halcyon

2024

Ransomware and Data Extortion Business Risk Report

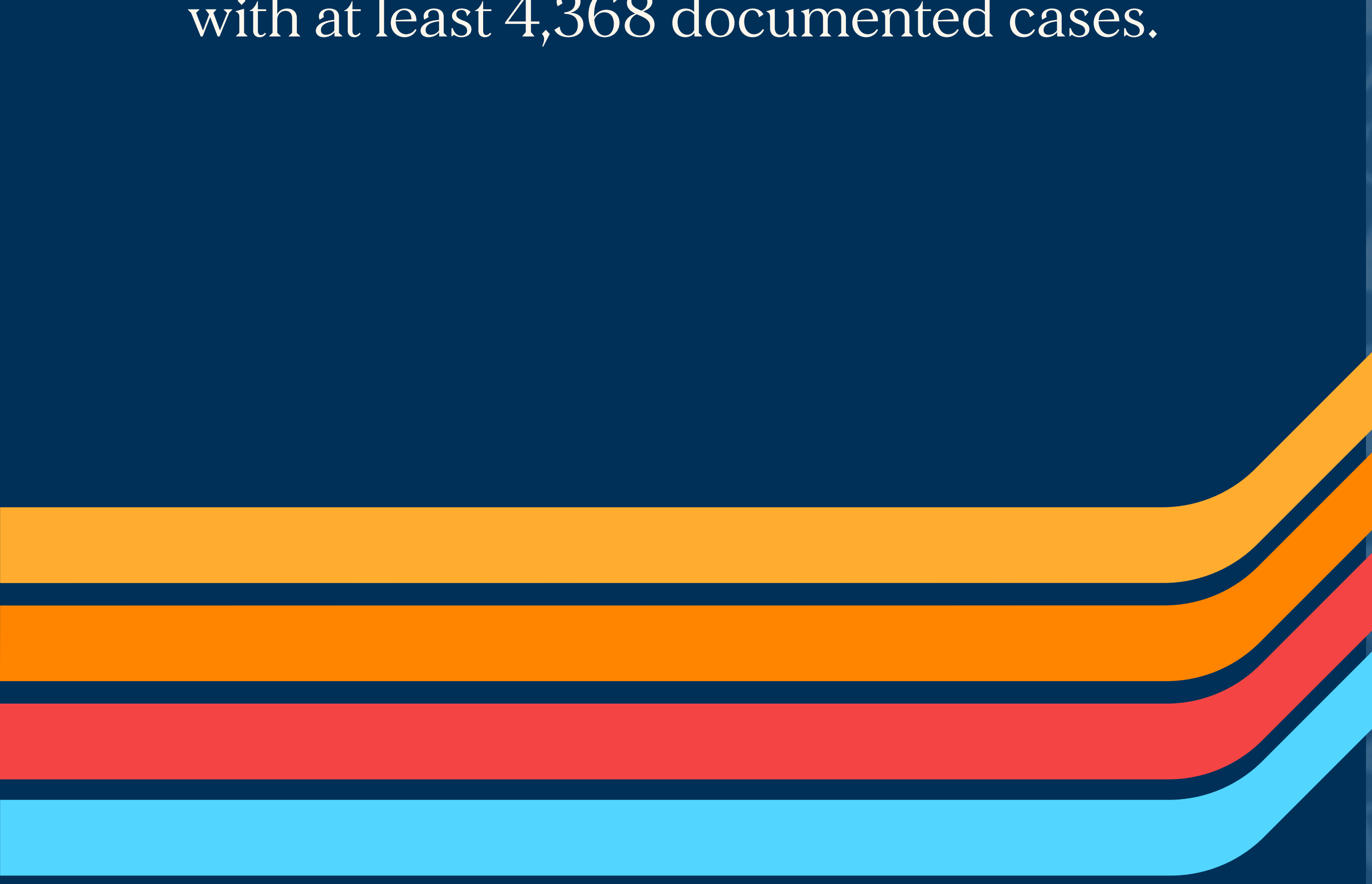
LOCKBIT 2.C

R IMPORTANT FILES ARE STOLEN A

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you s
data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VP
Open our letter at your email. Launch the provided virus on any com
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
[redacted]
Using Tox messenger, we will never know your real name, it means your privacy is guarantee
If you want to contact us, use ToxID:
[redacted]
and we do not respond you, look for the relevant contact data on our website via T

Ransomware operators set numerous records in 2023 and extorted more than $1 billion in payments from victim organizations. The overall volume of attacks surged by 55.5% year-over-year with at least 4,368 documented cases.



In the second quarter of 2024 Halcyon surveyed 913 US-based cyber security decision-makers and practitioners on their experiences with ransomware since 2022.

Security teams remain confident in both their ability to prevent and quickly recover from a ransomware or data extortion attack. Yet in every in major ransomware attack that's been made public, the victim's security controls were bypassed, evaded or otherwise negated by the attacker's tactics, techniques and procedures.

Halcyon recently surveyed 913 Director-level security and IT professionals at North American organizations that were targeted by ransomware operators in the previous 24 months.

The survey results indicate that there is a disconnect between perception and reality when it comes to preparing for and responding to ransomware or data extortion attacks. Additionally malicious data exfiltration continues to put companies in legal and regulatory jeopardy, while disruptions to production environments are prolonged and costly.

Key findings in this study include:

- More than 22% said their organization was targeted with ransomware ten times or more in the last 24 months. 56% of remaining participants stated they were targeted between two and nine times in the same time period.
- 88% were somewhat or very confident their organizations could disrupt an attack before ransomware is delivered. 85% were somewhat or very confident their organizations could quickly resume regular operations following a successful attack.
- Despite this confidence, nearly one-in-five said the attacks resulted in 10 or more ransomware infections, an equal number saying they were targeted 5-9 times, and nearly one-third stating they were infected 2-4 times.
- 21% of victims said operations were disputed for more than 6 months, while 18% said systems were down for 2-4 months, and 24% said disruptions lasted 2-4 weeks.
- Nearly two-thirds said that sensitive or regulated data was exfiltrated in the attacks and nearly the same number said an additional ransom demand was made to protect that data, and that data loss put their organizations at additional risk of regulatory action or lawsuits.
- 59% of respondents indicated the total cost for network remediation (incident response only) cost their organization more than $1 million.
- Of the organizations that opted to pay a ransom demand, the majority (78%) said the attackers failed to provide a working decryptor or data was corrupted upon decryption.

All of the participants indicated their organizations were running some combination of prevention tools including AV, NGAV, EDR, XDR, and/or DLP when they were victimized in a successful ransomware attack.

Nearly four-in-five said that data backups are the primary recovery mechanism despite the fact backups are often targeted for encryption or destruction by attackers, and restoration from backups is an arduous manual process that can take weeks or months.

The findings of this study make it clear that organizations are overly confident in their ability to defend against and quickly recover from ransomware attacks, that data exfiltration is becoming nearly as big of a problem for victim organizations as the actual ransomware payload, and that the cost of recovery can far exceed expectations.

The C-suite and Boards of Directors need to understand that ransomware attacks continue to be one of the biggest threats facing every organization across every industry vertical, that even the most robust security deployments are being bypassed by ransomware operators, and that data loss in the course of a ransomware attack can put them in legal or regulatory jeopardy and end up being a bigger issue than the attack itself.

Security Deployments

Ransomware attacks are making headlines daily. One thing every major ransomware incident has in common: the attacks evade or get around traditional security controls.

Legacy security tools, while necessary and effective in neutralizing a large amount of threats, were simply not designed to address the unique threat that ransomware presents. This is why we continue to see destructive ransomware attacks impact organizations in new ways.

Almost daily we see large organizations with robust security programs get hobbled by ransomware attacks. It is demonstrative of the fact that, even if an organization has ample resources to stand up a security program, it takes the exploitation of just one unpatched vulnerability to bring them to their knees, as we saw repeatedly in the mass exploitation of the MOVEit and GoAnywhere file transfer software.

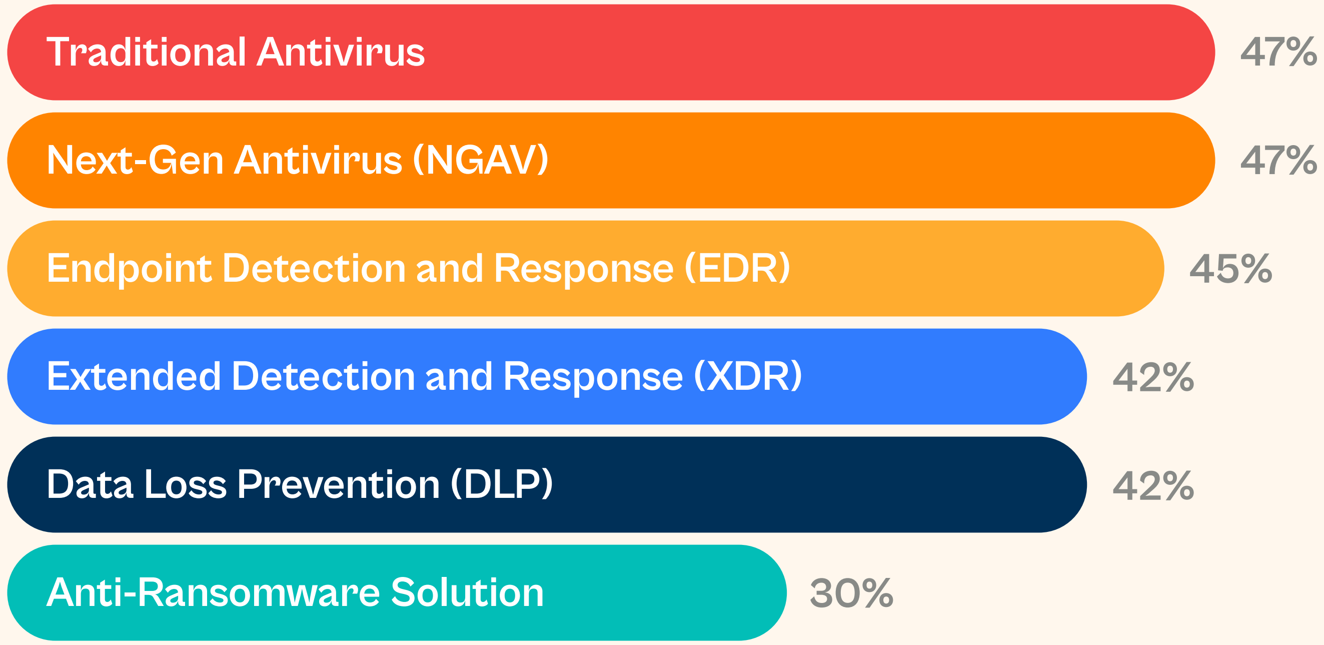
Organizations cannot simply focus on deploying preventative technologies or data backups and expect that to be enough. Threat actors have proven repeatedly that they can easily circumvent a variety of security controls.

Even if an organization has a mature security program, it takes the exploitation of just one unpatched vulnerability to bring them to their knees.

In this study, respondents indicated their organizations were running a variety of security solutions, either as stand-alone or alongside other solutions. Nearly half of respondents indicated their organizations had Traditional Antivirus (47%), Next-Gen Antivirus (47%), or Endpoint Detection and Response (45%) solutions deployed on their networks.

More than one-third indicated their organizations had Extended Detection and Response (42%) and Data Loss Prevention (42%) solution deployed, while less than one-third had a Anti-Ransomware Solution (30%) deployed.

Which types of security solutions were deployed?



What is the confidence level in the security stack?

Given the significant investments their organizations have made in their respective security programs, the majority of respondents (88%) were “very confident” (61%) or “somewhat confident” (27%) their security apparatus could disrupt an attack before the ransomware payload was delivered and data/systems encrypted.

Just about one-in-ten were unsure of the effectiveness of their security stack (8%), while just a fraction (4%) lacked confidence attacks could be disrupted before data/systems were encrypted.

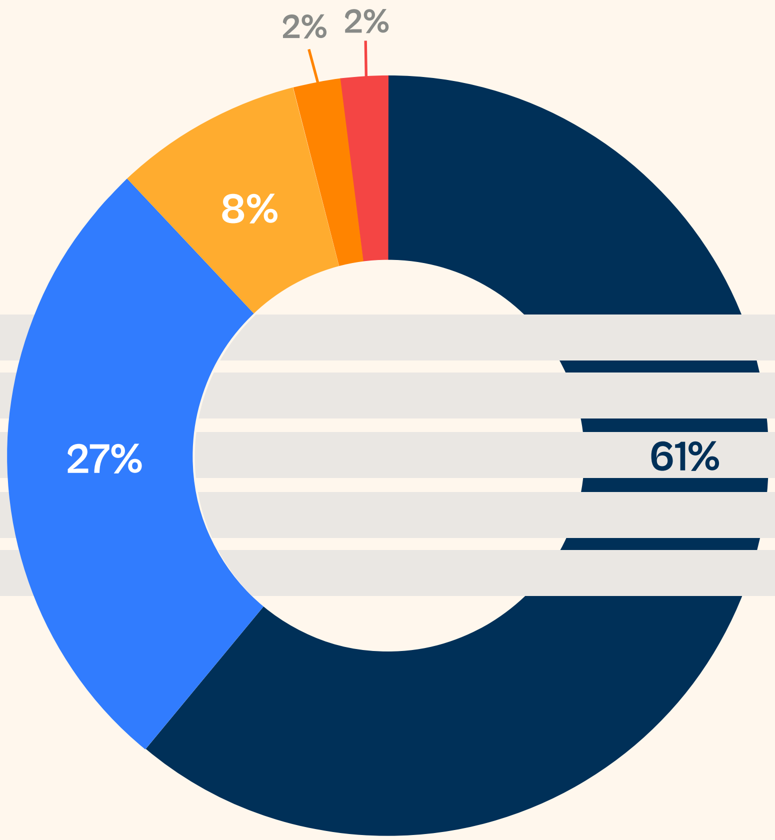
Furthermore, if an attack were to be successful and a ransomware payload was delivered resulting in a network infections, the majority of respondents (85%) felt “very” (58%) or “somewhat” (27%) confident their organizations could quickly resume regular operations, while just a fraction (4%) indicated they were not confident their organization could quickly recover from an infection, with about one-in-ten (11%) saying they were unsure.

On average, a ransomware attack takes 237 days to detect and 89 days to fully remediate (PDF). While some organizations may be able to withstand lengthy disruptions to some systems, for sectors like manufacturing and retail where losses are measured in minutes, this level of disruption could be catastrophic and represent an existential event. For healthcare providers the impact has been shown to negatively impact patient outcomes and potentially result in premature deaths.

There is a significant disconnect between confidence in security programs and the ability to actually detect and disrupt a ransomware attack before data is exfiltrated or an infection occurs.

How confident are you that current security deployments can stop a ransomware attack before infection?

●	Very confident	61%
●	Somewhat confident	27%
●	Uncertain	8%
●	Not very confident	2%
●	Not confident at all	2%



As you will see below, there is a significant disconnect between survey respondents' confidence that their security programs are prepared to detect and disrupt a ransomware attack - and that their organizations could quickly recover from a successful attack - and the number of attacks on their organizations that actually resulted in an infection by a ransomware payload, major disruptions to operations, and costly remediation efforts.

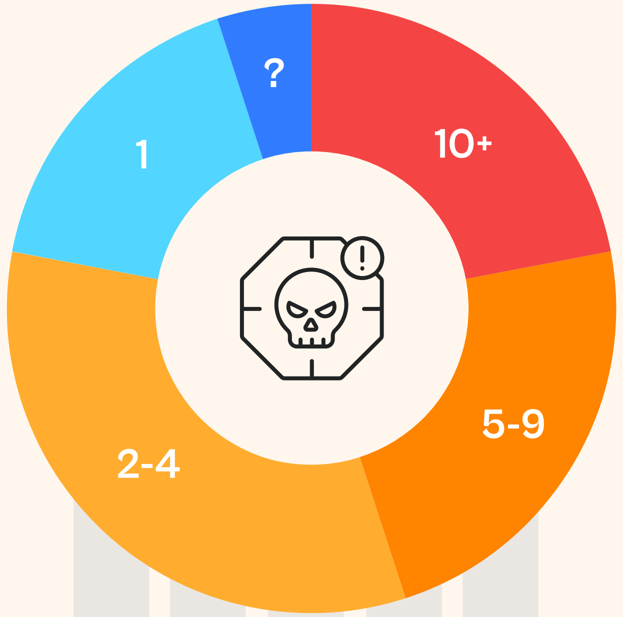
Ransomware Attacks

Ransomware is no longer considered a boutique threat, but rather one of the most significant threats to any organization. Recent research found that ransomware attacks surged by an alarming 55.5% in 2023, and the vast majority (75%) of organizations reported being targeted by at least one ransomware attack in the last 24 months, with 26% reporting they were targeted by ransomware operators four or more times.

```
A:\>dir

 Volume in drive A has no label
 Volume Serial Number is 2A07-6CE1
 Directory of A:\

COMMAND  COM        93,040  04-18-05   5:54p
DISPLAY  SYS        17,175  04-18-05   5:54p
EGA      CPI        58,870  04-18-05   5:54p
EGA2     CPI        58,870  04-18-05   5:54p
EGA3     CPI        58,753  04-18-05   5:54p
KEYB     COM        21,607  04-18-05   3:04a
KEYBOARD SYS        34,566  04-18-05   5:54p
KEYBRD2  SYS        31,942  04-18-05   5:54p
KEYBRD3  SYS        31,633  04-18-05   5:54p
KEYBRD4  SYS        13,014  04-18-05   5:54p
MODE     COM        29,239  04-18-05   5:54p
        11 file(s)          448,709 bytes
         0 dir(s)           889,344 bytes free

 A:\>
```

How many times was your organization attacked in last 24 months?

●	Attacked 10 times or more	22%
●	Attacked 5 - 9 times	23%
●	Attacked 2 - 4 times	33%
●	Attacked just once	17%
●	Attacked, but unsure how many times (?)	5%



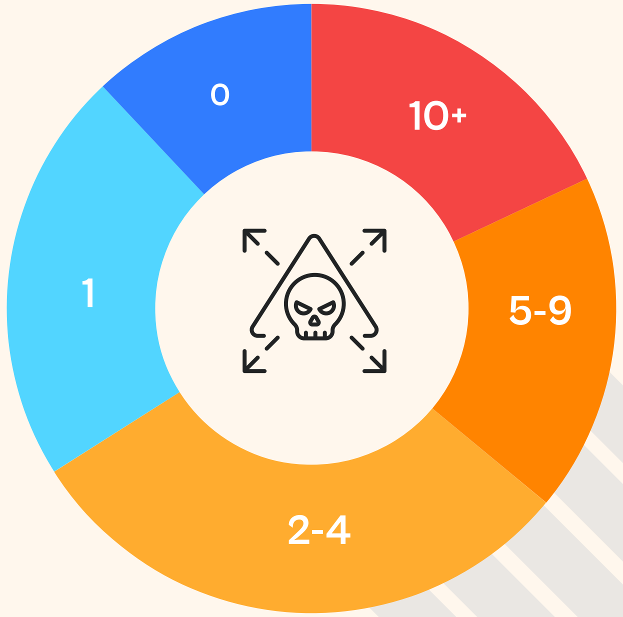
In this study, about one-in-five respondents (22%) indicated their organization was targeted by ransomware operators a staggering ten times or more in the last 24 months, while nearly one-in-four (23%) said they were targeted five or more times.

One-third (33%) of respondents were targeted two times or more, and about one-in-five indicated their organization was targeted just once or were unsure how many times they were attacked.

About one-in-five respondents indicated their organization was targeted by ransomware operators a staggering ten times or more in the last 24 months.

How many attacks resulted in ransomware infection?

●	Infected 10 times or more	18%
●	Infected 5 - 9 times	18%
●	Infected 2 - 4 times	30%
●	Infected just once	22%
●	Never infected	12%



How many attacks were successful?

Of the organizations that were targeted by ransomware operators, nearly one-in-five (18%) indicated the attack resulted in the encryption of data/systems ten or more times, and the same number of respondents (18%) indicated the attack resulted in encryption more than five times.

Nearly one-third (30%) indicated data/systems were encrypted on at least two occasions, and just over one-fifth (22%) indicated just one successful infection. More than one-in-ten (12%) of respondents said that they were targeted by ransomware operators but never infected.

As we can see from the contrast, while confidence is high that ransomware attacks can be detected and blocked before delivery of the ransomware payload and subsequent encryption of data and systems.

Today's more complex ransomware and data extortion operations are multi-staged attacks where the threat actors are looking to infiltrate as much of the targeted network as possible while exfiltrating sensitive data along the way to be used as leverage.

Unfortunately, most organizations are unaware they are the victim of a ransomware attack until the encryption payload and ransom note are delivered, which are the tail-end of the larger ransomware operation.

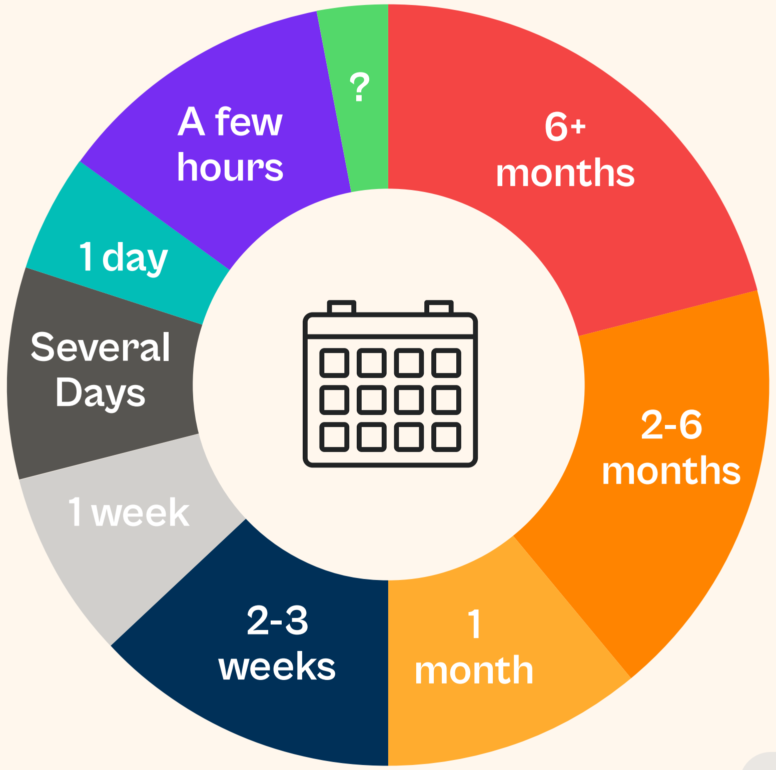
Business Impact

There are several statistics available for the average operational downtime resulting from ransomware attacks, with the average being about three to three and a half weeks. Yet in this study, shockingly half of respondents (50%) indicated that a ransomware attack disrupted business operations at their organization for a month to more than half a year.

How long were business operations disrupted?

Specifically, one-in-five (21%) said operations were disrupted for 6 months or more, while nearly as many said disruptions lasted 2-6 months. About one-in-ten (11%) said disruptions lasted for about one month, while only about one-in-five (21%) said disruptions lasted one or more weeks, and only about one-in-seven (14%) said they resolved disruptions in a matter of days.

Research indicates that remediation costs following a ransomware attack average more than $4.5M per incident for targeted organizations. This figure does not include additional incident response costs or tangential costs like damage to the brand, lost revenue, or lost production from downed systems.

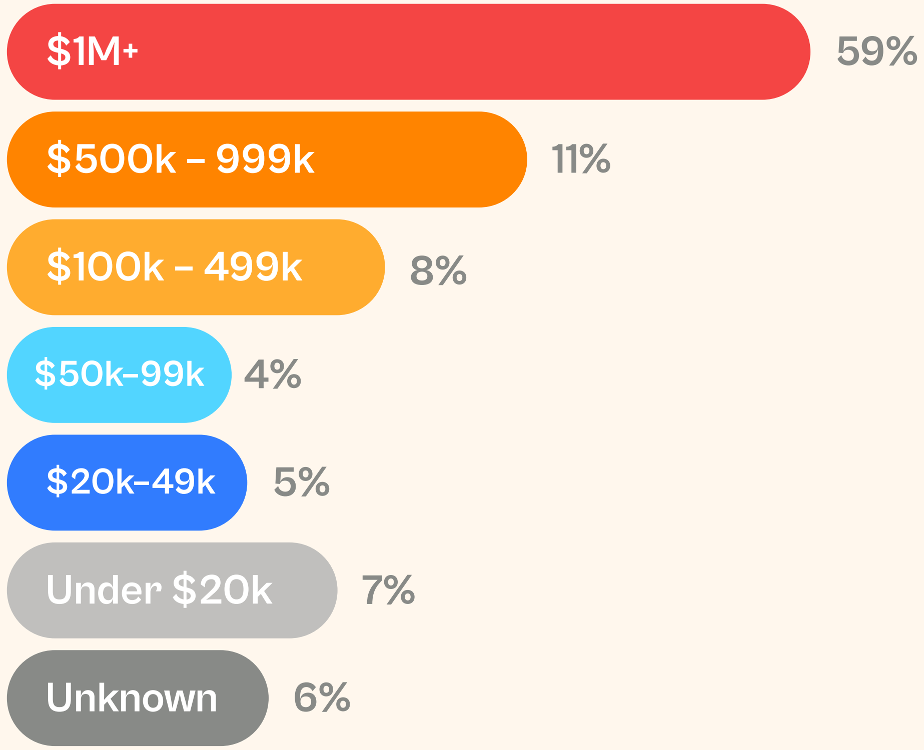


●	Over 6 months	21%
●	2-6 months	18%
●	1 month	11%
●	2-3 weeks	13%
●	1 week	8%
●	Several days	9%
●	One day	5%
●	A few hours	12%
●	Uncertain (?)	3%

How much were incident response costs (IR only)?

In this study, 59% of respondents indicated the total cost for remediation (incident response only) cost their organization more than $1 million, one-in-ten (11%) said incident response costs ran about $500,000 – $999,999, and less than one-in-ten (8%) said remediation cost their organizations between $100,000 – $499,999.

Just about one-in-six (16%) said incident response cost less than $100,000. Collateral damage from ransomware attacks can include loss of intellectual property, loss of consumer trust, increased cyber insurance premiums, legal liability, and lost revenue, all of which can far exceed remediation costs.

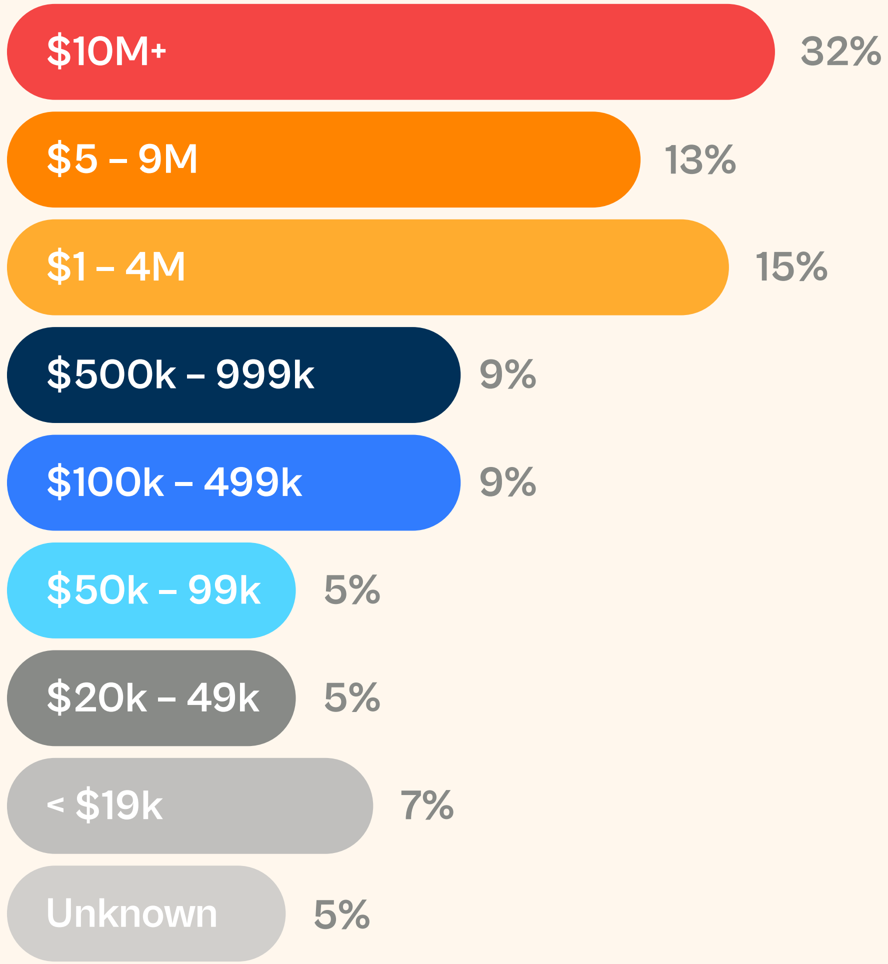


Fifty-nine percent (59%) of participants indicated remediation (incident response only) cost their organization more than $1 million.

What were the estimated total losses?

About one-third of respondents in our study (32%) said total losses to the organization from the costliest ransomware attack exceeded $10 million. More than one-quarter (28%) said total losses to the organization ranged between $1-$9 million and less than one-fifth (18%) said losses ran between $1,000,000 and $999,999, while a nearly equal number (17%) said total losses following a successful attack were below $100,000.

Ransomware attacks can have lasting impact, negatively impacting long-term operations, competitiveness, profitability, or overall viability of the organization.

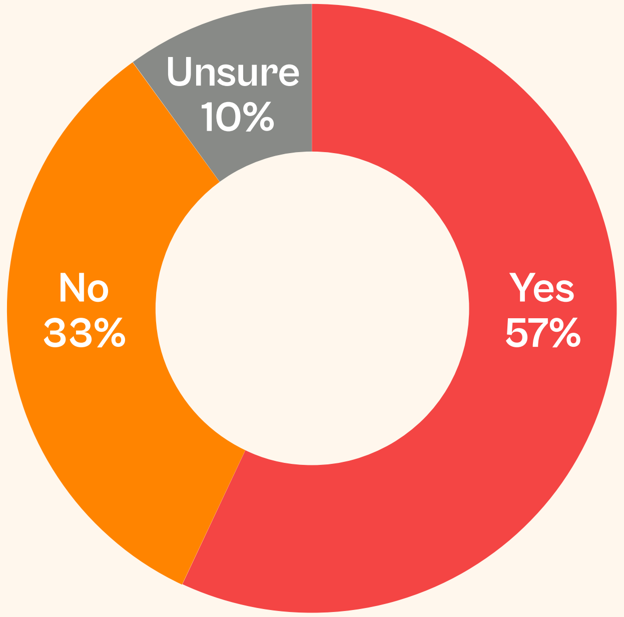


One-third of respondents in our study (32%) said total losses to the organization from the costliest ransomware attack exceeded $10 million.

Will there be long-term impact on the organization?

In this study, more than half (57%) of respondents said ransomware attacks have or will hurt our organization in the long-term, while one-third (33%) believed there would be no long-term impact to the organization and one-in-ten (10%) were unsure.

This, of course, again runs counter to the levels of confidence from respondents for both the capability to detect and disrupt an attack and the ability to swiftly recover from a successful attack reported above, highlighting the disconnect between perception and real-world outcomes.



More than half (57%) of respondents said ransomware attacks have or will hurt our organization in the long-term.

Data Exfiltration

Data exfiltration occurs when a threat actor engages in an unauthorized data transfer from a computer, server, or other network system without the consent of the system's owner.

The types of data threat actors exfiltrate typically include the personally identifiable information of clients or employees, information related to payment processing, the organization's business dealings, trade secrets, and intellectual property, and other data the attacker can leverage for tactical or financial gain.

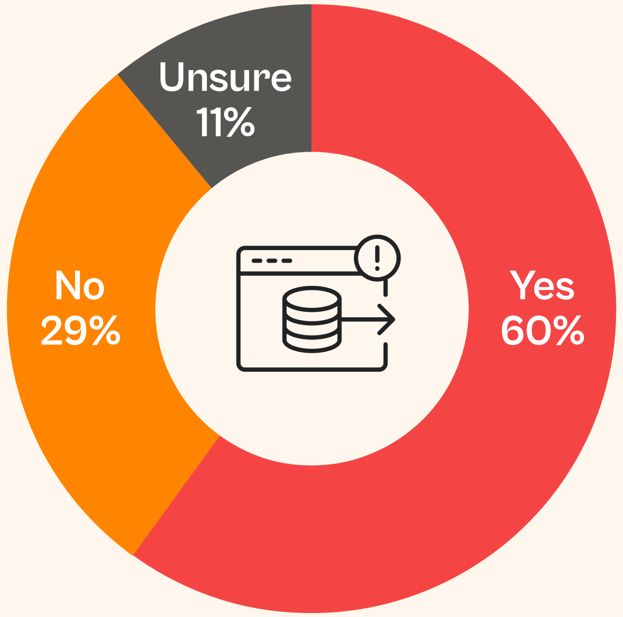
Data exfiltration and the threat of exposure are now a central aspect of nearly every ransomware operator's playbook and significantly increase the chances for the extortion efforts to be successful.

The double extortion tactic begins when they exfiltrate sensitive information from the target before launching the encryption routine. The threat actor then makes the additional demand that victims pay up to prevent the attackers from publishing their data online.

Was sensitive or regulated data exfiltrated?

In this study, nearly two-thirds of respondents (60%) indicated that sensitive or regulated data was exfiltrated by ransomware operators, while less than one-third (30%) said no data was lost and one-in-ten (11%) were unsure of any data was exfiltrated.

In many cases, attackers may not only demand payment of a ransom to regain access to encrypted systems, but they may also demand further payment for the stolen data itself. And of course, there is no guarantee that payment will protect the stolen data from being exploited.



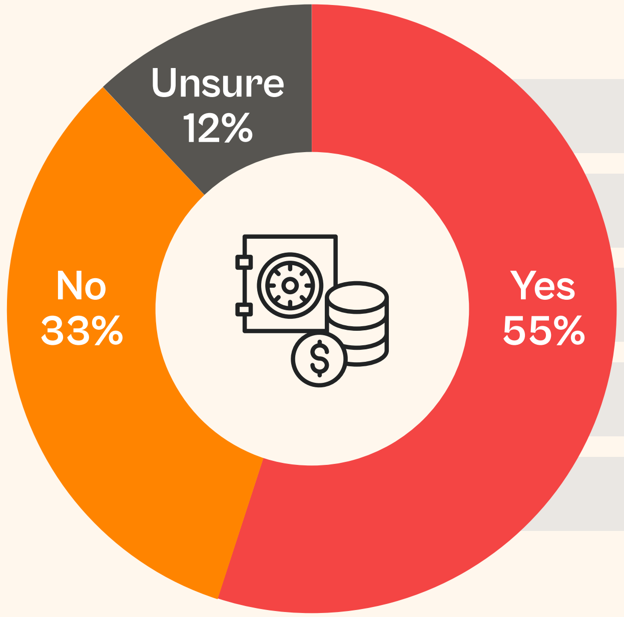
Was additional ransom payment required for exfiltrated data?

Of the organizations who said data was exfiltrated by ransomware operators, more than half (55%) said the attackers required an additional ransom payment for the data in addition to the ransom demanded to provide a decryptor to recover data/systems.

Fully one-third (33%) said the attackers only demanded one ransom payment for the decryptor and assurance the exfiltrated data would not be exposed, while about one-in-ten (12%) were uncertain whether an additional ransom payment was demanded to protect or recover the exfiltrated data.

Ransomware operators are more often threatening to publish or sell stolen data if the ransom is not paid. This can lead to regulatory fines, legal liability, and severe damage to the company's brand and customer trust.

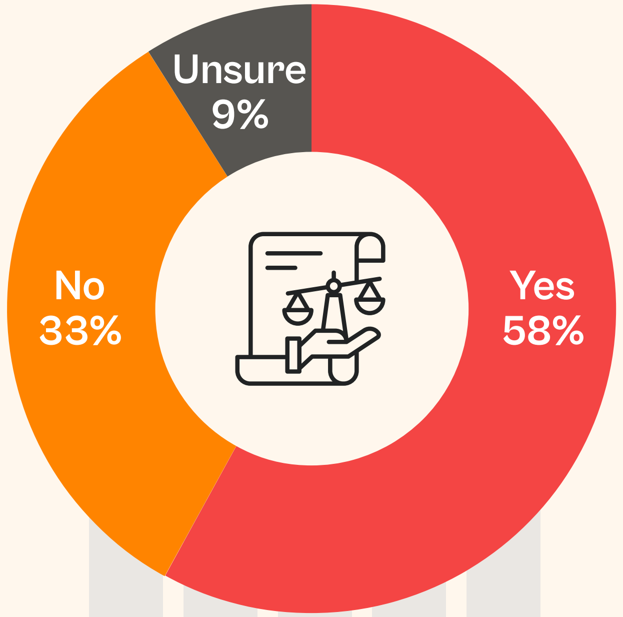
The number of class action lawsuits spurred by ransomware attacks that include data exfiltration has skyrocketed in the last two years, and liability risk is also specifically hitting the C-suite and Boards of Directors. Even if organizations are prepared to respond and recover from a ransomware attack, the fact that sensitive data was stolen or exposed puts them at additional liability risk.



Did exfiltration result in regulatory or legal risk?

Of the organizations who said data was exfiltrated by ransomware operators in this study, more than half (58%) indicated the exfiltration of sensitive data put their organization at additional legal and regulatory risk.

One-third (33%) said they did not believe the exfiltration of data put their organization at additional legal and regulatory risk, while less than one-in-ten (9%) were uncertain if the exfiltration of data put their organization at additional legal and regulatory risk.



More than half (58%) indicated the exfiltration of sensitive data put their organization at additional legal and regulatory risk.

Recovery

The targeting of data backups, whether stored on-site or in the cloud, has increasingly become a favored tactic of ransomware attackers. Today's attacks typically include the exfiltration of sensitive data, so even if systems can be restored without having to pay the ransomware operators for a decryption key, there is no guarantee that a ransom payment will prevent the stolen data from being exploited.

This challenge is further complicated by a common tactic where the attackers use legitimate network tools like the Windows VSSadmin process to delete shadow copy backup files.

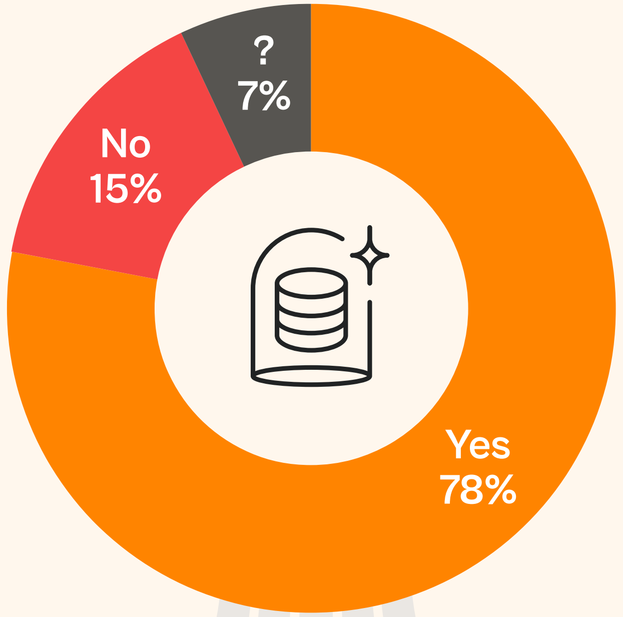
Are data backups as primary means of recovery?

This study found that the vast majority of respondents indicated their organizations depend on data backup solutions as the primary recovery mechanism for ransomware attacks (78%), while about one-in-seven (15%) said their organizations did not depend on data backups, and a fraction (7%) were uncertain what their organization planned to use to recover from a ransomware attack.

It is increasingly likely that ransomware operators will wipe backups during the attack, so backups have limited utility regarding ransomware attacks. Even when uncorrupted backups are available, restoration of every infected device is an arduous task involving a manual wiping and re-imaging process that can take weeks or months, and at great cost.

Data backups are still highly recommended for disaster recovery, but organizations cannot depend on them as the primary means of recovering from a successful ransomware attack.

Organizations need to also understand that paying the ransom does not guarantee that data and systems will be restored, and there are numerous cases where a ransom was paid, and key received, but the data was corrupted during decryption. Also, even if all is restored, paying the ransom may result in further attacks.

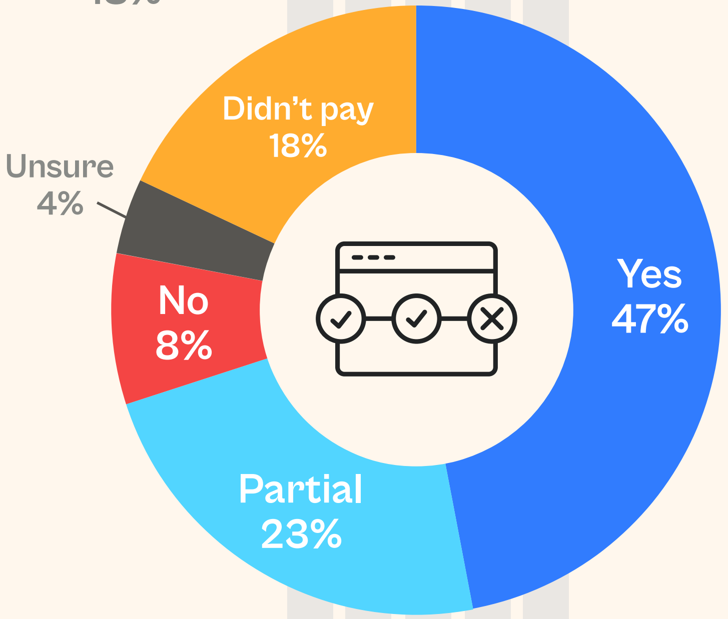


The vast majority of respondents indicated their organizations depend on data backup solutions as the primary recovery mechanism for ransomware attacks (78%).

If ransom paid, did the attackers provide a working decryptor?

●	Yes, the key restored systems to normal	47%
●	Yes, but only on partially restored systems	23%
●	No, the key did not restore systems	8%
●	Unsure (?) if the attacker supplied a valid key	4%
●	My organization did not pay a ransom	18%

Nearly one-fifth of respondents in this study (18%) said their organization refused to pay a ransom demand. Of the organizations that opted to pay a ransom demand (82%), less than half (47%) said the attackers provided them with a encryption key that restored data/systems to normal, while nearly one-third (31%) said the attacker provided an encryption key but it only partially restored systems or did not work at all.



Of the organizations that opted to pay a ransom demand, the majority (78%) said the attackers failed to provide a working decryptor or data was corrupted upon decryption.

Cyber Insurance

As it stands, insurance companies have not been able to put their finger on the magic equation that allows for affordable policies for both the insured and the insurer. Ransomware attacks vary in severity, and ransom demands range from tens of thousands to tens of millions of dollars.

Furthermore, organizations may handle different kinds of sensitive data that put them in different liability categories, and they may use a wide range of security solutions, each filling one small gap in protection, all of which need to work together to prevent a disruptive event. This is a complicated ecosystem for insurers to cover.

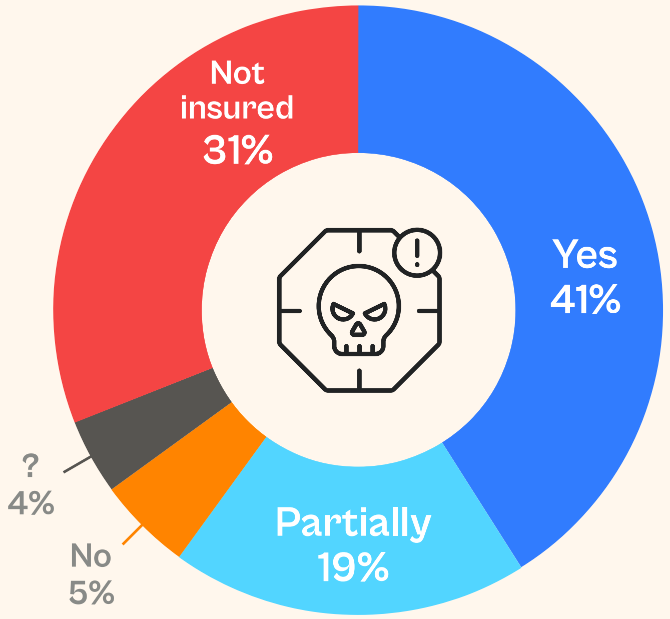
Did cyber insurance cover the incident response costs?

●	Yes, cyber insurance covered the cost of recovery from the attack(s)	41%
●	Yes, but cyber insurance only covered a portion of the cost of recovery	19%
●	No, cyber insurance did not cover recovery costs	5%
●	Unsure (?) if cyber insurance covered recovery costs	4%
●	My organization does not carry cyber insurance	31%

In this study, of the organizations that do have a cyber insurance policy in place, less than half of respondents indicated (41%) said their organization's cyber insurance policies covered the incident response costs, while one-in-five (19%) said their policies only covered some of the costs of remediation and a fraction (5%) said their policies did not cover any of the remediation costs.

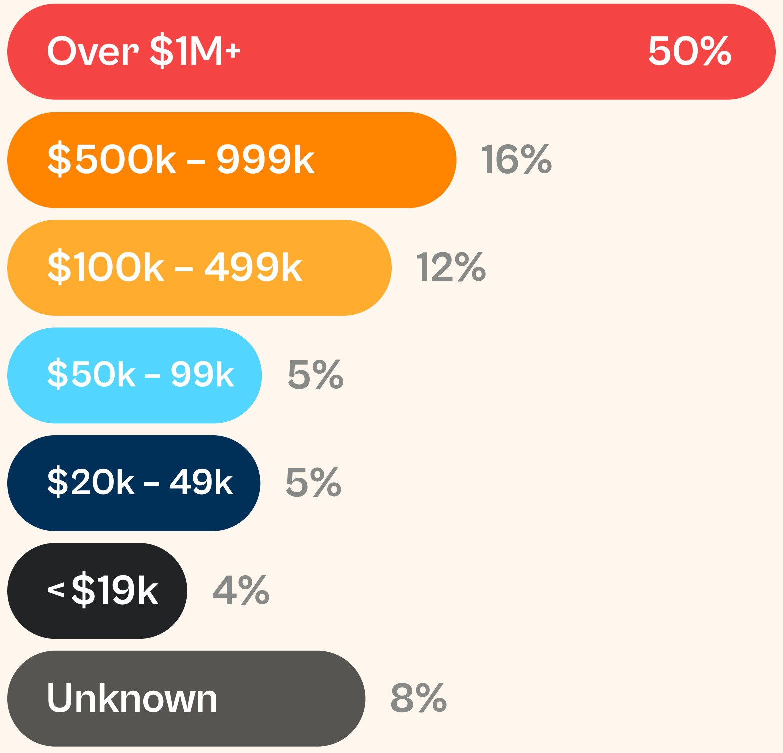
Policy holders are facing more restrictive policies with add-ons for covering ransomware-related losses, more comprehensive audits of security controls, and ever-increasing premiums, while insurance providers are facing a crunch on pricing the policies accurately to cover the losses they see in the real-world, which are continuing to grow.

Then there is the debate over whether to pay ransom demands, which has become a contentious issue among experts. The simple answer would seem to be that organizations should never pay a ransom demand, which would significantly diminish the financial incentives for these attacks. In many circumstances that might be the logical approach, but it may not be the right approach for every organization.



It has been observed that most victims who paid a ransom demand were attacked again, often by the same threat actor who demands a higher ransom payment knowing the victim is likely to pay. The average ransom demand 2023 was $5.3 million, and in this study fully half of the respondents (50%) indicated that ransomware operators demanded a ransom payment of more than $1 million or well into the tens-of-millions of dollars.

What was the highest ransom demand?



50% of participants indicated attackers demanded a ransom payment of more than $1 million or more. More than one-quarter (28%) said ransom demands ran between $100,000 and $999,999, while half as many (14%) indicated the ransom demands were less than $100,000.

Many organizations consider or have already purchased cyber insurance policies to cover the cost of a cyberattack or data breach event. The increased risk of ransomware attacks in recent years had made cyber insurance even more appealing. But today most insurers no longer cover all potential losses from ransomware attacks, and those that do have increased premium costs.

Insurers simply do not know how to quantify the risk from ransomware accurately to set premiums. Whether or not cyber insurance is the right instrument for organizations when considering the impact of ransomware attacks is in question.

For cyber insurance policies that do offer ransomware coverage, many will no longer cover the ransom payment – they can vary too wildly, so it is too hard to define actuarially. Only after a ransomware attack hits an organization do they find the policy will only cover a fraction of the costs/ losses/remediation.

Did cyber insurance cover the ransom demand?

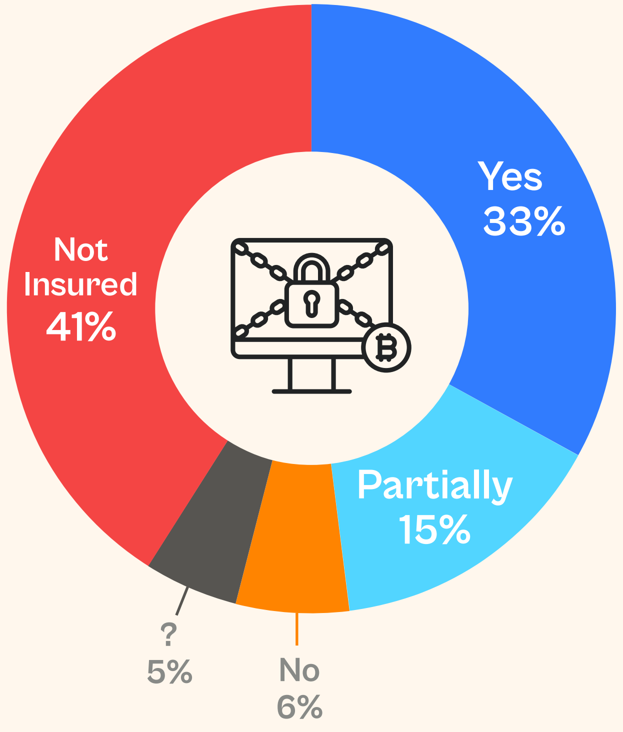
●	Yes, covered the ransom	33%
●	Yes, but only a portion	15%
●	No, did not cover ransom	6%
●	Unsure (?) if cyber insurance covered the ransom demand	5%
●	My organization does not carry cyber insurance	41%

In this study, of the organizations who paid a ransom demand, one-third indicated cyber insurance covered the full ransom demand, while about one-in-seven (15%) said the policies only covered a portion of the ransom demand, and a fraction (6%) said cyber insurance did not cover any of the ransom demand.

Cyber insurance is not always a viable option for all organizations, and it is certainly not for companies who think they can indemnify instead of investing in security. For a policy to be in force, the organization needs to have an extensive accounting of its security program.

If and when the time comes to submit a claim, if the organization is out of compliance – for example, if it did not apply patches in a timely manner or misconfigured security applications – they may be disappointed to find that their policy does not cover the attack.

Furthermore, ransomware attacks vary in severity, and ransom demands range from tens of thousands to tens of millions of dollars. Insurance customers are facing more restrictive policies with add-ons for covering ransomware-related losses, more comprehensive audits of security controls, and ever-increasing premiums, while insurance providers are facing a crunch on pricing the policies accurately to cover the losses they see in the real-world, which are continuing to grow.

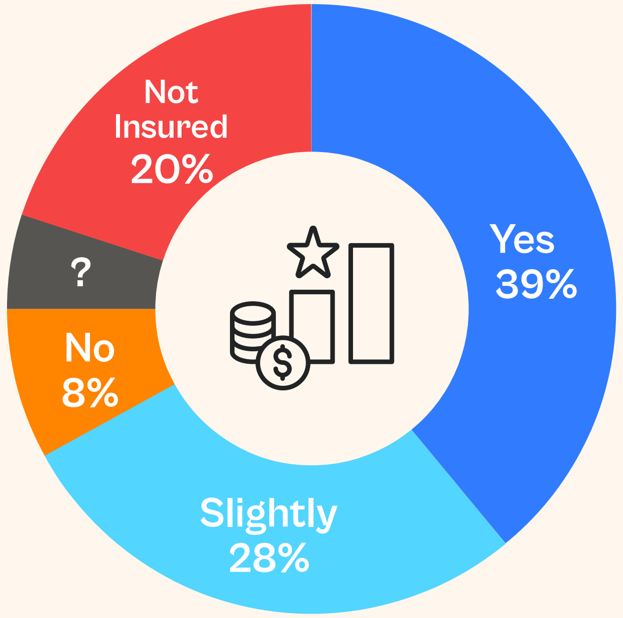


According to the Insurance Journal, cyber insurance premiums jumped 50% in 2022 due to the surge in ransomware attacks and tripled over the previous three years. As well, Beta News reported that insurance provider Coalition reported a 12% spike in cyber insurance claims related to ransomware attacks over the first six months of 2023, with organizations having over $100 million in revenue seeing the largest increase (20%).

Have premiums increased in the past 24 months?

●	Yes, premiums increased significantly	39%
●	Yes, premiums increased slightly	28%
●	No, premiums remained same	8%
●	Unsure (?) if premiums changed	5%
●	My organization does not carry cyber insurance	20%

In this study, of the organizations who have cyber insurance policies, nearly two-in-five (39%) said their premiums increased significantly following a successful ransomware attack, while more than one-quarter (28%) said their premiums increased slightly. Less than one-in-ten said their premiums stayed about the same following a ransomware attack.



Nearly two-in-five (39%) said their premiums increased significantly following a successful ransomware attack.

Takeaway

More focus needs to be placed "left of boom" – at initial ingress, command and control (C2), lateral movement, data exfiltration, and so on. If we are doing our jobs right and disrupt an operation at these earlier stages, then we would not even know it was a ransomware attack, just another intrusion event.

As well, there is not enough focus on what comes after "boom" – how the organization can plan for the failure of security controls and be positioned to respond efficiently and effectively to a future ransomware attack, making the organization and its operations as resilient as possible by reducing the potential for mass disruption.

The findings of this study demonstrate that organizations are overly confident in their ability to defend against and quickly recover from ransomware attacks, that the risk from data exfiltration is not being adequately addressed by organizations, and that the cost of recovery can far exceed expectations.

The C-suite and Boards of Directors are increasingly at risk from lawsuits and regulatory actions due to the exfiltration of sensitive data as even the most robust of security programs continue to be routinely bypassed by ransomware operators.

Achieving cyber resilience requires more than just robust cybersecurity measures; it demands a comprehensive understanding of an organization's preparedness to withstand and rebound from cyber incidents. Central to this endeavor is the strategic selection and diligent monitoring of key performance indicators (KPIs) and metrics tailored to assess cyber resilience effectively.

Here are some of the essential metrics that can assist in bolstering organizational resilience:

Mean Time to Detect (MTTD):

This measures how long it takes for an organization to detect a cyber threat or incident. A lower MTTD indicates better detection capabilities. MTTD is a key indicator that can be used to determine whether an organization is properly prepared to respond to threats in a timely manner. Lowering the MTTD can help contain the lateral movement within an organization and is an effective way to reduce the potential impact spread in a breach.

Mean Time to Respond (MTTR):

This measures how long it takes for an organization to respond to a cyber threat or incident once it has been detected. A lower MTTR indicates faster response capabilities. Once an incident has been detected how quickly is an organization able to respond to the event, in order to effectively lower this metric, consider the outcomes of tabletop exercises and implementation of lesson learned during incidents that should provide indications of area for improvement in the response.

Incident Response Plan Effectiveness:

Assess the effectiveness of the incident response plan by measuring how well it is followed during a cyber incident, including factors like containment time, communication effectiveness, and coordination among response teams. In order to have an effective cyber resilience strategy it is key that an organizations response plans are effective and followed, if the plan is not being followed it can lead to an increase in the time required to respond and effectively mitigate the issue. Evaluate whether the plan needs to be changed to address changes in the threat landscape, risk themselves, or the organization response.

Cybersecurity Training and Awareness:

Measure the effectiveness of cybersecurity training programs by tracking metrics such as employee awareness levels, completion rates of training modules, and performance in simulated phishing exercises. At the end of the day cyber incidents often have at least some if not a major human component. Evaluate the effectiveness of the training you are providing and the way it is provided. Often organizations provide a "one size fits all" approach to cyber training and awareness, this unfortunately misses the mark, a successful approach for a developer will not address the same needs for the CFO.

Cybersecurity Hygiene:

Track metrics related to cybersecurity hygiene practices, such as the frequency of system patching, vulnerability scanning results, and compliance with security policies and standards. Hygiene should be table stakes for any organization trying to increase their cyber resilience, however this is often not the case. Create a prioritized approach to address the hygiene issue. Avoid the pitfall of chasing the next new cyber solution until you have a successful approach to address your organization's cyber hygiene.

Cyber Risk Exposure:

Quantify cyber risk exposure by assessing the organization's risk posture based on factors such as asset criticality, vulnerability severity, and threat likelihood. If you do not have a valid way to measure your exposure, then you have little ability to identify where to prioritize your resources and increase your resilience.

Third-Party Risk Management:

Track metrics related to third-party cyber risk, including the number of third-party assessments conducted, the level of compliance with security requirements, and any incidents or breaches involving third-party vendors. In today's interconnected world it is impossible to have any perspective on the resilience of your organization if you can understand the risk that your third-party relationships and connections are introducing into the ecosystem you operate in.

Security Controls Effectiveness:

Assess the effectiveness of security controls by monitoring metrics such as intrusion detection/prevention system (IDS/IPS) alerts, firewall rule effectiveness, and malware detection rates. Are your controls effective? Should you be investing in other areas with potentially better ROI? Measuring whether you have implemented the right controls and are delivering the right results is important to consider.

Backup and Recovery Metrics:

Measure the effectiveness of backup and recovery processes by assessing metrics such as backup success rates, recovery time objectives (RTO), and recovery point objectives (RPO). In an incident, can you get the data back? How long will recovery take? Does it match the desired recovery window? This should be tested and confirmed that the expectation meets real world results.

Business Continuity and Disaster Recovery Metrics:

Business Continuity and Disaster Recovery (BCDR) metrics measure the organization's ability to maintain operations during and after a cyber incident by tracking metrics such as recovery time objectives (RTOs), recovery point objectives (RPOs), and the success rate of BCDR exercises.

Effective cyber resilience requires a holistic approach that incorporates proactive measures, rapid detection, efficient response, and robust recovery mechanisms. By monitoring and optimizing these key metrics, organizations can enhance their ability to withstand and recover from cyber threats, safeguarding their operations and maintaining business continuity.

Lastly, think about how often the plan is tested and confirm disaster recovery planning. Sometime this is outside of cyber, but it is important to confirm that your plans can be implemented in a true DR scenario and services remain available.

halcyon

The Halcyon Mission: Defeat Ransomware

Halcyon is the cyber resilience platform that Global 2000 companies rely upon to defeat ransomware-as-a-service attacks. With the fastest endpoint recovery capabilities and multiple layers of resiliency that includes bypass and evasion protection, key capture and automated decryption and data extortion prevention, the Halcyon Anti-Ransomware Platform reverses the impact of ransomware attacks in just minutes. For more information on how Halcyon efficiently and effectively defeats ransomware attacks, contact an expert here or visit halcyon.ai to request a free consultation.