Ransomware: the true cost to business 2024

Our Annual Global Study on Ransomware Business Impact

Attackers are evolving. Paying isn't the solution. **It's time to reject the ransom.**

cybereason©

Foreword

If I could have one wish for 2024, it would be that we stop calling ransomware by the same name.

It fails to describe the true impact of an attack. What started as the simplest of notions—encrypting data and extorting money to return access to it—evolved into a complex "Swiss army knife", like the blended attacks back in the early 2000s.

Now ChatGPT has arrived on the scene and it's driving the next evolution of ransomware.

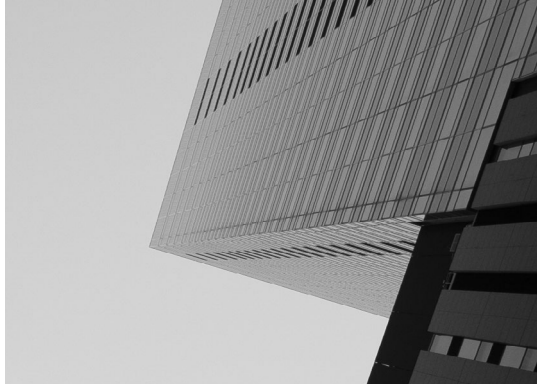
In last year's survey, we began to see ransomware attackers have greater success in non-English language countries (Italy, Germany, France and Japan). This trend is being accelerated by generative AI tools that enable attackers to translate and localize their activities faster and at scale. These tools also enable them to scrape public information on people and companies, which they use to develop highly personalized social engineering attacks. Generative AI also reduces the skills required to codify attacks, lowering the barrier of entry and increasing automation in writing attacks, especially with tools such as wormGPT.

This year's research shows that, while most businesses have a ransomware strategy in place, many are incomplete. They're either missing a documented plan or the right people to execute it. As a result, we see that many organizations are paying the ransom. Likewise, whilst many have cyber insurance, too many simply don't know if or to what degree it covers them for ransomware attacks.

This is problematic on several levels. It's no guarantee that your data and systems will be returned uncorrupted, that attackers won't sell your data on the black market, or that you won't be attacked again. And if there's any evidence that your payment was used to fund terrorism or organized crime, you could find yourself facing criminal charges.

So, what's the takeaway this year? It's that the threat continues to evolve at pace while businesses' ransomware resilience capabilities struggle to keep pace. Now is the time to stress test your capabilities, involve the rest of the business, and ensure you are sufficiently protected against today's attackers as well as tomorrow's.

Greg Day
Global Field CISO, VP Cybereason



Objective: Learn from those who have been breached

This report was commissioned to help defenders share their experiences as they work to educate their business peers on the importance of keeping ransomware at the top of the agenda.

Ransomware attacks are becoming more frequent, more sophisticated, and more effective. This year we wanted to find out how those who have been breached prepare for future attacks.

We also wanted to know:

- How attackers are getting into networks
- What they're after
- How many breached organizations agreed to pay a ransom
- Whether paying the ransom was worth it

We surveyed

1,008

enterprise IT professionals

were responsible for cybersecurity

All have been **breached** at least once in the previous

24

months.

The results continue to surprise us.

As you'll see, organizations that have been breached in the past are still at risk, and many of them don't think they're fully prepared for another ransomware attack.

The results at a glance

This year's results paint an interesting picture. Despite being breached before, many defenders don't believe their organizations have the right people and plans in place to manage the next attack.

Attackers are evolving

More complex, low-and-slow attacks are designed to compromise as much of the targeted network as possible to exact the highest ransom in 'RansomOps' attacks.

56%

said their organization didn't detect a breach for **3-12 months.**

What were they after?

- **Intellectual Property (IP)/ Trade secrets**
- **Personally Identifiable Information (PII)**
- **Protected Health Information (PHI)**
- **Customer data**
- **Account credentials**

How did they get in?

41% got in via a **supply chain partner.**

24% got in **directly.**

22% got in with the help of **an insider.**

Paying the ransom isn't the solution

Despite most victims agreeing to pay the ransom, **less than half who did got their systems and data** back uncorrupted. And **most were breached again** within a year.

84% paid the ransom.

But only 47% got their data and services back **uncorrupted.**

Why did they pay the ransom?

- **Attackers threatened to disclose sensitive information**
- **We feared loss of business**
- **It seemed to be the fastest solution**
- **It was a holiday/weekend and we were short-staffed**
- **It was a matter of life and death**
- **We didn't have backup files**

78% were then breached again.

And 63% of these were asked to **pay more** the second time.

82% were **breached again** within a year.
36% by the **same actor.**
42% by a **different actor.**

The true impact is staggering

Ransom fees remain high, and they're **just the tip of the iceberg** when it comes to the **true cost** to a business.

Average ransom payments over the last 24 months:

USA: $1.4 million

France: $1 million

Germany: $762k

UK: $423k

46% estimate business losses of $1-10 million.

16% estimate losses of over $10 million.

The true **cost** is much **higher** and includes:

- Brand damage
- Lost revenue
- Temporary closure
- C-level resignations
- Layoffs

Businesses need to do more

Most organizations **increased their investment** in cybersecurity after a breach, but the **risk remains.**

Less than half of defenders say they're adequately prepared for the next attack.

87%

increased cybersecurity spend.

Yet only

41%

feel they have the right people and plan to manage the next attack.

37%

have the **right people** but not the plan.

18%

have the **right plan** but not the people.

They're investing in:

1. Cybersecurity talent
2. Awareness training
3. New tech (e.g. endpoint tech & identity services)
4. Increased internal/supply chain compliance
5. Cyber insurance
6. Cryptocurrency wallets

What's happening and how to prepare for it

Attackers are making use of generative AI and machine learning to find new ways into networks and to scale their activities. At the same time, organizations are being held back by several challenges.

We have identified **6 core challenges** and, while none of these are easy to overcome, here is some advice on how to help your business prepare for each.

1/ Attackers are becoming more effective, thanks in part to generative AI

What's happening

Businesses everywhere are working out how best to leverage generative AI to become more effective and efficient at scale. And so are bad actors. They are using tools like ChatGPT 4.0 to collect personal information, craft professional-looking messages, and more effectively translate them into any language.

How you can prepare

Ensure all employees are aware of the increased risk of bad actors using these tools to create messages that seem less suspicious. Show them what to look out for and run regular drills. Make sure all teams are following basic good practice when it comes to security hygiene. And work with a cybersecurity provider to secure critical systems and data. Some providers are now using AI to automate ransomware detection and protection.

Is generative AI dangerous?

> In February 2023, researchers from security firm Checkpoint discovered that malicious actors had been able to alter a chatbot's API, enabling it to generate malware code and putting virus creation at the fingertips of almost any would-be hacker.

Hear more on this episode of our **Malicious Life podcast.**

2/ The talent gap continues to widen

What's happening

The global cybersecurity workforce may have reached record levels, but the demand for skills still far exceeds the supply of skilled workers. Hiring cybersecurity talent was the number one investment being made by our respondents, but they simply can't match the pace required.

How you can prepare

Increase efficiency so that you can make full use of the cybersecurity staff you already have. This may mean consolidating, automating, and outsourcing various parts of your security and incident response capabilities. You can read more about the MalOp™ and Cybereason's operation-centric approach here:

cybereason.com/platform#malop

3/ Legacy systems increase network vulnerability

What's happening

While most parts of the network are being migrated to the cloud, many critical systems remain offline or in dark networks. These may seem to be less at risk from an attack, but they're also less protected. And their critical nature makes them ideal targets for social engineers, who only need to find the weakest link once to access passwords or gain physical access.

How you can prepare

Don't ignore offline or closed systems. Control access, ensure they are password protected, and teach employees about the dangers of social engineering. Secure these systems by working with a cybersecurity provider who can deploy lightweight, non-intrusive security solutions.

> **When the Sellafield nuclear site hack was discovered, investigators found several weaknesses including that external contractors were able to plug memory sticks into the system while unsupervised.**

4/ Insurance only mitigates a portion of the attack

What's happening

Despite almost all respondents having cyber insurance, only 40% are sure that a ransomware attack would be covered. Only around half of those who claimed from their insurance after an attack recovered the full costs.

How you can prepare

Cyber insurance mitigates a portion of the total impact of an attack, so take the time to fully understand your organization's cyber insurance policy(ies) against the true cost of a breach.

5/ Defenders need help planning for the next attack

What's happening

Despite the high chance of falling victim to another attack, only 41% of organizations are ready for the next attack and the biggest gap is in the planning.

How you can prepare

Focus on what you can control with the resources available to you today. The best way to start is by pressure testing your current incident response plan. Consider working with a cybersecurity partner to conduct a ransomware risk assessment. The assessment should consist of 'tabletop exercises' that simulate a ransomware attack and test the people, process, and technological aspects of your plan. The results will show you how to direct your resources.

6/ It still doesn't pay to pay

What's happening

84% of respondents said their organization paid the ransom. This makes sense of our finding that opening a cryptocurrency wallet is a popular investment. Unfortunately, most of those who paid didn't get their systems and data back uncorrupted. And 78% were held to ransom again, with 63% saying they were asked to pay more the second time around.

How you can prepare

As we have seen for the last two years running, it still does not pay to pay. Prevention is always better than cure. Put a stop to ransomware breaches by partnering with a cybersecurity leader with specific ransomware protection technology. When potential losses are predicted to reach millions of dollars, you can't afford not to protect your business.

Conclusion: It's time to reject the ransom

Once again, we see that paying millions of dollars to ransomware attackers is not always the solution. It doesn't guarantee that you will get all your systems and data back uncorrupted, that your data won't be sold on the black market, or that you won't be attacked again. If anything, this survey shows that once a weakness has been identified, you're likely to be attacked again.

A much better approach to the scourge of ransomware is to make your business invincible to attacks. And you can. But first, you need to help the business understand the true risk and impact of an attack.

Help the business understand the real risk of an attack

You can use the findings of this survey to help your business understand the true risk and cost of a successful breach by ransomware attackers. This should quickly raise the issue to the top of the agenda and help you secure sufficient investment to bolster the organization's security position.

Invest in ransomware talent, planning and technology

The tabletop exercises recommended in the previous section of this report will help you identify the weaknesses in your protection and response planning. We recommend working with cybersecurity provider to cover all your bases, but here are some recommendations on how to get started:

People

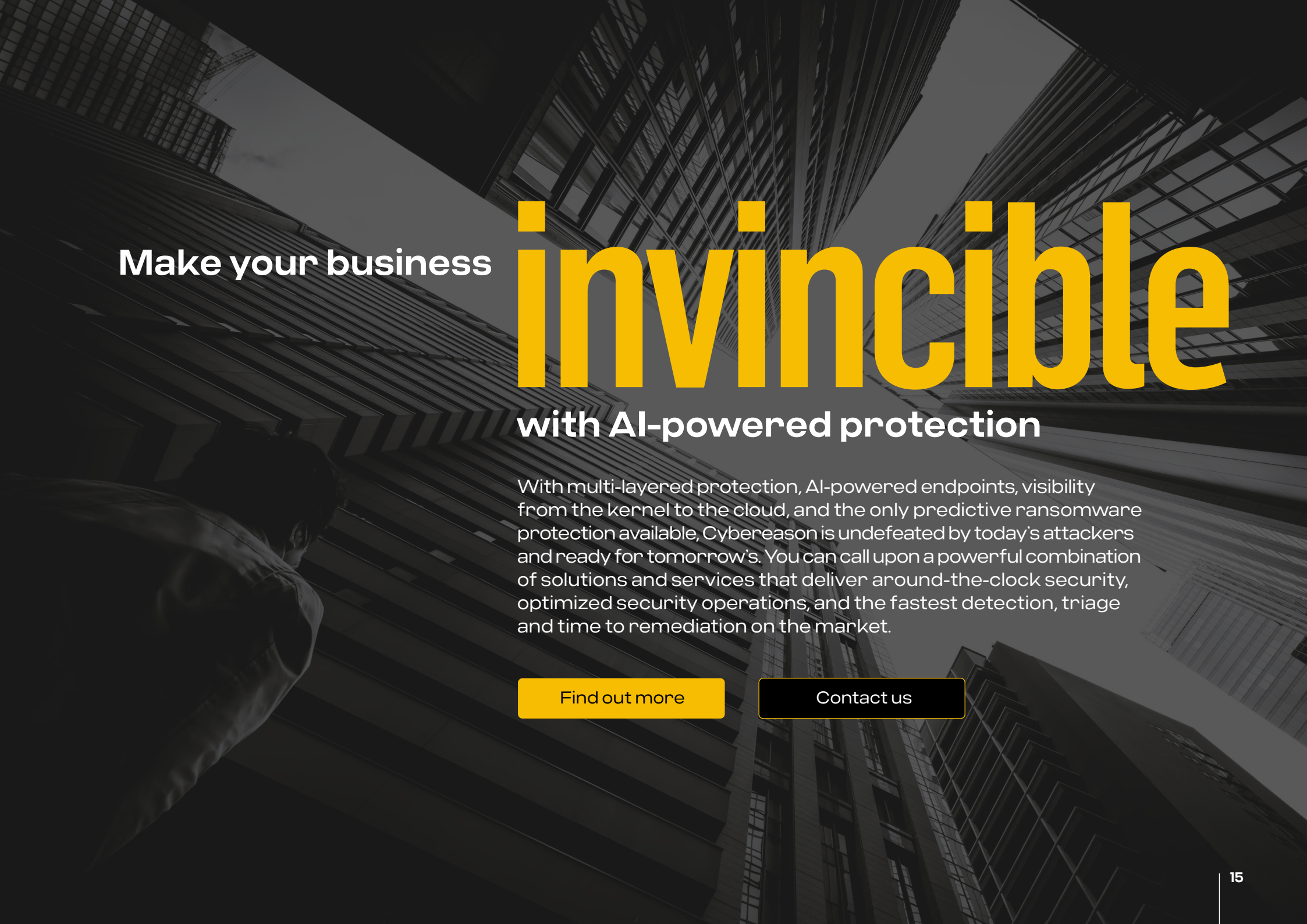
Hire a cybersecurity expert with experience in ransomware protection and empower them to do more with less by automating the protection of your data and systems. Consider outsourcing elements of your security operations to fill any gaps, such as out-of-hours monitoring, or threat detection and response services that can isolate machines automatically in the earliest stages of an attack.

Process

Work with the business to ensure it commits resources to proper planning. Be sure to engage all aspects of the business, including the Board (clarify who is responsible for decision-making and that they are contactable after hours), PR and Marketing (for crisis management and customer communications), etc. Test your plans regularly.

Technology

Turn the tables by investing in the very latest technology. Ensure it covers both online and offline networks. And look for ransomware-specific solutions that protect at every stage of an attack and include a roll-back for any impacted files as a last line of defense. Work with your vendor to deploy managed detection and response services with 24x7x365 monitoring, helping to detect, halt and even remediate attacks within moments, no matter when they occur.



Make your business invincible

with AI-powered protection

With multi-layered protection, AI-powered endpoints, visibility from the kernel to the cloud, and the only predictive ransomware protection available, Cybereason is undefeated by today's attackers and ready for tomorrow's. You can call upon a powerful combination of solutions and services that deliver around-the-clock security, optimized security operations, and the fastest detection, triage and time to remediation on the market.

Find out more

Contact us

About Cybereason

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud, and across the entire enterprise ecosystem. Only the AI-driven Cybereason Defense Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in La Jolla, California with customers in more than 40 countries.

Cybereason's Ransomware Protection Capabilities

Cybereason brings unique capabilities to our customers, ensuring they remain undefeated against ransomware. Our unique combination of nine layers of endpoint prevention (EPP), with Cybereason Endpoint Detection (EDR) integrated technologies and our Managed Detection and Response (MDR) service combine to form a complete ransomware protection solution that protects our customers across every stage of the most advanced ransomware attacks.

The outcome: Customers are protected. One minute to detect, five minutes to triage and 30 minutes to remediate attack. All day, all week, all year—including out of hours and over the weekends (when attackers prefer to strike).

Survey methodology

This research was conducted by Censuswide on behalf of Cybereason. A total of 1,008 cybersecurity professionals from organizations with 500 or more employees took part in the online survey between September 25th and October 6th 2023. Participants are from the United States, United Kingdom, France and Germany. The survey sample includes responses from a variety of industries. IT and Telecommunications had the highest representation at 31%, followed by Manufacturing and Utilities (13%) and Retail, Catering and Leisure (10%). Other industries include Architecture, Engineering and Building, Art and Culture, Education, Healthcare, Legal, Transportation, and more. Only organizations with at least 500 employees were surveyed. Those with 500-999 employees made up 87% of the group and those with more than 1000 employees made up the remaining 13%.

cybereason©