

# 2024 Ransomware Risk Report

Essential guidance for building operational resilience against cyberattacks

Semperis experts weigh in on results from a ransomware survey of 900 IT and security leaders



"We must assume an ever-present state of threat...You cannot keep ransomware off the field. It's like trying to fence a field to keep off water. The water is an ever-present and resourceful foe."

**Chris Inglis**

Strategic Advisor, Semperis  
First US National Cyber Director

# Executive Summary

**Ransomware, once a sporadic menace, has evolved into an unrelenting adversary. Attacks are no longer isolated incidents; they occur incessantly.**

Criminal groups orchestrate multiple strikes in rapid succession, exploiting vulnerabilities across organizations. Ransomware infiltrates diverse sectors – healthcare, IT/telecom, education, utilities, and more – leaving chaos in its wake. Critical systems, including Microsoft Active Directory, have become a top attack target.

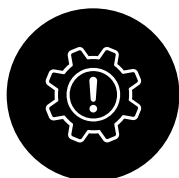
Semperis partnered with international research firm Censuswide to conduct a comprehensive study, spanning **multiple industries** across the **United States, the United Kingdom, France, and Germany**, to examine the alarming trends in ransomware's frequency, severity, and consequences. The **2024 Ransomware Risk Report** reveals concerning statistics for business, IT, and security leaders.

## Attacks are frequent and continuous



Organizations must recalibrate their defenses to embrace an “assume constant breach” stance. The *2024 Ransomware Risk Report* reveals that **74% of victims were attacked not once, but multiple times**. Certain countries and industries were more likely to experience subsequent attacks. But overall, more than half the companies we surveyed were successfully breached two or more times – sometimes within the same day.

## Business disruption is widespread and pervasive



We found evidence of widespread business damages resulting from ransomware attacks: **87% of attacks caused some level of disruption**. This might not seem surprising. However, we discovered that disruption – including data loss and the need to take all systems offline – occurred even though organizations had general disaster recovery and backup systems in place. And the domino effect is stark: revenue loss, layoffs, reputational damage, and business closures.

## Most companies feel compelled to pay ransom



The majority of companies – **78%** – that suffered a ransomware attack paid **ransom**. Moreover, **32% paid 4 times or more** during the past 12 months. With about **10% of companies paying in excess of \$600K in ransom** alone, the costs of ransomware are clearly skyrocketing.

## Organizations lack Active Directory-specific backup and recovery systems



In Semperis' experience helping some of the world's largest organizations defend their identity systems, the clearest path to fighting back against ransomware is the ability not just to defend the environment but also to rapidly detect, stop, and recover from breaches. At the heart of these capabilities are identity systems like Active Directory, a Tier 0 service that manages access to nearly all users, groups, applications, and resources and is a top target for attackers.

The good news is that nearly 70% of respondents said they had an identity recovery plan. Unfortunately, a plan alone isn't enough. **Only 27% maintained dedicated systems for recovering Active Directory**, Entra ID, and identity controls – the Tier 0 infrastructure that all systems depend on for recovery. Organizations must fortify their identity threat detection and response (ITDR) stance by building resiliency through automated recovery systems, safeguarding their ability to conduct business.

## Operational resilience is a strategic imperative



Ransomware transforms business landscapes, leaving scars that linger. Businesses evaluating investments in critical cybersecurity solutions and planning must weigh not just the price of ransom but the costs of near-term recovery efforts and long-term consequences.

IT and security teams must communicate the true risk of ransomware to business leaders to **gain Board support for cybersecurity efforts – a top concern for study participants**. This report reveals why Board-level commitment is essential: Cybersecurity is no longer simply an IT concern but a strategic imperative.

## CONTRIBUTING EXPERTS



**Mickey Bresman**

Semperis CEO



**Sean Deuby**

Semperis Principal  
Technologist  
(North America)



**Guido Grillenmeier**

Semperis Principal  
Technologist (EMEA)



**Simon Hodgkinson**

Semperis Strategic  
Advisor, former  
bp CISO



**Chris Inglis**

Semperis Strategic  
Advisor, former  
US National Cyber  
Director



**Marty Momdjian**

Semperis Executive  
VP of Services



**Jeff Wichman**

Semperis Director  
of Incident  
Response

# TABLE OF Contents

- 1 ..... **The Key to Operational Resilience:**  
Coming to Terms with the Never-Ending Breach
- 2 ..... **Key Findings**
- 3 ..... Assume **Constant Breach**
- 5 ..... Traditional Defenses **Fail to Protect**  
Business Operations
- 7 ..... Can Companies **Say “No” to Ransomware?**
- 11 ..... The **True Cost of Ransomware**  
Extends Beyond Payments
- 14 ..... **Prioritizing Resilience:**  
Identity Threat Detection and Response
- 16 ..... Future **Challenges and Next Steps**

# The Key to Operational Resilience: Coming to Terms with the Never-Ending Breach

In-the-trenches IT and security teams disclose serious cyberattack consequences that go under-reported and unacknowledged by business leaders.

Enterprise leaders across industries and around the globe recognize ransomware as a critical threat. However, many still underestimate the full scope of its damage.

Reports of high-profile ransomware attacks are now a media staple. Yet our survey reveals that the frequency with which companies are successfully attacked – not once per year, but multiple times within the same year – is not widely acknowledged. Neither are the long-term impacts, including closures, layoffs, collateral loss of revenue, and cancellation of insurance.

As a result, security, technology, and business leaders can miscalculate the true cost of ransomware, leaving them unequipped to build decisive operational resilience in response to never-ending attacks.

At Semperis, our mission is to be a force for good. As part of this mission, our Breach Preparedness and Response team has seen first-hand the devastating effects of ransomware and the ways in which attackers exploit organizations' identity systems – Microsoft Active Directory in most cases – to gain leverage, disrupt business, and plant persistent footholds.

To provide a clearer understanding of the prevalence, mechanism, and implications of ransomware attacks, Semperis conducted a detailed study of 900 IT and

“Paying ransom is not doing anyone any good. The cost of what you pay to a ransomware group is not where the damage will end. And certain attacks aren't money-driven; rather they aim to cause chaos and disruption.”

**Mickey Bresman**  
CEO, Semperis

security professionals from global organizations across the United States, the United Kingdom, France, and Germany. We surveyed enterprises across multiple industries, including education, finance, healthcare, manufacturing and utilities, IT and telecommunications, and travel and transportation. This report summarizes our study responses, collected in the first half of 2024, and provides expert insights into the implications of ransomware attacks for global enterprise IT, security, and risk-management professionals.

**We encourage you to share this information with your IT and security teams. Most important, share these findings with your organization's business leadership – and build alignment around the actions your organization must take to ensure operational resilience in the face of ransomware's never-ending threat.**

**Companies are suffering successful ransomware attacks multiple times within the same year – resulting in closures, layoffs, loss of revenue and customer trust, and cancelation of cyber insurance.**

# Key Findings

Attacks are pervasive, successful – and lucrative.

Ransomware attacks aren't a one-time threat.

**74%** of respondents that were victimized by ransomware within the past 12 months were **attacked multiple times**, many **within the span of a week**.

Companies are not prepared to beat ransomware.

**78%** of targeted organizations paid the ransom – **72% paid multiple times**. A whopping **32% paid a ransom 4 times or more**; in Germany, this figure rose to **nearly 50%**.

Few companies see an alternative to payment.

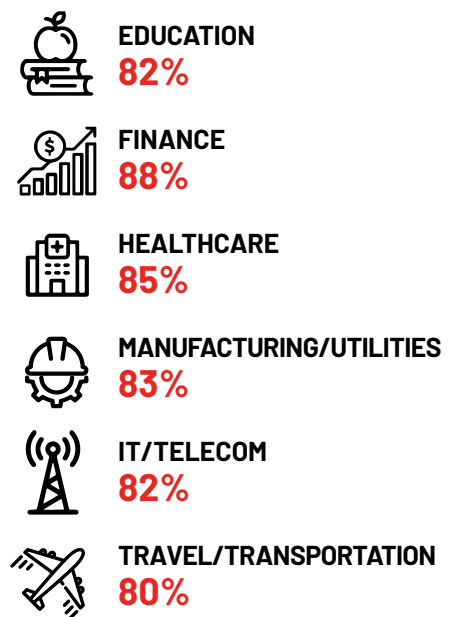
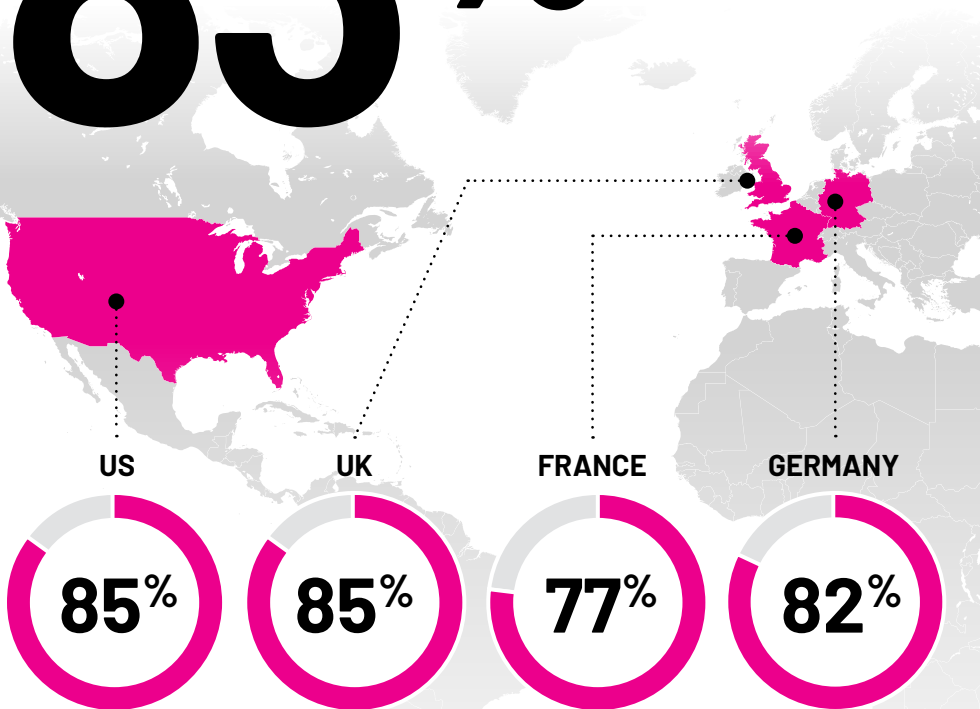
**87%** of attacks **disrupted the business**. And for 16% of those who paid ransom, recovering their systems was a **matter of life or death**.

Paying attackers does not solve the larger problem.

**35%** of organizations that paid ransom **failed to receive decryption keys** or were unable to recover their files and assets. In addition, many suffered long-term collateral damage even if they paid.

# 83%

of responding organizations were targeted by ransomware in the **past 12 months**



# Assume Constant Breach

Companies must expand their “assume breach” mindset to prepare for multiple and even simultaneous attacks.

Ransomware is not a new challenge, but it is an increasingly sophisticated one. Today, bad actors share information across vast criminal networks. They purchase ready-made ransomware-as-a-service (RaaS) kits. They use regulatory fines as leverage. They attack sectors that were once considered off limits. Their criminal ingenuity seems to know no bounds.

Ransomware is highly coordinated, strategically timed, and deeply embedded throughout your systems before being executed. Breaches of identity systems like Microsoft Active Directory give multiple attackers access to multiple operational systems – so they can execute multiple strikes.

The “assume breach” mindset has been much discussed recently. Our study uncovers a new prerequisite to resilience: **assume constant breach**. Organizations must be on continual alert, always ready for the success of not one, but multiple breaches.

Organizations must understand that cybersecurity has moved beyond a binary, “secure or not secure” approach, says Semperis Strategic Advisor Chris Inglis, former US National Cyber Director and former Deputy Director of the NSA.

“Cyber threats are persistent: always on the field, always in play,” says Inglis. “The cost of entry for attackers is too low, the potential rewards too high. You cannot keep ransomware off the field. It’s like trying to fence a field to keep off water. The water is an ever-present and resourceful foe.”

“When multiple attacks happen, they tend to happen in quick succession. These data points suggest that multiple criminal gangs are leveraging organizations’ vulnerabilities to detonate a second or third malicious attack – in some cases, simultaneously.”

**Simon Hodgkinson**

Strategic Advisor, Semperis  
Former bp CISO



“We must assume an ever-present state of threat. This is not just the notorious cases that we hear about every quarter or so. This is happening all day, every day, to a range of companies.”

Chris Inglis

## KEY TAKEAWAYS



**Initial attacks** were most likely to succeed in **France**; **subsequent attacks** were most successful in **Germany**.

**Initial attacks** were most successful in the **education** and **healthcare** sectors; **subsequent attacks** were most likely to succeed in the **IT/telecom** and **travel/transportation** industries.

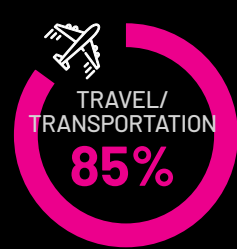
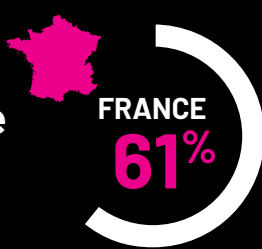
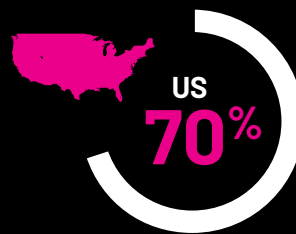


Most companies that saw multiple attacks experienced **secondary attacks** within the **span of a week**. **Healthcare organizations** were more likely to suffer **multiple simultaneous attacks**.

## BY THE NUMBERS

# 74%

of organizations that were attacked were targeted more than once



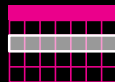
Of organizations that were attacked multiple times:



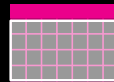
**26%**  
were attacked **simultaneously**



**28%**  
were attacked the **same day**



**37%**  
were attacked the **same week**



**8%**  
were attacked the **same month**

**35%**  
of healthcare organizations were attacked **simultaneously**



# Traditional Defenses Fail to Protect Business Operations


Business disruption is pervasive and widespread, even for organizations that have general backups in place.

The high-profile Colonial Pipeline attack in May 2021 still stands out as one of the top critical infrastructure attacks. The attack marked the escalation of a wider trend targeting critical industries. Attackers have become emboldened to conduct strikes that will cause the maximum amount of disruption by interrupting daily life or endangering public health and safety – surefire ways to secure hefty ransom payments.

Since then, we've seen widespread disruption caused by attacks on healthcare (Change Healthcare and Ascension Health in 2024), IT/telecom (Frontier Communications in 2024), and education (Los Angeles Unified School District and Minneapolis Public School District in 2023).

The industries included in our survey rely on a hybrid IT infrastructure and a range of devices. Their networks serve users working on external laptops and mobile devices as well as on premises. And many incorporate IoT devices and SCADA systems that run technologies such as life-saving equipment in hospitals, manufacturing equipment on shop floors, or pipeline monitoring devices in the field.


These wide-ranging systems create a broad attack surface that offers entry through embedded operating systems, outdated technology that hasn't had regular security updates, and long-forgotten backdoors. Critical infrastructure – such as identity systems like Active Directory and Entra ID – are primary targets that enable lateral movement, privilege escalation, data exfiltration, and ransom of the entire network.



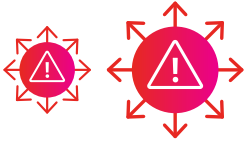
“Overall, complexity is rising, and you can only do so much in a day. Cloud computing has not lessened the burden or reduced operational complexity. You have to assume that malicious activity is happening in your network, and you need the ability to find and undo it.”

**Guido Grillenmeier**

Principal Technologist (EMEA), Semperis



## KEY TAKEAWAYS



Most ransomware attacks were **successful** in causing **widespread business and data disruption.**

Critical infrastructure and services – such as **healthcare, utilities, communications,** and **transportation** – continue to be **prime targets.**



## BY THE NUMBERS

**87%**

of attacks caused business disruption, even for those that paid ransom



**37%**

suffered data loss



**33%**

had to take all systems offline

**25%**

EDUCATION

**27%**

**43%**

FINANCE

**34%**

**40%**

HEALTHCARE

**29%**

**42%**

MANUFACTURING/  
UTILITIES

**30%**

**42%**

IT/TELECOM

**40%**

**27%**

TRAVEL/  
TRANSPORTATION

**24%**

# Can Companies Say “No” to Ransomware?


Despite widespread adoption of cybersecurity and disaster recovery planning, many companies are paying multiple ransoms per year.

According to our survey, most respondents maintained some form of backup, including “tamper-proof” security-based backups and general-purpose data protection systems. Yet 78% of companies that suffered a ransomware attack paid the ransom rather than refuse and attempt recovery.

Our study reveals a flaw in many cybersecurity models:

Only about one-quarter of respondents maintained dedicated, Active Directory-specific backup systems. As Gartner has noted, adding a dedicated tool for backup and recovery of Active Directory accelerates and simplifies recovery from cyberattacks.<sup>1</sup> Without an AD-specific recovery plan and the tools to implement it, organizations are at risk of revenue losses, downtime, reputational damage, and litigation while they scramble to recover the Tier 0 infrastructure that users and applications depend on and restore access to the services that power their business operations.

Without the ability to rapidly recover their identity systems – and thus, their business operations – companies might feel they have little choice other than to pay their attackers. Many respondents



“Once you understand how your recovery will play out in real time, you can rework and validate your recovery plan until you have an accurate picture of the required effort. Then you can present that information to your Board with confidence. Without that confidence, you put your leaders in a position where it’s very hard to avoid paying ransom. But with accurate recovery information – you give them the power to say no to attackers.”

**Mickey Bresman**

noted a desire to return to normal business as quickly as possible as a reason for paying ransom. Others, especially those in the IT/telecom industry, paid because they had cyber insurance to defray the costs. Still others considered the threat to patients, customers, their business, or their reputation to be worth the price of ransom.

Unfortunately, our experts note that this reasoning is likely to increase, rather than decrease, the likelihood of future attacks.

“There is some degree of confidence on the part of ransomware negotiators that if you deal in good faith with the attacker, they have an incentive to deliver what they promised,” explains Chris Inglis. “But proving to be a ‘successful’ victim is a dangerous thing.” ▶

<sup>1</sup> Simpson, Nik. “How to Protect Backup Systems from Ransomware Attacks.” Gartner Research. Sept. 21, 2021. <https://www.gartner.com/en/documents/4005993>.

## CAN COMPANIES SAY “NO” TO RANSOMWARE?

“Ransomware attacks today are often the sum of activities by a loose confederation of groups,” Inglis says. “You’re going to need to negotiate with more than one of them to find your way out of it. Any company that thinks, ‘I’ll just pay my way out,’ is setting themselves up for a harder ride than they might have imagined.”

Jeff Wichman, Semperis Director of Incident Response, agrees. Wichman leads the company’s Breach Preparedness and Response team, helping scores of organizations around the world recover their systems and protect their business against the onslaught of aggressive cyberattacks.

“No organization can pay their way out of ransomware,” he says. “There are no ‘good’ criminals. Nearly every time, the hackers are at an advantage because the victims are either trying to prevent the release of sensitive data or regain access to their systems. Yet there are countless examples of companies paying ransoms only to have the hackers release the data anyway. Organizations are better served putting the money into the security of their infrastructure and applying the least amount of privilege needed to work.”



“All companies are at risk of multiple ransom demands. The first ransom might be to regain access to your systems; another – or multiple others – might be to prevent your data from being leaked. Regardless, everything relates to the identity systems – the core of access. Once an attacker gets Tier 0 access, you have limited time to protect your remaining infrastructure.”

**Jeff Wichman**

Director of Incident Response, Semperis

Effective ITDR includes both **dedicated, identity-specific backup systems** and a **tested identity recovery plan** that includes cyber-specific use cases.

# CAN COMPANIES SAY "NO" TO RANSOMWARE?

## KEY TAKEAWAYS



Finance saw the **biggest risk to its business.**

However, this sector **paid fewer ransoms** overall.

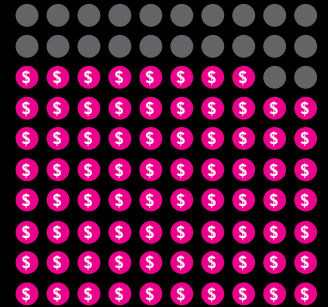
Jeff Wichman notes that this is likely due to the industry's **wealth of controls** and **regulatory oversight** to protect both customer information and money. The finance industry also **benefits from FS-ISAC**, the not-for-profit organization established for **protection and threat-intelligence sharing.**



For **healthcare**, paying ransom was most often seen as a matter of **life or death.**

## BY THE NUMBERS

# 78%



of companies that were attacked paid ransom



**72%** paid ransom multiple times

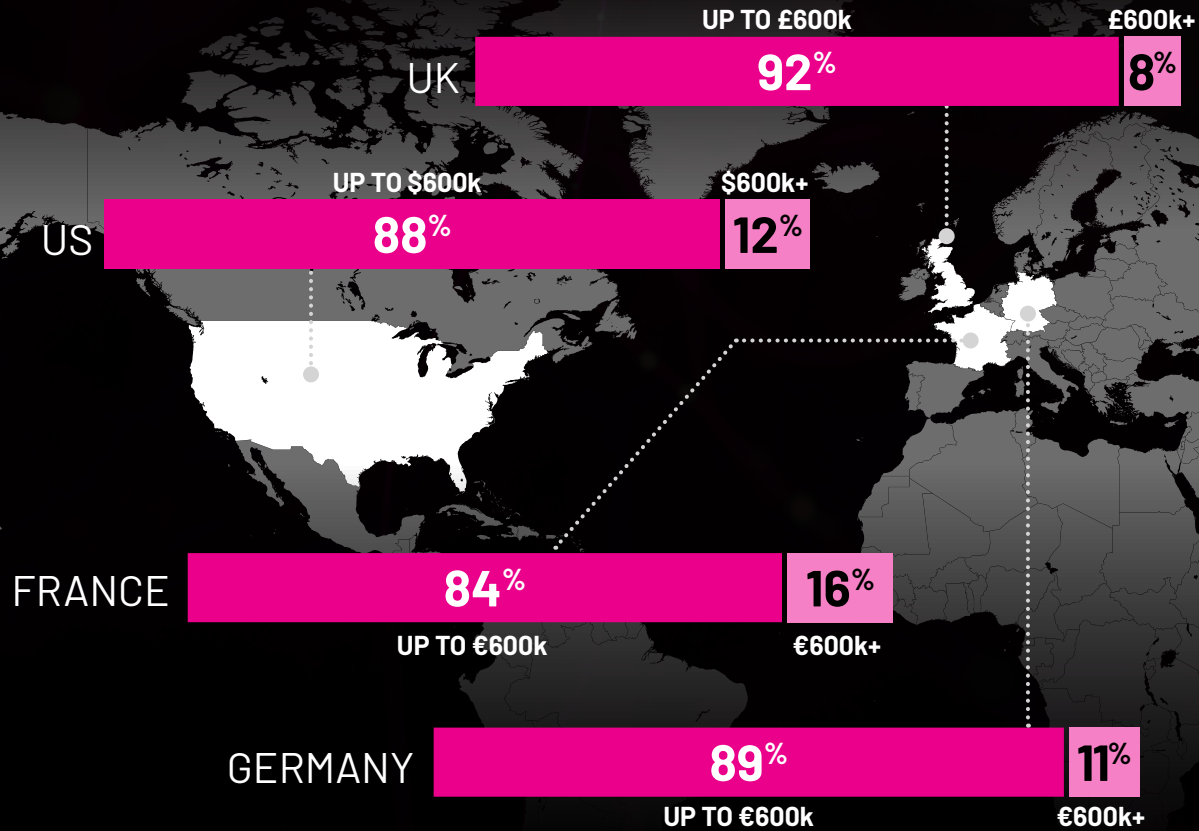


**32%** paid four times or more

	PAID MULTIPLE TIMES	PAID 4+ TIMES
US	70%	21%
UK	73%	38%
FRANCE	80%	36%
GERMANY	66%	49%
EDUCATION	79%	27%
FINANCE	68%	20%
HEALTHCARE	76%	39%
MANUFACTURING/UTILITIES	67%	25%
IT/TELECOM	74%	25%
TRAVEL/TRANSPORTATION	74%	50%

BY THE NUMBERS *CONTINUED*

How much ransom did companies pay, on average?



Why did companies pay?



Threat to business, customers, or reputation



Access to cyber insurance



Attempt to return to normal business as quickly as possible



Matter of life or death

# The True Cost of Ransomware Extends Beyond Payments

Risk analysis must consider long-term damage to the business, consumers, and the workforce.

**“Ransomware attacks are life-changing events that have enduring effects across every dimension of the business.”**

**Chris Inglis**

In any complex organization, security budget, staffing, and resource decisions are a balancing act. Executives weigh the costs against the potential losses. However, in the case of ransomware, executive leadership might be making those decisions without a complete understanding of the potential costs after an attack.

Ransom payment does not guarantee the receipt of usable decryption keys. Furthermore, attackers often use ransomware to deliver malware that can reinfect systems or cause other damage.

“The cost of the ransom payment is not the sum total of the actual damage,” notes Semperis CEO Mickey Bresman. “Certain attacks aren’t money-driven; rather they are aimed at causing chaos and disruption. In addition, the money that you pay is being used for other criminal activities, like human trafficking, drugs, and weapons.”

Ransomware attacks also have ripple effects across the organization. This “collateral damage” means that a successful attack typically costs much more than a ransom payment.

“The threat of a business closing permanently does exist,” says Marty Momdjian, Semperis Executive VP of Services. “I’ve seen it happen in real time – sometimes just a couple of months after a breach – because of the loss of revenue and financial burden of mitigation. So how do companies try to prevent that? In my experience, layoffs always occur six months to a year after the attack.”

“This is not a one-time event or time-limited event that you can quickly address and then move on from,” notes Chris Inglis. “This is a life-changing event that has enduring, lingering effects. Loss of customer trust, loss of cyber insurance, regulatory prosecution ... that scrutiny never goes away.”

# THE TRUE COST OF RANSOMWARE EXTENDS BEYOND PAYMENTS

## KEY TAKEAWAYS



Paying ransom offered **no guarantee** that decryption keys **would be received** or **work even if delivered**. Furthermore, our experience shows that many attacks also **insert malware or backdoors** to future attacks.

Organizations in **Germany** and in **education, healthcare, and manufacturing/utilities** were most likely to suffer **business disruptions** due to offline systems.



Companies in the **UK** and **France**, as well as those in the **finance** industry, suffered the **greatest brand damage**.



Many **travel/transportation** organizations were hit with **lawsuits**.

**IT/telecom** companies most often had to **close up shop** – temporarily or permanently.



**US** businesses received the most **regulatory fines**.

## BY THE NUMBERS

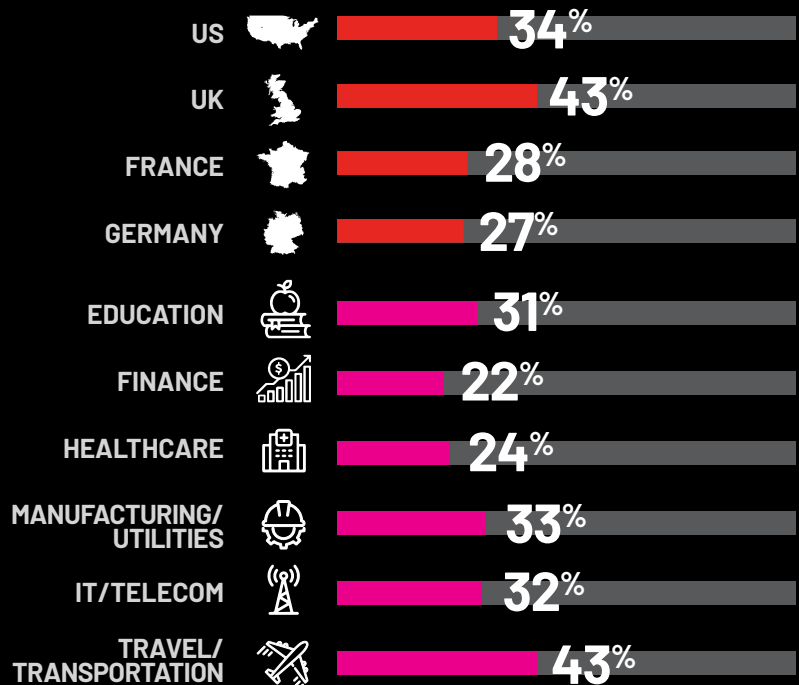
Despite meeting attackers' ransom demands,

# 35%

of companies that paid either **didn't receive decryption keys** or **received corrupted keys**.

BY COUNTRY

BY INDUSTRY





In any event, ransomware costs more than the ransom.

## Organizations must also consider the **collateral damage** that attacks cause.



“The threat of a business closing permanently does exist. I’ve seen it happen in real time –sometimes just a couple of months after a breach – because of the loss of revenue and financial burden of mitigation.”

**Marty Momdjian**  
Executive VP of  
Services, Semperis



Business disruption



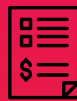
Temporary or permanent closings



Brand damage



Loss of revenue or customers



Fines or lawsuits



Layoffs and resignations



Cyber insurance cancellation or price increase

# Prioritizing Resilience: Identity Threat Detection and Response

Identity is the new security perimeter, yet few companies maintain dedicated identity protection.

The digitization of the modern enterprise has eliminated the idea of a defensible perimeter, creating a complex landscape for security professionals – and a broad attack surface for cyber criminals.

Attackers are adept at quickly sizing up an organization's technology ecosystem and nimbly navigating across entry points, from mobile devices to IoT devices, remote data centers to on-premises servers, local desktops to hybrid and multi-cloud environments.

This digital complexity makes it imperative to secure your identity system – the heart of every process in your network. Jeff Wichman notes that when it comes to ransomware, "everything relates to the core of access. Once an attacker gets Tier 0 access, you have limited time to protect the remaining infrastructure."

Marty Momdjian sees the survey data as "a wake-up call for organizations to shine a spotlight on their identity systems. In previous years, the focus has been on removing friction for users. Today, organizations are realizing that overprovisioned access invites attackers in."

Mickey Bresman explains why the identity system, particularly Active Directory, is now the security perimeter for enterprise organizations. "Every minute that the identity system is down is extremely painful. I chatted

with a customer who tested their Active Directory recovery plan with the systems that they had in place. They concluded that mitigation of an attack would take them seven days. That's not acceptable, because it means that everything else in the organization will be down for seven days as well."

Chris Inglis sees identity as the core issue for successfully resisting ransomware demands. "At the center of this whole discussion is business viability: the ability of the company to achieve its aspirations and its commitments on behalf of its shareholders and customers," he explains. "Attackers are trying to hold that at risk so that they can then convince you to buy them out. If they can achieve a successful attack on identity, then they own privilege, and they can then use that privilege to their benefit."

**"It's not surprising to me that the majority of ransomware targets the identity system. If an attacker wants to create the maximum impact to extort money, they want to take control of your environment – and they will absolutely want to own Active Directory. Once Active Directory is compromised, the threat actors hold the keys to your kingdom."**

**Simon Hodgkinson**



## KEY TAKEAWAYS



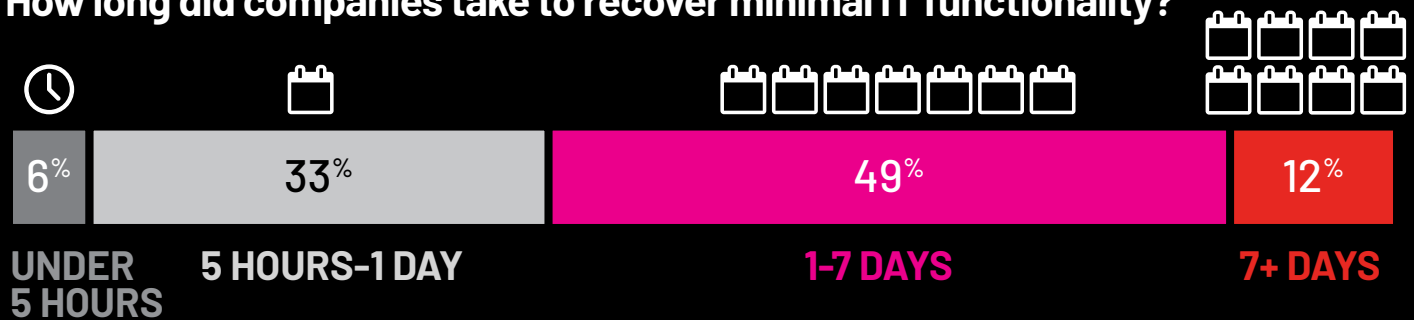
61% of ransomware victims required **more than a day** to recover **minimal IT functionality**, extending business disruptions.

**Healthcare** and **travel/transportation** – the two industries most-often attacked 4 times or more – reported the **lowest adoption** of **dedicated, AD-specific backup systems**.



## BY THE NUMBERS

How long did companies take to recover minimal IT functionality?

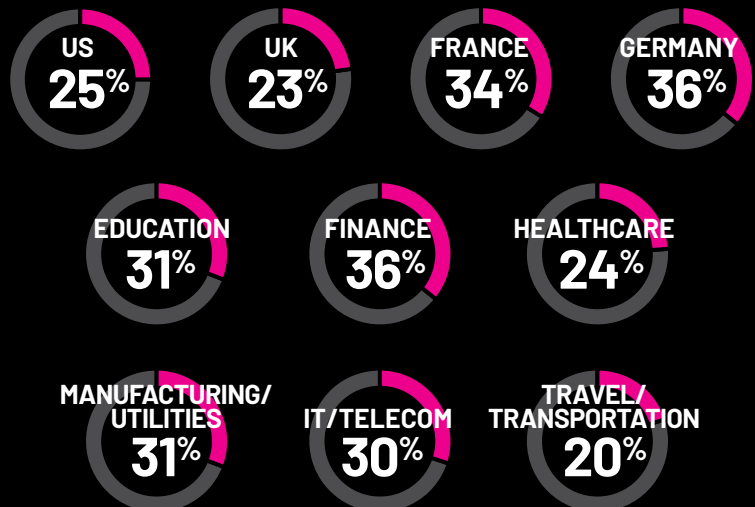


Although 70% of respondents say they had an identity recovery plan in place, only

# 27%

of respondents reported **dedicated, AD-specific backup** systems.

WHO HAD DEDICATED, AD-SPECIFIC BACKUP SYSTEMS?



# Future Challenges and Next Steps

What are organizations worried about in the months ahead?  
Our experts offer insights and actions to improve cyber and business defense.

We asked survey respondents about their biggest challenges in the year ahead. You might expect budget woes to be the top concern for most organizations. In reality, most respondents reported that their biggest hurdle to resilience was lack of support from their Board of Directors.

This news didn't surprise Chris Inglis. He notes that effective cybersecurity requires a three-pronged approach comprising corporate doctrine, skill building, and technology.

"Technology can help us analyze and assess what's happening, moment by moment," Inglis says. "It can help us respond more quickly and recover more quickly. But the thing that is most wanting now is a collective realization that we all have a part to play. That starts with the Board, not with the IT shop. The Board is accountable; the SEC has made that clear. Regulations are increasingly making it clear: cybersecurity is a business issue."

So, what can organizations do to meet these challenges and ward off future ransomware demands? Explaining the value of identity-first security, in business terms, is a good first step.

"Identity is the new perimeter," says Inglis. "It's the mechanism by which attackers can hold your core asset. You have your company's liability at risk, so you must defend it. When you focus on identity, you have a much clearer window into how the life forces within your systems are operating. And when you find anomalies in those life forces, you can track those back not just to the outsider who is trying to reach across that boundary, but to anything that can manipulate privilege."

Mickey Bresman says that the goal of identity recovery and resilience plans is the ability to say "no" to attackers.

"Make sure that you have a choice in your response to a ransom situation," he advises. "Put a backup and disaster recovery plan in place — and not just on paper. **Be absolutely sure that you have tested it.** Know what your response will look like if systems go down and ensure that you fully understand how long recovery is going to take. Understand the sequence and the dependencies between the systems, because you cannot recover your database server until your identity system is up and running."

"People tend to put their resources and effort into endpoint protection. But threat actors will get past the endpoint. And once they're inside the network, they go through the whole identity system. What defense do you have when that happens? Because once they own your identity system, they have all the power. If your identity system goes down, none of your other solutions will work."

**Sean Deuby**

Principal Technologist (North America), Semperis



# KEY TAKEAWAYS



Most respondents reported that their **biggest hurdle to resilience** was **lack of Board support.**



A **detailed, tested identity resilience plan** can empower organizations to **say "no" to ransomware** demands.

"Considering that there is a 24/7 threat arrayed against today's organizations, you can never say 'I am safe' or take a moment off. The best you can do is to make your environment defensible and then defend it. That defense is a mix of doctrine, skilling, and technology, all of which are essential. That's where layered defense comes in."


Chris Inglis

After facing a never-ending onslaught of ransomware attacks, what are the **biggest challenges** to organizations moving forward?

  
**Budget**  
constraints

  
**Staffing**  
shortages

  
Lack of  
**Board-level**  
**support**

  
**Outdated**  
**or legacy**  
systems

  
Cybersecurity  
**regulations** and  
**directives**

## What is your #1 concern?



**US**  
Board support



**UK**  
Staffing



**EDUCATION**  
Board support



**FINANCE**  
Board support



**HEALTHCARE**  
Board support



**FRANCE**  
Budget



**GERMANY**  
Outdated/  
legacy systems



**MANUFACTURING/  
UTILITIES**  
Staffing



**IT/TELECOM**  
Budget



**TRAVEL/  
TRANSPORTATION**  
Regulations

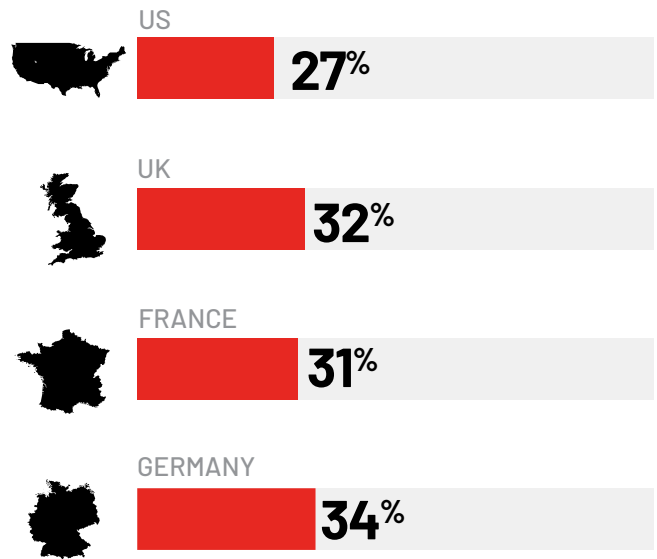
# FUTURE CHALLENGES & NEXT STEPS

Surprisingly, despite the damage that ransomware has inflicted,

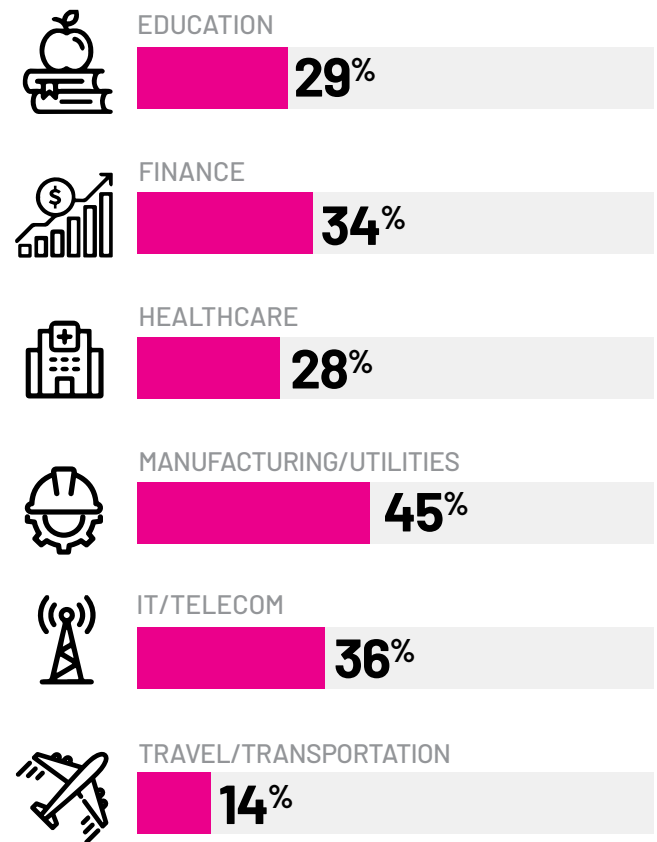
**ONLY  
30%**

of responding organizations plan to increase their security budgets in the next year.

## BY COUNTRY



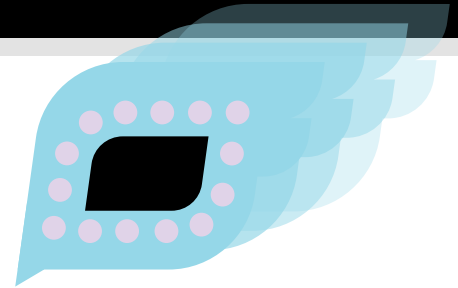
## BY INDUSTRY



# Level up Your Identity Security Skills at HIP Conf 24

## 5 reasons you need to attend HIP Conf 24

84% of organizations experienced an identity-related breach in the last year, and with the average cost of a breach north of \$4 million, identity security skills are more valuable than ever. The Hybrid Identity Protection Conference (HIP Conf) is the premier educational forum for identity-centric cyber defenders to meet, share knowledge, and win together.



**1**

### Get expert security tips for hybrid AD—the #1 new target for threat actors.

Meet the world's foremost Active Directory, Entra ID, and Okta security experts at HIP Conference. Learn how to defend your identity systems at every step in the cyber kill chain, from posture assessments to post-breach forensics and recovery.

**2**

### Acquire new skills to help improve your company's cyber resilience.

With 9 out of 10 attacks exploiting AD, identity security expertise is in high demand. After all, cyber risk is business risk. You'll walk away from HIP Conf with new skills to improve identity-driven cyber resilience and dramatically reduce risk from operational errors and cyberattacks.

**3**

### Join us for knowledge-sharing and technical training with no sales pitches.

Are you sick of attending cyber conferences only to be sold to? HIP Conf is different as we have strict rules against vendor sales pitches. As an attendee, you'll enjoy practical, expert-led context to help you be successful in your day-to-day role.

**4**

### Network with your peers charged with defending hybrid identity environments.

Get to know your peers working at the intersection of identity and security through hands-on workshops, networking sessions, and group activities in NOLA. Share your own experiences and make lasting connections.

**5**

### Hear real-world incident response success stories and lessons learned from the field.

The HIP community ranges in cyber disciplines, including incident response experts with unrivaled experience protecting the world's most sensitive hybrid identity environments. Learn how front-line responders deal with complex identity breaches, ransomware, and other destructive attacks.



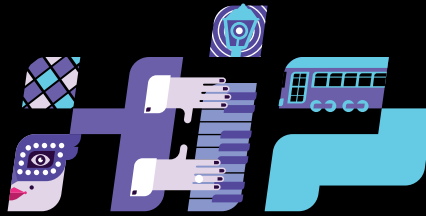
### **BONUS: Visit "The Big Easy" New Orleans.**

Okay, here's a bonus reason to attend HIP Conf: Visit vibrant New Orleans, a city with a rhythm, style, and attitude all its own. Take in the jazz, the local food and drink, and freewheeling fun! The conference schedule allows plenty of time for you to create your own NOLA adventure.

**ISC2**

## Earn CPE credits through ISC2!

Each keynote and technical session at HIP Conf 24 is eligible for 1 CPE credit. You'll earn up to **10 CPE credits** over the two days.



HYBRID  
IDENTITY  
PROTECTION

conf24

## NEW ORLEANS

MARDI GRAS WORLD, NOVEMBER 13-14, 2024



"At the center of this whole discussion is business viability: the ability of the company to achieve its aspirations and its commitments on behalf of its shareholders and customers. Attackers are trying to hold that at risk so that they can then convince you to buy them out. If they can achieve a successful attack on identity, then they own privilege, and they can then use that privilege to their benefit."



**Chris Inglis**  
Semperis Strategic  
Advisor & First US  
National Cyber Director



"I'm excited to be able to join HIP again this year. Organizations are facing an increasing skills gap between what's needed to implement, secure, and support their digital transformation to the cloud, and what's needed to support the technical debt of their existing on-premises environment. In the face of these attacks, the HIP conference is focused on building practical identity security skills where it matters most - in hybrid environments - so we can be prepared for these attacks."



**Alex Weinert**  
VP Director of Identity  
Security at Microsoft



"If there's something that you're curious about especially in the hybrid identity world, there's someone at the HIP events that has something to say about it."



**Sean Metcalf**  
CTO at Trimarc Security

### HIP CONF BRINGS TOGETHER THE WORLD'S FOREMOST CYBERSECURITY EXPERTS



**NITIKA GUPTA**  
GROUP PRODUCT  
MANAGER, MICROSOFT



**ERIC WOODRUFF**  
SR. CLOUD SECURITY  
ARCHITECT, SEMPERIS



**PAM DINGLE**  
DIRECTOR OF IDENTITY  
STANDARDS, MICROSOFT



**HENRIQUE TEIXEIRA**  
SVP, STRATEGY,  
SAVIYNT



**CHASE CUNNINGHAM**  
VP, SECURITY MARKET  
RESEARCH, G2



**BEN CAUWEL**  
VP, SECURITY MARKET  
RESEARCH, G2



**NESTORI SYYNIMAA**  
PRINCIPAL IDENTITY SECURITY  
RESEARCHER, MICROSOFT

For the full speaker line-up visit the HIP Conf website

The focus of HIP Conf 24 is Gartner's "top trending" category of Identity Threat Detection and Response (ITDR), a discipline that includes tools and best practices to protect the identity infrastructure from attacks. Enterprise identity infrastructure is in cyberattackers' crosshairs because enterprises rely on AD and other identity systems to manage user accounts and control access to corporate resources.

Tickets available now:



Hosted by semperis

Participating partner





## METHODOLOGY

In the first half of 2024, global organizations across the United States, the United Kingdom, France, and Germany participated in a detailed study on their experience with ransomware. To conduct this study, we partnered with experts at Censuswide, an international market research consultancy headquartered in London. Censuswide surveyed 900 IT and security professionals across multiple industries, including education, finance, healthcare, manufacturing and utilities, IT and telecommunications, and travel and transportation.

## HOW TO CITE INFORMATION IN THIS REPORT

The data in this report are provided as an information source for the cybersecurity community and the organizations it serves. Semperis encourages you to share our findings. To cite statistics or insights, reference *Semperis 2024 Ransomware Risk Report* and link to the full report, downloadable from the Semperis website. To interview Semperis experts, contact Bill Keeler at [billk@semperis.com](mailto:billk@semperis.com). Lastly, we'd love to hear your questions or thoughts on the topic of ransomware and resilience.

## ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid identity environments – including Active Directory, Entra ID, and Okta – Semperis' patented technology protects over 100 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series and built the community hybrid Active Directory cyber defender tools, Purple Knight and Forest Druid. The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2024 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner and is a member of the Microsoft Intelligent Security Association (MISA).

