March 2023

MARKET REPORT

2023 ransomware insights

The prevalence and impact of ransomware attacks around the world »

Barracuda®
Your journey, secured.

Contents

Introduction

Ransomware — an enduring and evolving threat

Ransomware is malicious software that is designed to infect a target's network and lock data and systems until a ransom is paid. It is an evolving and diversifying threat that can include the theft of sensitive or confidential information and a threat to publicly leak the data unless a ransom is paid. The criminal business model is a lucrative one — often available as a service and accessible to adversaries regardless of their resources or skill level.

Every organization is a potential target. Ransomware attacks can cripple day-to-day operations and customer supply chains, causing chaos and financial losses. They can destroy company reputations as well as customer relationships.

Our international survey explored the experience of ransomware attacks on organizations over the last 12 months. The findings show that almost three-quarters (73%) of respondents report being hit with at least one successful ransomware attack in 2022 — and 38% say they were hit twice or more.

The organizations that were hit multiple times with ransomware were more likely to say they had paid the ransom to restore encrypted data. Of those hit once, 31% paid the ransom to restore encrypted data — compared to 34% of those hit twice and 42% of those affected three times or more. Repeat victims were also less likely to use a data backup system to help them recover.

The findings show that for 69% of organizations, the ransomware attack started with a malicious email, such as a phishing email designed to steal credentials to gain access to the network so the cybercriminals can research assets, servers, and databases before ultimately launching the ransomware attack. Web applications and web traffic are in second place and represent an area of growing risk as part of an ever-expanding threat surface.

Organizations with cyber insurance were more likely to be hit by ransomware.

More than three-quarters (77%) of organizations with cyber insurance were hit by at least one successful ransomware attack, compared to 65% of organizations without cyber insurance. This could mean cybercriminals are more likely to target organizations with insurance, in the belief that the insurers will be willing to cover the ransom cost to speed up recovery.

The research also found that over a quarter (27%) of the organizations surveyed say they are not fully prepared to deal with a ransomware attack.

The security industry has an essential role to play in helping organizations address the threat of ransomware through deep, multilayered security technologies, threat hunting and extended detection and response (XDR) capabilities, and effective incident response to spot intruders and close gaps so that attackers cannot find an easy way in.

Methodology

Barracuda commissioned independent market researcher Vanson Bourne to conduct a global survey of IT managers and technical IT professionals, senior IT security managers, and senior IT and IT security decision-makers. There were 1,350 survey participants from a broad range of industries, including agriculture, biotechnology, construction, energy, government, healthcare, manufacturing, retail, telecommunications, wholesale, and others. Survey participants were from the U.S., Australia, India, and Europe. In Europe, respondents were from the United Kingdom, France, DACH (Germany, Austria, Switzerland), Benelux (Belgium, the Netherlands, Luxembourg), and the Nordics (Denmark, Finland, Norway, Sweden). The survey was fielded in December 2022.

The report also references Barracuda-commissioned research published in 2019. That survey included responses from 660 executives, individual contributors, and team managers serving in IT security roles in the Americas, EMEA, and APAC.

FINDING #1

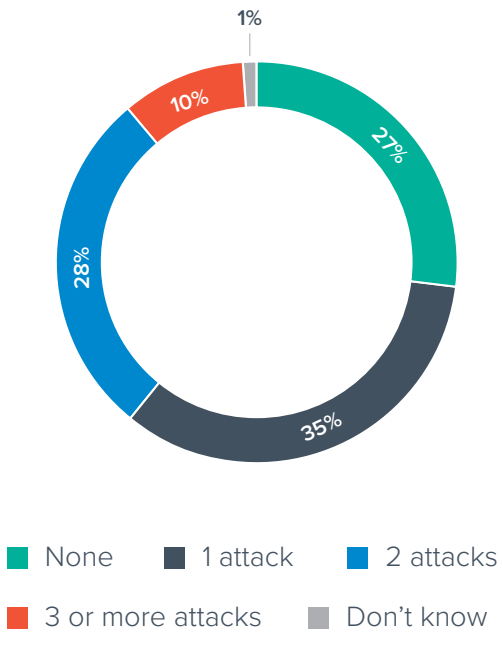
Most organizations have experienced a ransomware attack — a third have been hit twice or more

Just under three-quarters of the organizations surveyed (73%) reported at least one successful ransomware attack in the past 12 months.

The high proportion of organizations affected by ransomware overall should not be surprising. Hackers are increasingly turning to the ransomware-as-a-service model, which makes it easier — and cheaper — for attackers to launch ransomware attacks, often with little or no technical knowledge necessary. Ransomware-as-a-service (RaaS) is pay-for-use malware where the developers lease out their ransomware infrastructure to other cybercriminals.

How many successful ransomware attacks has your organization experienced in the past 12 months?

(n=1,350)



Over a third (38%) of the organizations surveyed reported two or more successful ransomware attacks in the past 12 months.

The fact that multiple successful attacks are possible suggests that security gaps are not fully addressed after the first incident.

There may be several reasons for this. For example, a lack of security controls, incident response, and investigation capabilities, coupled with growing attacker sophistication and stealth, could mean that implanted backdoors or other persistence tools left by attackers are not identified and removed. Access points might be left open and account passwords not reset so that stolen credentials can be abused again.

Fully neutralizing an attack is made harder because the attackers often misuse legitimate IT admin tools that are also used by IT teams for benign, everyday business purposes, so their appearance in the network may not immediately arouse suspicion.

Industry variations

There were significant variations in the industries targeted by ransomware. For example, almost all (98%) of consumer services organizations experienced at least one ransomware attack.

Consumer services often deal with a lot of personal customer data and receive a significant amount of communication from outside their organization, making them a good target for ransomware. At the same time, just 22% of respondents from this industry felt underprepared to deal with a ransomware attack.

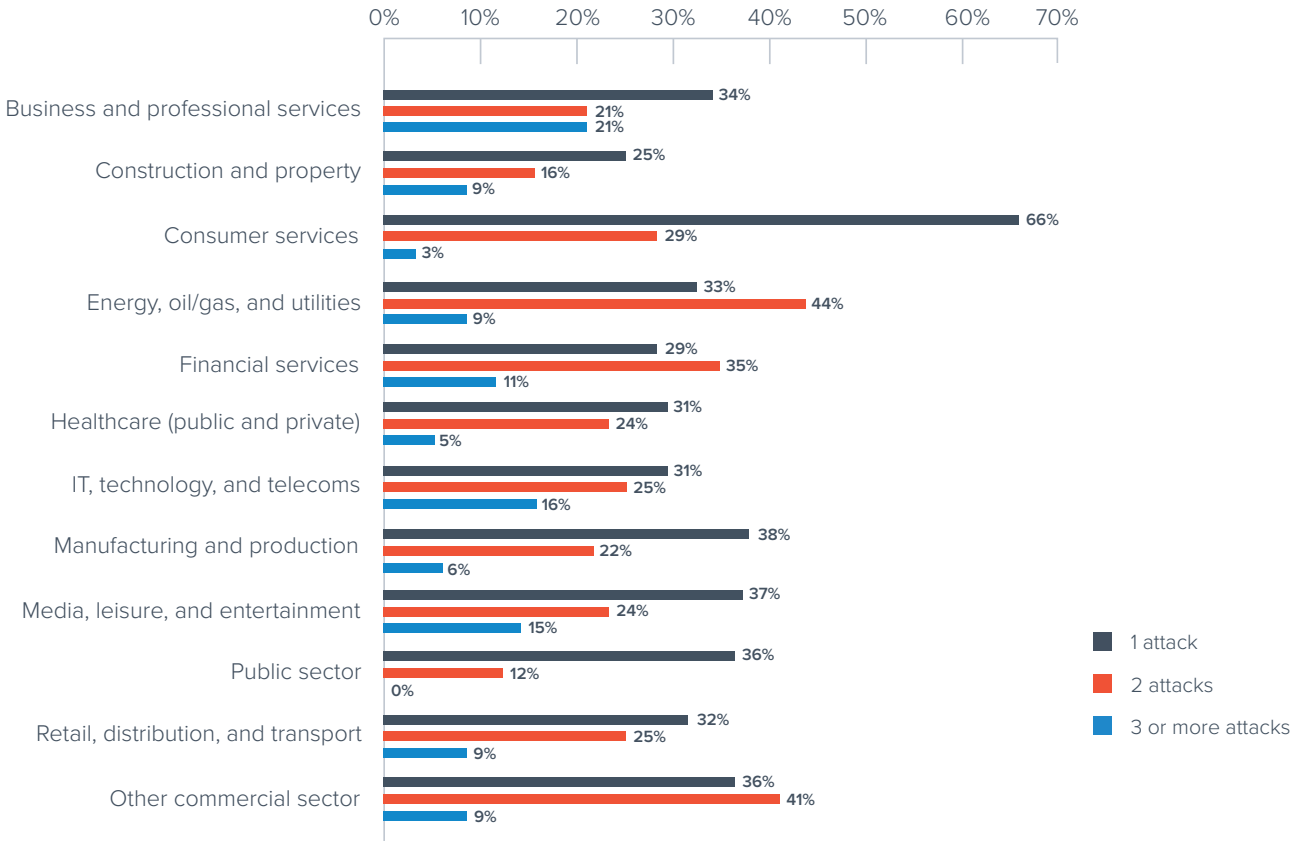
Energy, oil/gas, and utility organizations also reported an above-average success rate of ransomware attacks — 85%. Critical infrastructure is becoming a popular target, given the amount of disruption ransomware attacks can cause and the size of the potential payout. Our research last year into publicly reported ransomware attacks showed that infrastructure-related cyberattacks have quadrupled, which signals cybercriminals' intent to inflict greater damage beyond the impact on the immediate victim.

Energy, oil/gas, and utility organizations were also the most likely to be affected by multiple attacks, with 53% reporting two or more successful ransomware incidents, compared to an overall total of 38%.

46% of financial services organizations reported being hit twice or more. High-profile targets of ransomware, such as healthcare, were less likely to be hit with multiple attacks, with just 29% of respondents from that sector reporting two or more successful attacks.

Number of successful ransomware attacks in 12 months by industry

(n=1,350)



FINDING #2

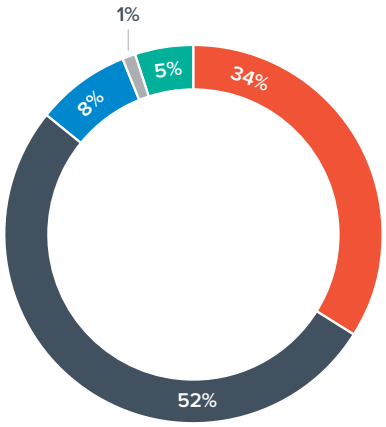
Repeat victims are more likely to pay the ransom to recover encrypted data

A successful ransomware attack will usually encrypt valuable data within an organization. A full 95% of surveyed organizations that have experienced a successful ransomware attack in the last 12 months reported that their data was encrypted, causing major disruption to their business.

Overall, only 1% lost the encrypted data, 34% chose to pay the ransom, and 52% used their backup systems to get the data back.

Did cybercriminals manage to encrypt your organization's data during the most significant ransomware attack experienced in the last 12 months?

(n=982)



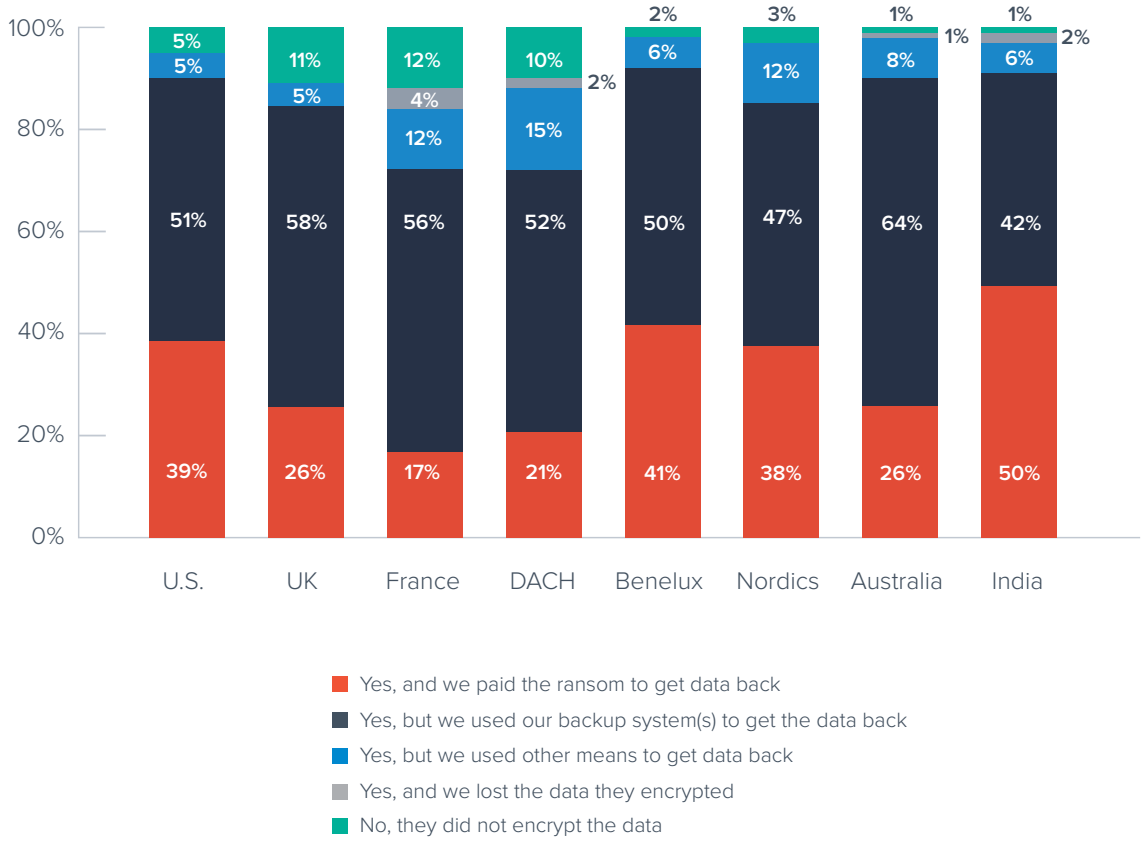
- Yes, and we paid the ransom to get data back
- Yes, but we used our backup system(s) to get the data back
- Yes, but we used other means to get data back
- Yes, and we lost the data they encrypted
- No, they did not encrypt the data

The willingness to pay a ransom, regardless of the number of attacks, varied significantly by country and industry.

The UK, France, DACH countries, and Australia had fewer instances of organizations paying the ransom to get their data back, while in India, the ransom was paid in 50% of attacks. But almost across the board, restoring from backup was the top method of recovery.

Did cybercriminals manage to encrypt your organization's data during the most significant ransomware attack experienced in the last 12 months?

(n=982)

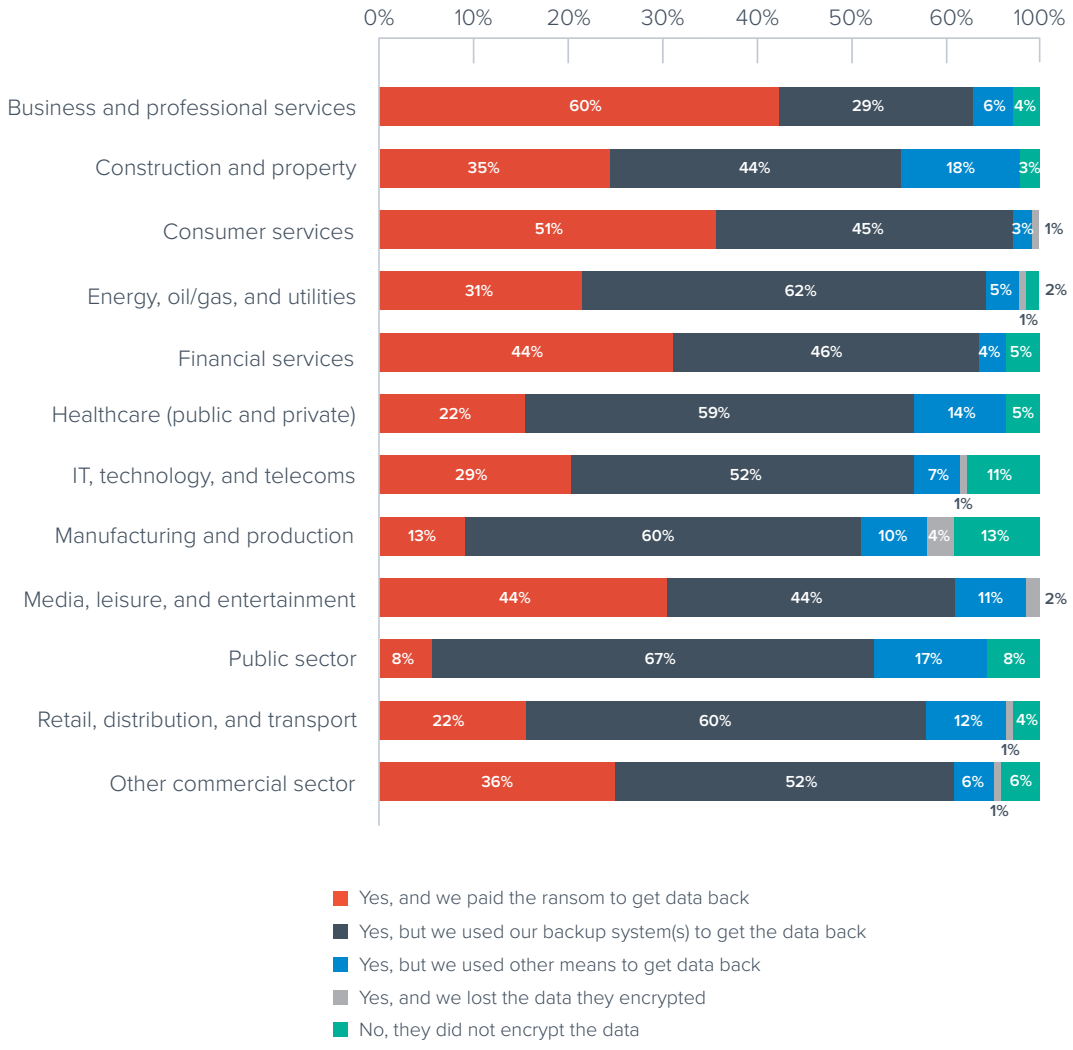


Organizations in the business and professional services sector were the most likely to pay the ransom to get the data back, with companies doing so in 60% of cases. Consumer services organizations paid the ransom in 51% of cases, while both financial services and media, leisure, and entertainment organizations paid in 44% of attacks.

Healthcare organizations were less likely to pay the ransom and did so in only 22% of cases.

Did cybercriminals manage to encrypt your organization's data during the most significant ransomware attack experienced in the last 12 months?

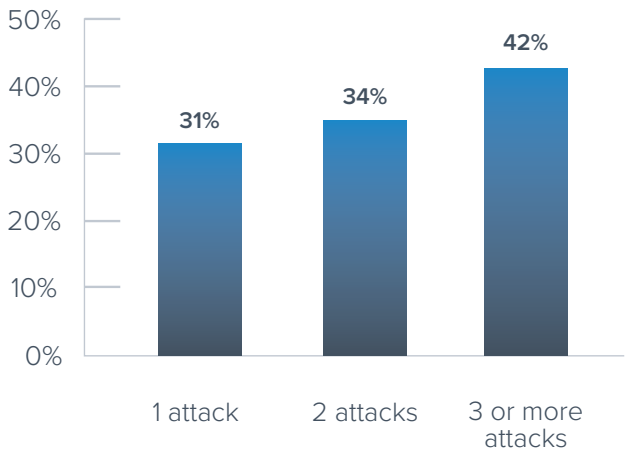
(n=982)



The survey found that organizations that were hit most often with ransomware were also more likely to pay the ransom to restore encrypted data — 42% of those who experienced three or more attacks paid the ransom. They were also less likely to use a data backup system to help them recover.

Organizations that paid the ransom to restore encrypted data

(n=982)



The proportion of organizations that paid the ransom despite, or possibly because of, being hit with two or more successful ransomware attacks aligns with the findings of other studies. For example, a 2022 study on ransom payments found that 80% of ransomware victims that pay the ransom are hit a second time — and often pay the ransom again.

One possible explanation for a connection between multiple attacks and ransomware payments is that once it is known that an organization is willing to pay, other attackers will target the same victim.

Underground marketplaces and initial access brokers (IABs) are likely to place a premium on access credentials to victims that are known to be willing to pay and remain vulnerable. In some reported instances, the same attackers return for more.

Investing in a data protection solution that helps to back up and restore data can help to avoid paying a ransom that could otherwise encourage cybercriminals to attack again.

FINDING #3

Email is the most common starting point for ransomware attacks

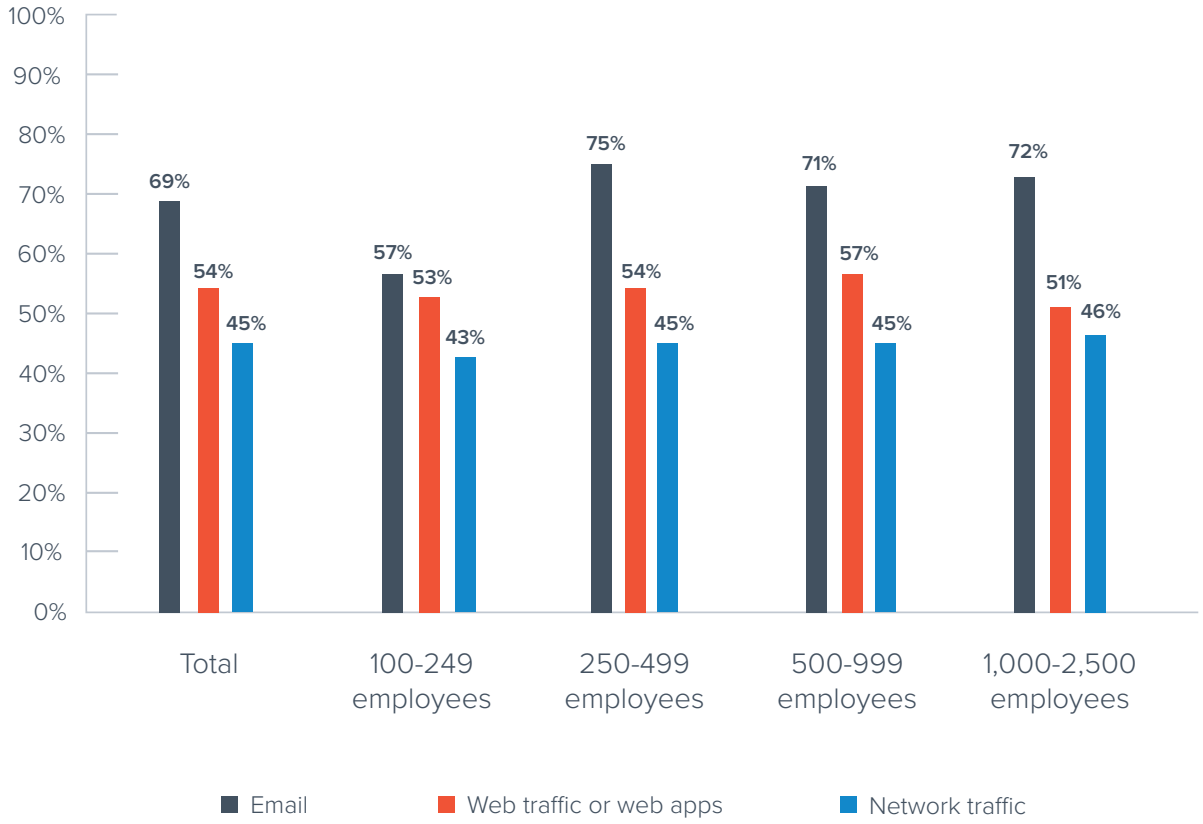
For 69% of organizations, ransomware attacks started with a malicious email.

For slightly larger organizations with over 250 employees, this percentage is higher than average (75%). Sending an email is much simpler than penetrating an organization's network.

Traditionally, hackers would attach a document with a malicious payload or a URL leading to a fake website capable of distributing malware. As organizations deployed advanced threat protection such as sandboxing and time-of-click URL protection, cybercriminals turned to social engineering tactics to phish for users' login credentials. Compromised accounts can be an easy launchpad for ransomware attacks, allowing cybercriminals to move laterally inside the organization and avoid detection. Organizations that want to improve their defenses against ransomware should start with investing in their email security and dedicated phishing detection in particular.

Where did the ransomware attacks your organization experienced originate?

(n=982)

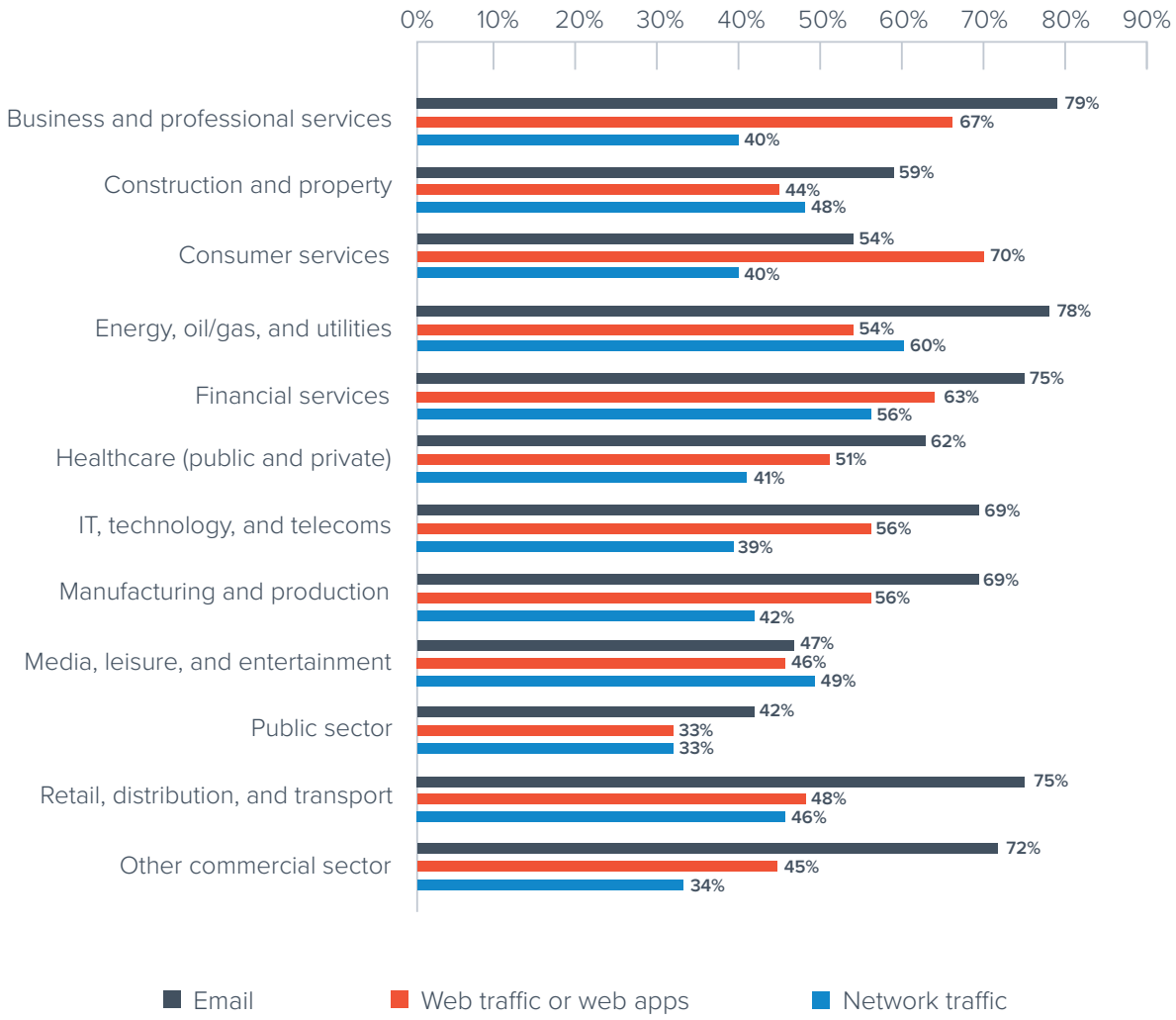


However, email is not the No. 1 ransomware threat vector for every industry. For example, most ransomware attacks in consumer services originated from web traffic and web applications.

Online applications like file-sharing services, web forms, and e-commerce sites can be compromised by attackers. Web applications are attacked through the user interface or an API interface. Often these attacks involve credential stuffing, brute force attacks, or OWASP vulnerabilities. Once the application has been compromised, the attacker can introduce ransomware and other malware into the system. This can go on to infect the network as well as users of the application.

Where did the ransomware attacks your organization experienced originate?

(n=982)



FINDING #4

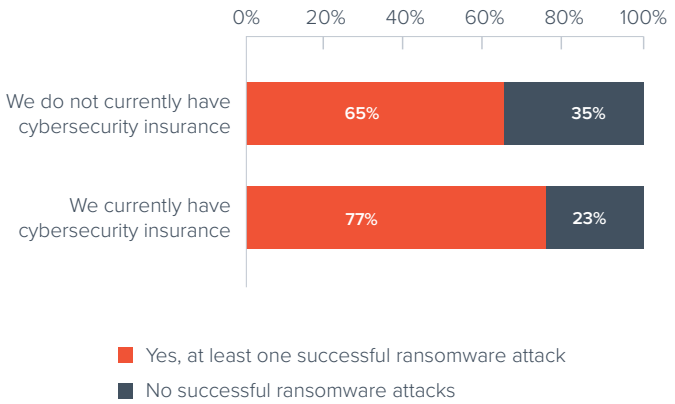
Organizations with cyber insurance are more likely to be hit by ransomware

63% of surveyed organizations have invested in cybersecurity insurance to help them minimize costs associated with any kind of data breach. While cyber insurance companies can help negotiate ransom payments or even provide the funds for the payment, multiple exclusions within their policies often mean that organizations will still face a very large bill.

Organizations that have cyber insurance were more likely to be hit by a successful ransomware attack in the past year. **77% of organizations with cyber insurance were hit by a successful ransomware attack, compared to 65% without cyber insurance.** This could mean cybercriminals are more likely to target organizations with insurance, in the belief that the insurers will be willing to cover the ransom cost to speed up recovery.

Has your organization experienced at least one successful ransomware attack in the past 12 months?

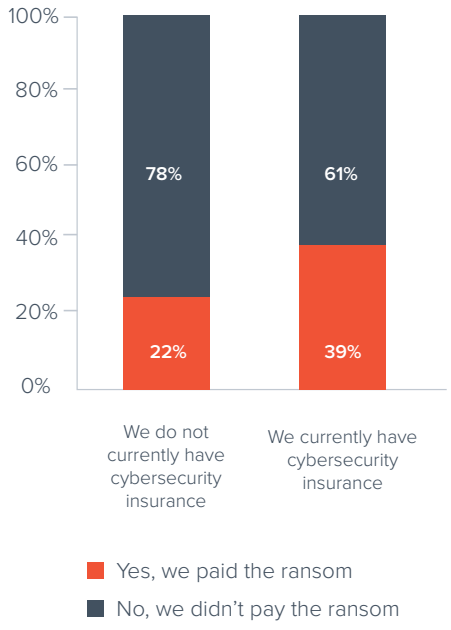
(n=1,350)



For example, the survey results show that **companies with cyber insurance were more likely to pay the ransom to get their data back (39% vs. 22% of organizations without cyber insurance)**. And while a connection can't be established, it is also worth noting that **organizations affected by two or more ransomware attacks were also more likely to have cyber insurance in place (70%)**.

Did you pay the ransom to get the data back?

(n=982)



FINDING #5

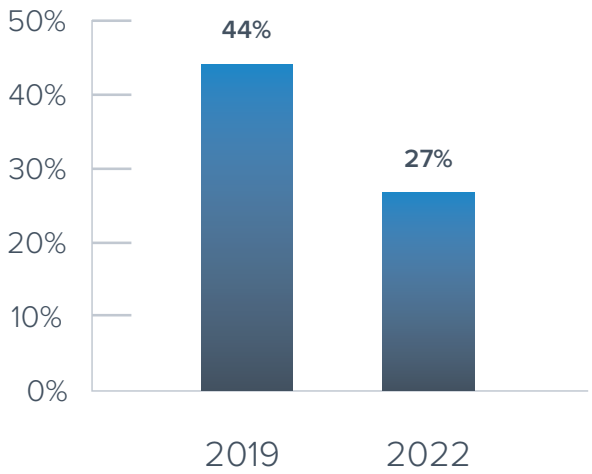
Many organizations feel they're not fully prepared for ransomware

Over a quarter (27%) of the organizations surveyed say they are not fully prepared to deal with a ransomware attack.

This is an improvement from an earlier study conducted in 2019, when almost half (44%) said they were unprepared for a ransomware attack. Since 2019, we've seen some very high-profile ransomware attacks that have resulted in significant financial losses. The extensive publicity surrounding these attacks likely resulted in many organizations investing in their security and preparing for potential ransomware attacks.

Not fully prepared to deal with ransomware

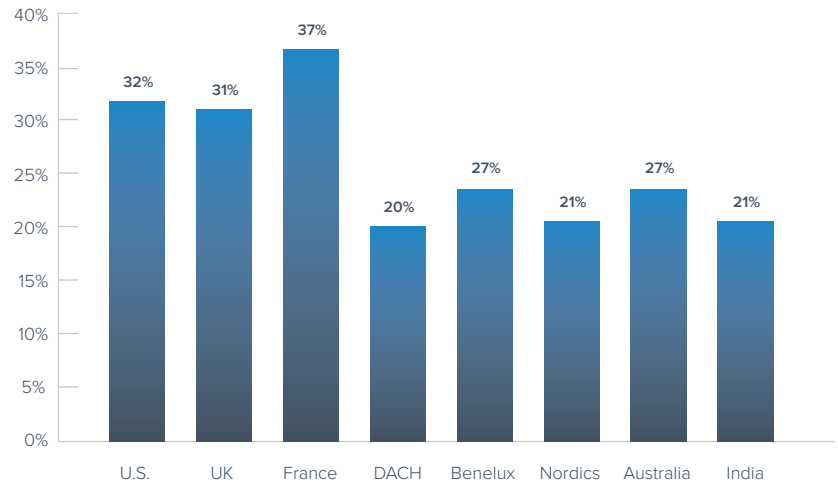
(n=660 for 2019; n=1,350 for 2022)



Previous research from NordLocker found that the U.S., UK, Canada, and France experience the highest number of ransomware attacks at a global level. Our research found that respondents from the U.S., UK, and France also feel less prepared to deal with ransomware. Most likely, the number of attacks feels overwhelming, and they're concerned the high volume increases the chances of the threat actors' success. Larger organizations also feel less prepared as they have a large volume of data to protect and a much larger attack surface.

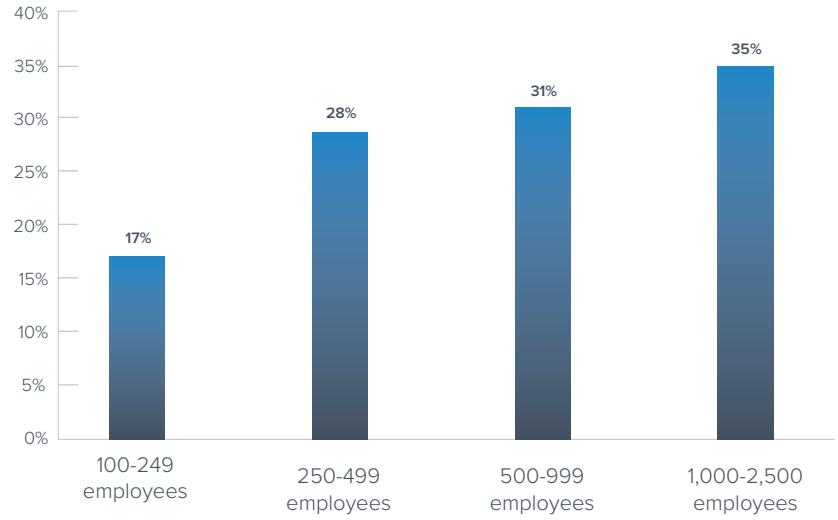
Not fully prepared to deal with ransomware

(n=1,350)



Not fully prepared to deal with ransomware

(n=1,350)



Conclusion

Organizations need integrated and multilayered security to protect their ever-expanding attack surface from evolving threats such as ransomware. Here are the top cybersecurity areas to focus on to minimize your risk and exposure to ransomware and other cyberthreats.

- **Protect your credentials.** Securing credentials requires a two-pronged approach: First, invest in detection and response tools, and then focus on training your users.

- Email protection technology should be able to detect malicious payloads delivered through links or attachments and also recognize when attacks use advanced social engineering tactics designed to bypass filtering technology and trick users into action. Look for email security that integrates machine learning technology as this will identify social engineering attacks with a higher degree of accuracy, looking for the smallest deviations from usual communication patterns.

- It is also important that employees know how to recognize and report suspicious emails. Use tools such as phishing simulation, and test the effectiveness of any training.

- **Secure access to accounts, applications, networks.** Multifactor authentication (MFA) remains a best practice and is something that should be adopted by every organization. However, attackers have been finding ways to get around MFA. Consider implementing a more advanced Zero Trust access strategy that continuously verifies users and devices and only allows the right users to access the right resources.

- **Secure your web applications.** Online applications like file-sharing services, web forms, and e-commerce sites can be compromised by attackers. Applications are often targeted through the user interface or an API interface. Consider implementing API-based application security and a next-generation web application firewall that will provide multilayered security to block advanced threats, including zero-day attacks; intrusion prevention and sandboxing of malware; and powerful network segmentation to prevent lateral movement within the network.

- **Back up your data.** To protect your organization from the full impact of a ransomware attack, data needs to be properly and securely backed up and isolated — even when it's in the cloud. You also need to make sure that your data backup will allow you to restore data in a reasonable time frame, so regularly test your backup recovery process to confirm it works.

- **Build defense-in-depth with threat intelligence, incident response, and XDR.** The release of ransomware is often the final stage of attack and can be preceded, for example, by lateral movement, data exfiltration, the installation of additional tools, and more. If you can detect and block the attack at these earlier stages, you might be able to prevent the full impact of the ransomware.

- This is where services such as XDR come in. XDR (extended detection and response) provides visibility of an entire IT environment, underpinned by continuously updated threat intelligence. XDR and other automated incident response solutions will help you identify, contain, and neutralize incidents before they escalate.

- It is also important to keep up to date with the evolving threat landscape, including the latest attacker behaviors and tools, so you know what to look out for and how to respond. You should aim to investigate everything that doesn't look or feel right. If you are concerned that you lack the resources to do this, consider the services of an outsourced Security Operations Center, for example, as part of your XDR platform that will monitor your network 24/7 and investigate anomalous or suspicious behavior.

Further information and practical guidance on how to protect against ransomware can be found in Don't pay the ransom – a three step guide to ransomware protection, which includes a downloadable ransomware protection checklist to get you started.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

Get more information at barracuda.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and Their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit vansonbourne.com.

Barracuda®
Your journey, secured.