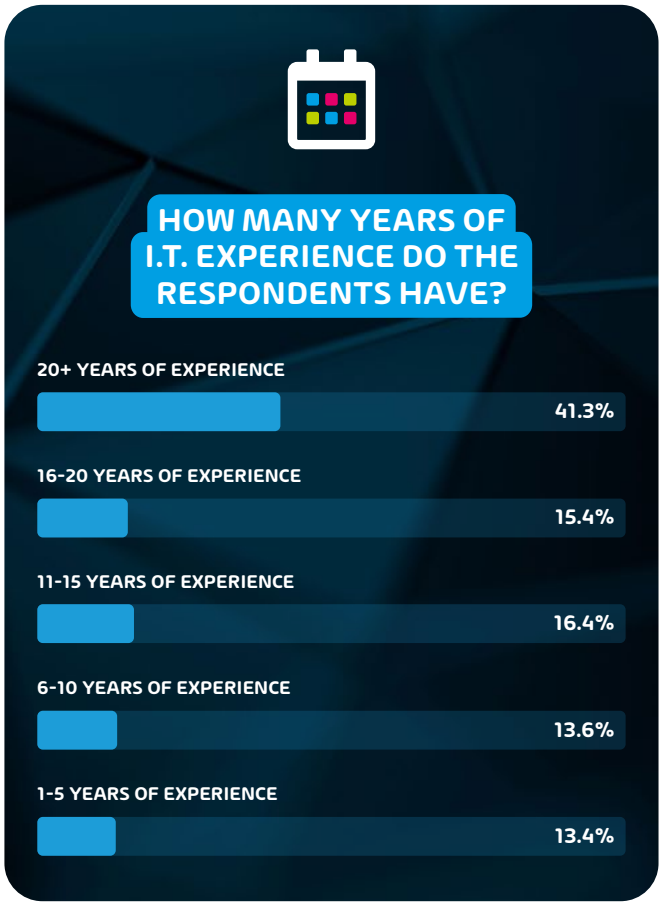
The three most common IT infrastructures among our respondents were: 'uses only internal IT resources' (34.1%), 'provides IT managed services' (35.2%) and 'uses an MSP (Managed Service Provider), IT Consultant, or Value Added Reseller' (16%). The remaining respondents are split between having 'a single individual responsible for IT' (7.4%) and using 'a shared IT resource' (7.3%).

What is the size of the organization the survey respondents work for by number of employees?

The size of the businesses that our respondents form part of varied between 1-50 (45.9%), 51-200 (20.5%), 201-500 (11.7%), 501-999 (5.9%), and 1,000+ (16%)

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

How many years of IT experience do the respondents have?



Nearly half (41.3%) reported over 20 years of experience in the field. The rest are split relatively evenly between 16-20 years (15.4%), 10-15 years (16.4%), 6-10 years (13.6%) and 1-5 years (13.4%).

Where are respondents based?

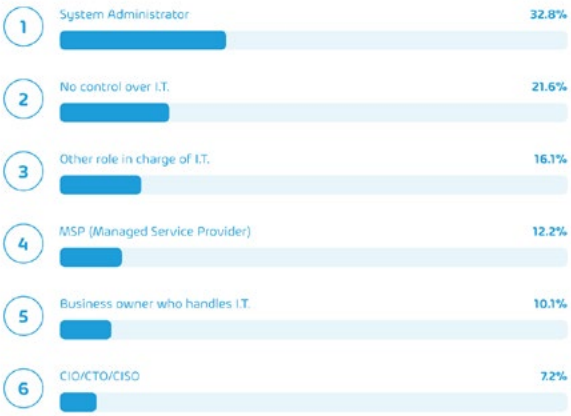
In terms of geography, the vast majority of respondents are based in Europe (45.5%) and North America (43%), while the remaining respondents are split between Asian territories (3.7%), Africa (3.1%), Australia (2.5%), the Middle East (1.2%) and South America (1.1%).

CONCLUSION

Based on the findings of this survey and its relationship to the data from last year's ransomware data survey, it's clear that the threat isn't going anywhere any time soon. The increase in overall incidence rate, and the fact that 1 in 20 IT professionals have experienced a ransomware attack in the last 12 months clearly indicates that organizations need to remain vigilant, especially as they begin to shift their IT infrastructure into the cloud.

While cloud technology provides significant benefits in terms of convenience and maintenance requirements, it requires a highly proactive approach to IT security in order to minimize the threat of cyber attacks and prevent ransomware incidents altogether.

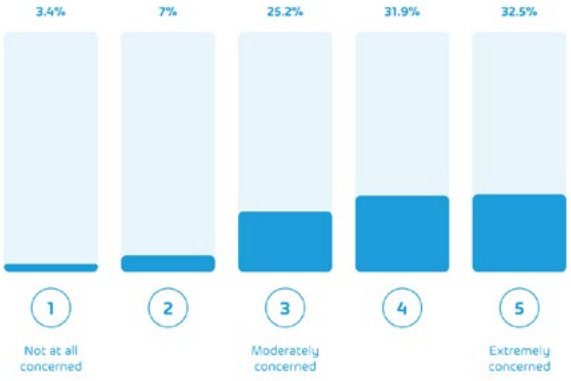
WHAT IS YOUR CURRENT ROLE?



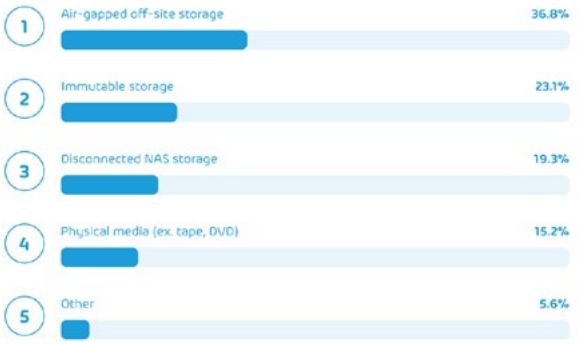
IN THE EVENT OF A RANSOMWARE ATTACK, DOES YOUR ORGANIZATION HAVE A DISASTER RECOVERY PLAN IN PLACE?

DO YOU CURRENTLY PROTECT YOUR BACKUPS FROM RANSOMWARE?

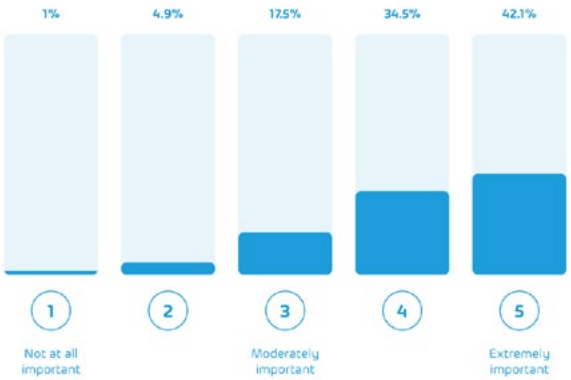
HOW CONCERNED ARE YOU ABOUT A RANSOMWARE ATTACK IMPACTING YOUR ORGANIZATION?



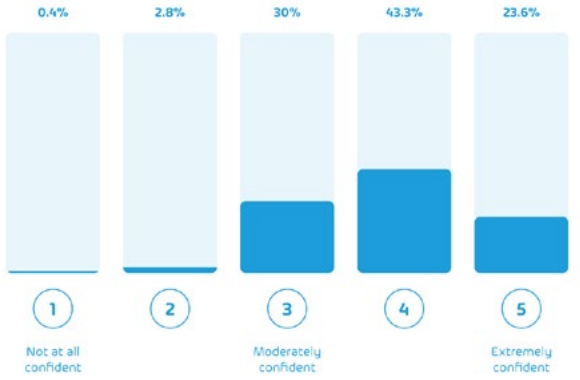
WHAT IS THE PRIMARY SECURITY FEATURE YOU USE TO PROTECT YOUR BACKUPS FROM RANSOMWARE?



HOW WOULD YOU RANK RANSOMWARE PROTECTION IN TERMS OF I.T. PRIORITIES FOR YOUR ORGANIZATION?



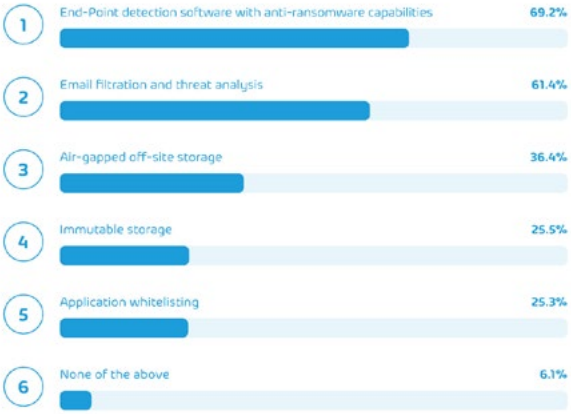
HOW CONFIDENT ARE YOU IN THIS METHOD?



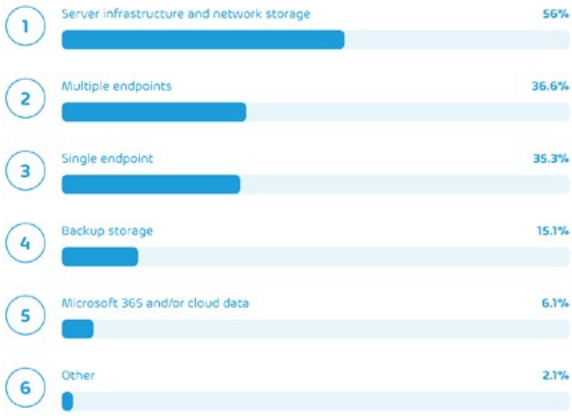
20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

HORNETSECURITY

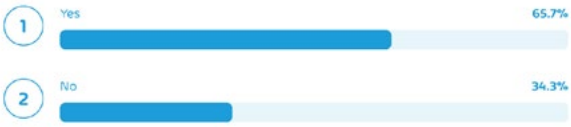
ARE YOU USING ANY OF THE FOLLOWING TECHNOLOGIES TODAY TO HELP COMBAT RANSOMWARE WITHIN YOUR ORGANIZATION?



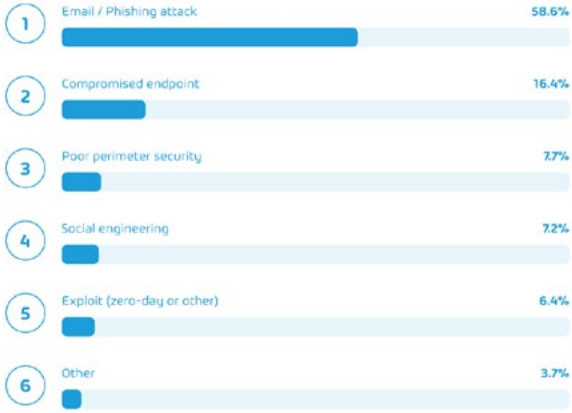
WHAT WAS THE LEVEL OF IMPACT OF THE RANSOMWARE ATTACK?



HAS THE THREAT OF RANSOMWARE ATTACKS CHANGED THE WAY YOUR ORGANIZATION BACKS UP ITS DATA?

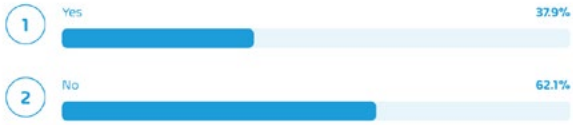


WHAT WAS THE VECTOR OF THE RANSOMWARE ATTACK?

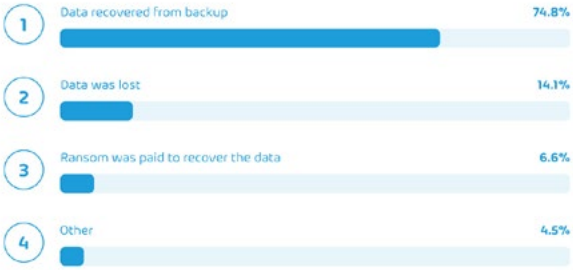


HAS YOUR ORGANIZATION BEEN THE VICTIM OF A RANSOMWARE ATTACK TO DATE?

DOES YOUR COMPANY HAVE, OR HAS IT EVER PURCHASED INSURANCE DESIGNED TO PROVIDE COVER IN THE EVENT OF A RANSOMWARE ATTACK?



WAS YOUR ORGANIZATION ABLE TO RECOVER FROM BACKUP, FORCED TO PAY THE RANSOM, OR WAS THE COMPROMISED DATA LOST?



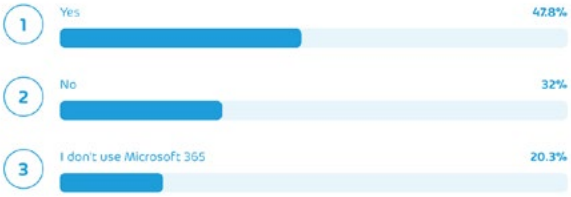
DOES YOUR ORGANIZATION PROVIDE TRAINING TO END USERS ON HOW TO RECOGNIZE AND FLAG POTENTIAL RANSOMWARE ATTACKS?

20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

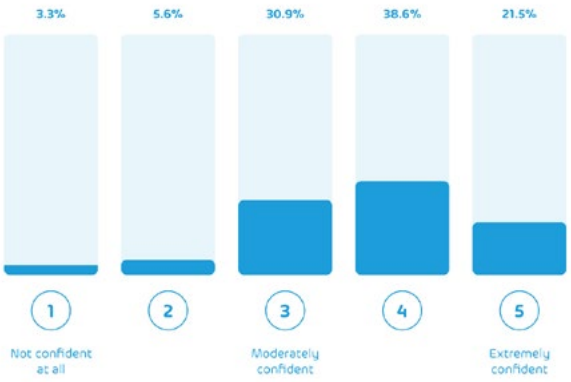
HORNETSECURITY

DO YOU THINK THAT MICROSOFT 365 DATA CAN BE IMPACTED BY A RANSOMWARE ATTACK?

IF YOUR MICROSOFT 365 DATA WAS COMPROMISED BY A RANSOMWARE ATTACK TODAY, DO YOU HAVE A RECOVERY PLAN?

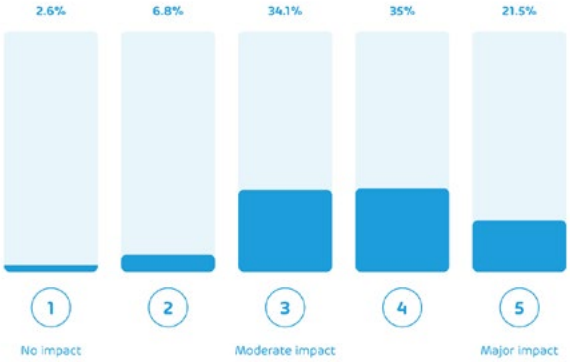


IF YOU FELL VICTIM TO A RANSOMWARE ATTACK TODAY, ARE YOU CONFIDENT YOUR DATA BACKUPS WOULD BE SAFE FROM HARM?



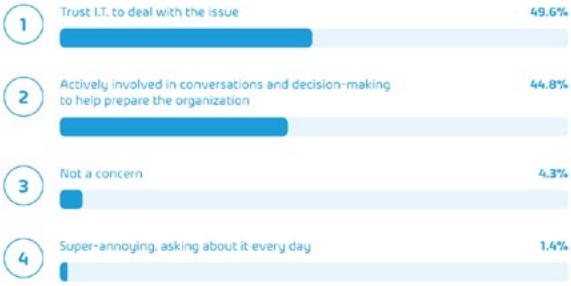
IF YOU HAD ACCESS TO MORE I.T. SECURITY BUDGET, WOULD YOU DIRECT THE MAJORITY OF IT TO:

HOW WOULD YOU RANK THE IMPACT THAT RANSOMWARE FEARS HAVE ON YOUR BACKUP/DISASTER RECOVERY PLANNING?



IS YOUR SENIOR LEADERSHIP TEAM AWARE OF RANSOMWARE AND ITS IMPACT?

HOW WOULD YOU DESCRIBE THE STANCE OF YOUR COMPANY'S SENIOR LEADERSHIP ON RANSOMWARE?

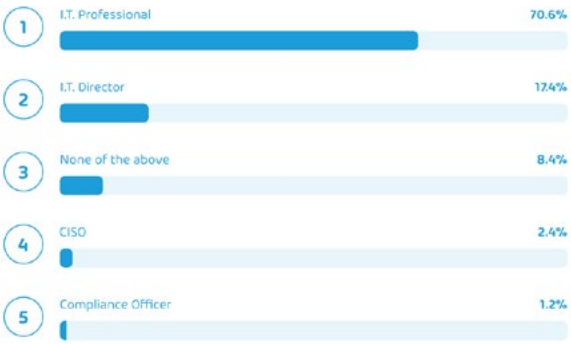


MY COMPANY:

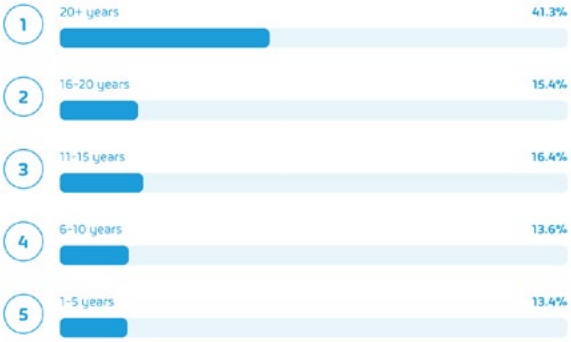
20% OF ALL REPORTED RANSOMWARE ATTACKS OCCURRED IN THE LAST YEAR, SURVEY FINDS

HORNETSECURITY

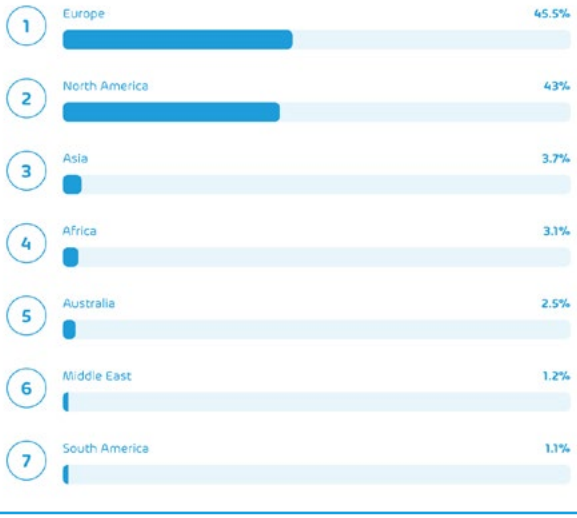
ARE YOU A/AN:



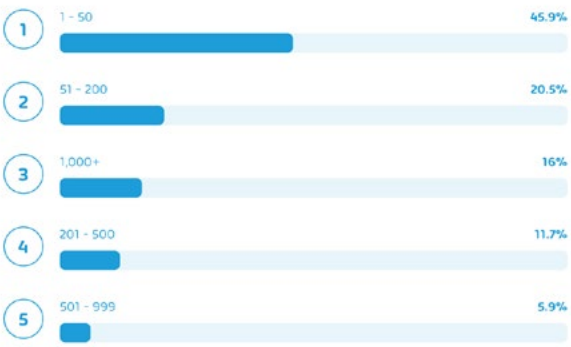
HOW MANY YEARS HAVE YOU BEEN IN THE I.T. INDUSTRY FOR?



WHERE ARE YOU BASED?



WHAT'S THE SIZE OF YOUR BUSINESS? (NUMBER OF EMPLOYEES)



WHAT INDUSTRY VERTICAL ARE YOU A PART OF?

HORNETSECURITY