

2022 Impacts: Ransomware attacks and preparedness

As ransomware threats continue to ramp up, do organizations understand the true financial risk and are they suitably equipped to mitigate the damages of attacks?



REPORT



The ransomware crisis is getting worse

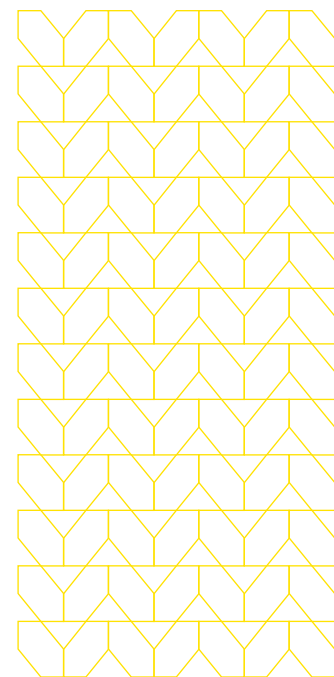
Ransomware is one of the biggest threats facing organizations today, and it is only likely to get worse.

The ongoing barrage of attacks shows no sign of slowing down. For cybercriminals, ransomware is a proven and effective mechanism for hitting a huge payday in one shot, with payouts totaling as much as \$40 million.

Threat actors are currently riding off the coattails of what can only be described as a perfect security storm.

The mass shift to remote and hybrid work has expanded the attack surfaces of many organizations, unveiling a host of new vulnerabilities, attack vectors, and network entry points for threat actors.

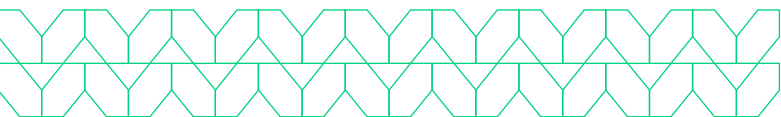
Ransomware attackers are also continuing to develop more advanced techniques to increase the likelihood of successfully demanding a ransom payment. There has been a surge in a class of cyberthreats known as [Highly Evasive Adaptive Threats](#) (HEAT), which are designed to bypass detection from traditional security tools such as Secure Web Gateways, sandbox analysis and phishing detection solutions.

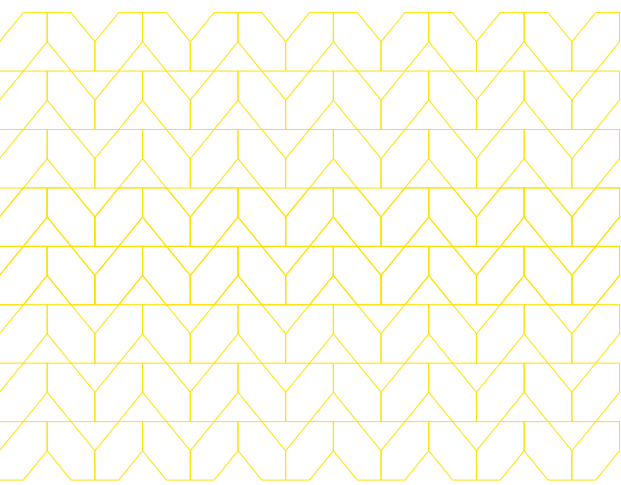


One third of organizations experience ransomware attacks at least weekly, and 9% do so more than once a day.



53% of organizations have been the victim of a ransomware attack in the last 18 months.





Unfortunately, it's not just sophisticated threat actors using these techniques. The threat landscape rapidly evolved, with ransomware-as-a-service (RaaS) enabling low-skilled cybercriminals to leverage ready-made ransomware tools in a quick, affordable, and scalable manner.

Owing to this perfect storm, the [European Union Agency for Cybersecurity \(ENISA\)](#) recently defined today's threat landscape as the "golden era of ransomware."

To assess the extent of the challenges organizations face in dealing with ransomware threats, Menlo Security surveyed 505 IT security decision makers across the UK and US.

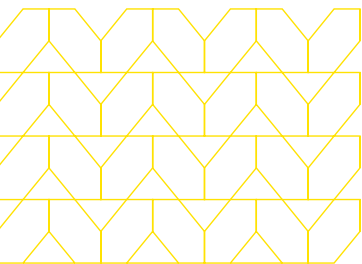
Key findings

- Between weak links in the security chain and an inability to identify where attacks stemmed from, the confidence of organizations in mitigating the threat of ransomware is lacking in several areas.
- Organizations need to consider unmanaged devices as part of their security strategy, with mobile highlighted as a leading attack vector.
- Many security professionals are underestimating the cost of recovery, with current insurance payouts unable to cover even a third of the financial damages inflicted by the average ransomware attack in 2021.
- There is a lack of consensus on how to deal with attackers, whether that's paying the ransom, never paying the ransom, or calling on insurance firms and governments to step up and take responsibility.
- Most organizations still don't have a detailed response plan outlining the immediate steps to follow in the event of an attack.
- Concerns around employees ignoring corporate security advice and attacks evolving beyond existing skillsets are among the worries keeping information technology decision makers (ITDMs) awake at night.



Insight #1:

Threats are outpacing security teams while vulnerabilities remain.



Having asked security professionals to rate their confidence in security solutions commonly deployed to protect data against the threat of ransomware, doubts remain over the ability of firms to mitigate attacks.

While responses suggest that organizations are taking a multi-layered approach to security, with several solutions acknowledged by more than half of respondents, no single solution garnered the confidence of more than three-quarters.

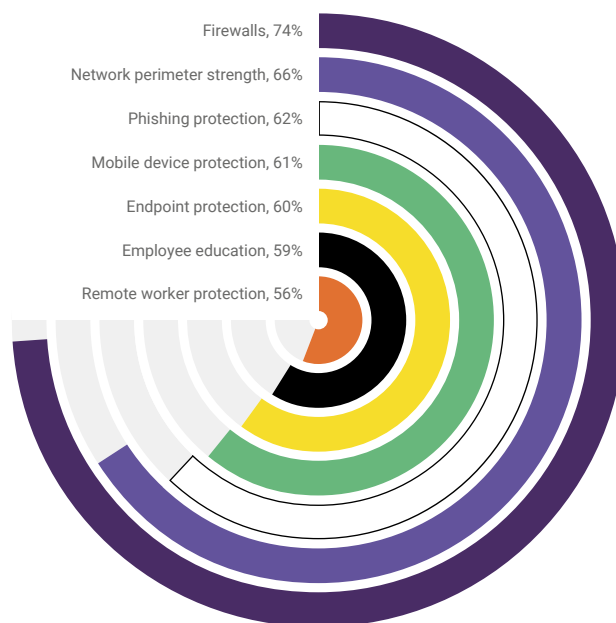
These doubts may stem from the belief that a series of weak links in the cybersecurity chain remain, with companies particularly concerned about the role of employees in facilitating cyberattacks. The fact that a notable proportion of firms that had been attacked were unable to identify where these had stemmed from equally highlights the need for progress.

Evolving threats (35%) and remote workers (34%) are the two greatest challenges organizations face when protecting against ransomware.

43% of organizations say employees are their weakest cybersecurity link.

17% of those targeted by a ransomware attack in the last 18 months were unable to identify how attackers got in.

With the solutions listed below, are you confident that your organization's data is protected against the threat of ransomware?





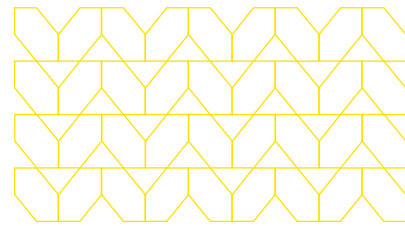
Insight #2:

Ransomware sources move beyond computer browser and email to include mobile devices.

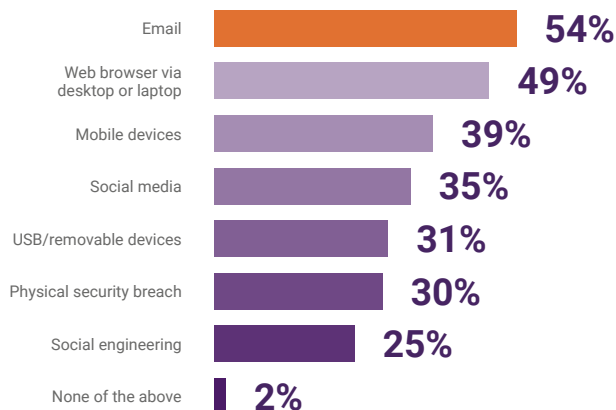
Mobile devices have joined email and desktop/laptop web browsers as one of the leading ransomware attack vectors facing organizations today.

Critically, mobile devices aren't typically managed by organizations. However, owing to the normalization of hybrid models and more flexible working habits, they are commonly used for work such as checking emails. Organizations must now consider unmanaged devices as part of their security strategy to mitigate these substantial threats.

Currently, there is greater confidence in legacy methods such as firewalls (74%) and network perimeter strength (66%) than more modern approaches such as mobile device protection (61%), endpoint protection (60%) and remote worker protection (56%) that are more effective in protecting against today's threats. This suggests that organizations need to urgently update and evolve, just as attackers continue to do.



In your opinion, what are the top 3 ransomware attack vectors that pose the biggest challenge to your organization?



Top ransomware attack vectors include email (54%), web browsers via a desktop or laptop (49%) and mobile devices (39%).

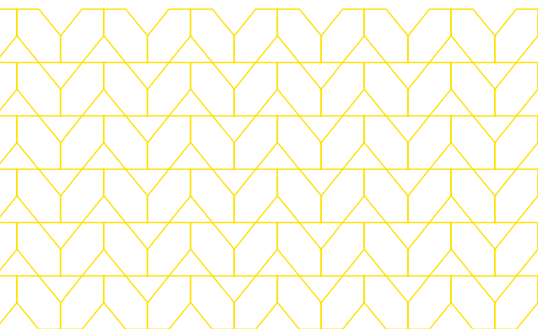
Firewalls (74%), network perimeter strength (66%) and phishing protection (62%) are seen as the top solutions for protecting against the threat of ransomware.





Insight #3:

Organizations lack knowledge/consensus in responding to ransomware attacks.



The transition to hybrid and remote working has expanded attack surfaces and exposed many new vulnerabilities, yet security has largely failed to adapt and properly serve these new operating environments. Organizations continue to rely on outdated technologies to mitigate HEAT attacks. From antivirus software to firewalls, many of the solutions deployed for on-prem environments a decade ago simply are not fit for purpose in dealing with modern cloud-based threats and defending against browser-led attacks.

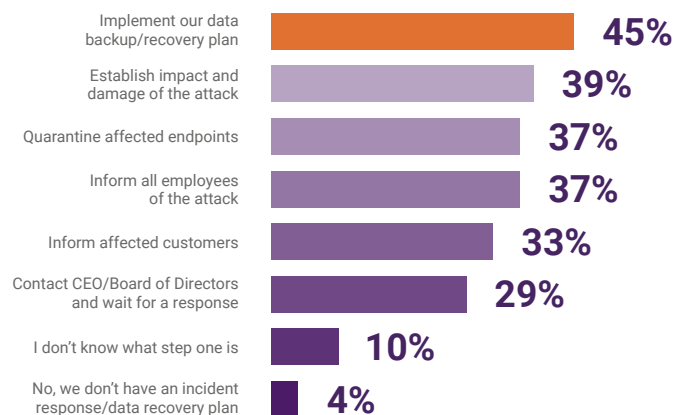


Almost one in 10 ITDMs don't know 'step one' in the event of a ransomware attack.

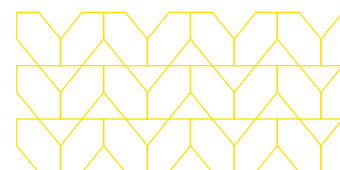


One in three decision makers worry about paying a ransom demand and not getting their data back, but 65% would still pay.

*In the event of a ransomware attack, do you have an incident response/data recovery plan?
If Yes, what is step one?*



There is also debate around how best to deal with ransomware demands. While nearly two-thirds (65%) of respondents would pay a ransomware demand, around a third (31%) say it's down to their insurance company to pay it, and nearly one in five (18%) say the government should pay. More than a quarter (27%) of respondents say they would never pay a ransomware demand.



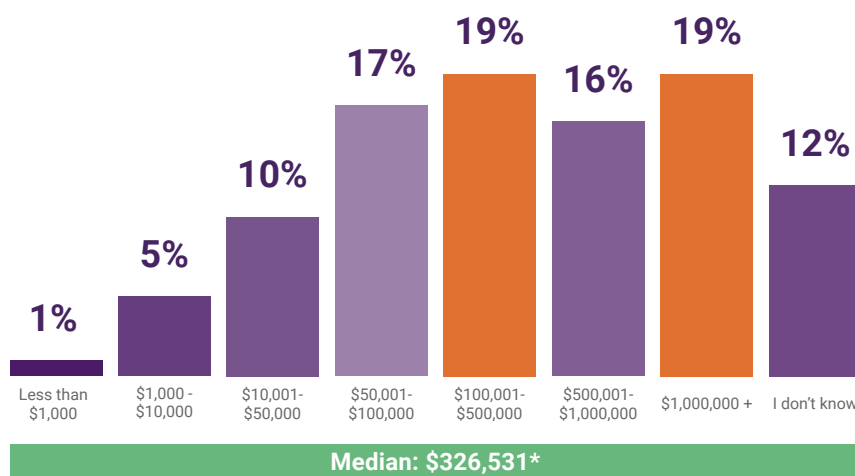
Insight #4:

Security professionals underestimate the cost of recovering from an attack.

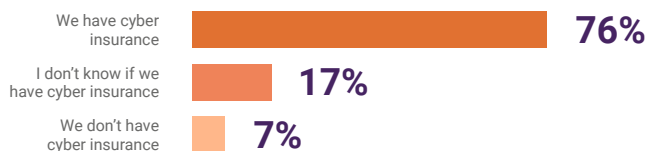
Industry figures suggest there is an alarming disparity between the perceived cost and actual cost of recovering from a ransomware attack among security professionals. The survey shows that the average perceived cost is \$326,531, with insurance payouts extending up to an average of \$555,971. However, [figures](#) show the average total cost of recovery from a ransomware attack in 2021 was \$1.4 million.

What do you think is the average cost of recovering from a ransomware attack?

The average cost of recovering from a ransomware attack is thought to be \$326,531, while the average value of cyber insurance cover is \$555,971.



Do you have cyber insurance, or business insurance, to cover a ransomware attack?



Almost one in four (24%) organizations either do not have or do not know if they have cyber insurance.

With current insurance payouts unable to cover even half of the average cost to recover from ransomware, many firms may be left on the brink of bankruptcy if they are hit. Further, it is perhaps more alarming that almost one in four organizations can't say with certainty that they have cyber insurance.

Almost one in four organizations either do not have or do not know if they have cyber insurance, rising to:

**31%**

of organizations with
10,000+ employees

**33%**

in the retail, leisure or
hospitality industry

**43%**

in government, local authorities
or other public sector bodies

CISOs face unprecedented pressure.

When asked what keeps them awake at night, 41% of respondents revealed that they worry about ransomware attacks evolving beyond their team's knowledge and skillset, while 39% worry about them evolving beyond their company's security capabilities.

Their biggest concern, however, is the risk of employees ignoring corporate security advice and clicking on links or attachments containing malware (46%). Respondents worry more about this than they do their own job security, with just a quarter (26%) of ITDMs concerned about losing their job.

Such worries are manifested in frustrations over the challenges that the IT industry currently faces when it comes to protecting organizations and employees against ransomware, from ransom demands increasing (29%), to the growth of RaaS (27%) and a feeling that government authorities are not treating ransomware seriously enough (26%).

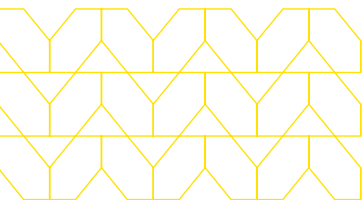
Continuing to operate on the frontline of cyber defenses and coming under huge levels of stress, it is little surprise that security decision makers are prioritizing the business's security over that of their own job. Indeed, the burnout and high churn rate of CISOs has been widely reported.

Such concerns are not conducive for an effective security environment. Current approaches therefore need to change, shifting towards empowering CISOs with the tools, technologies and solutions needed to reduce operational burdens and provide greater peace of mind, freeing up security leaders to focus on delivering high-value tasks effectively.

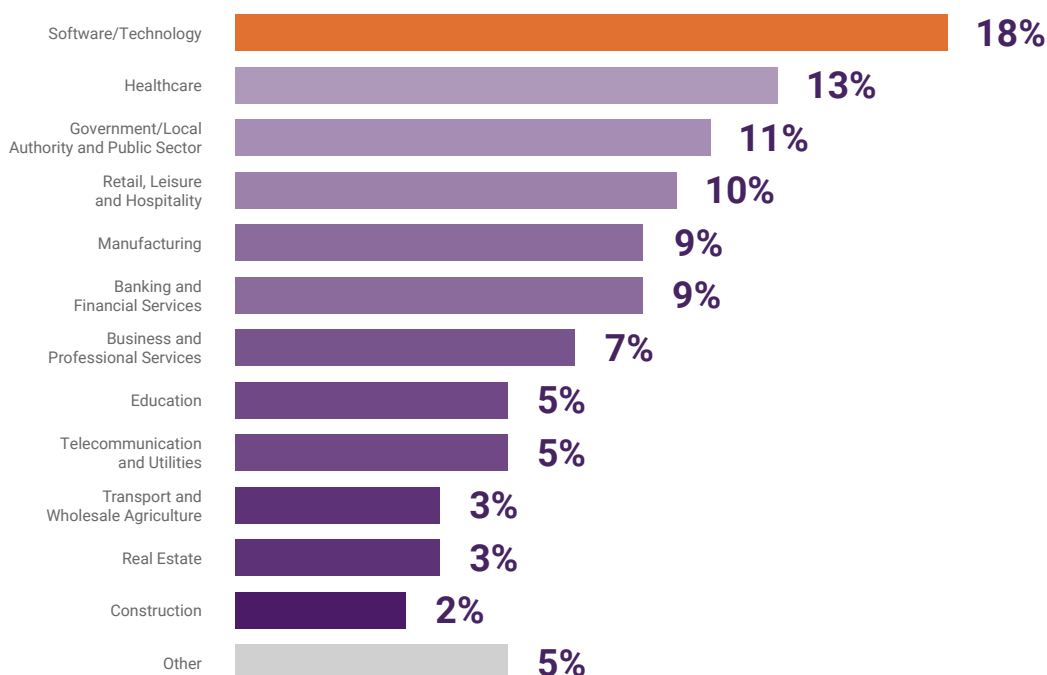
Learn more at www.menlosecurity.com



Methodology



Commissioned by Menlo Security, the research was conducted by SAPIO Research in June 2022 using an email invitation and online survey. The company surveyed 505 IT security decision makers working within organizations with 1,000+ employees across the US (251) and UK (254) – 61% at IT manager level and 39% at C-level. The top three business sectors were Software/Technology (18%), Healthcare (13%) and Government/Public Sector (11%). Results are accurate to ± 4.4 percent at 95 percent confidence limits.



To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com



About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by [major global businesses](#), including Fortune 500 companies, eight of the ten largest global financial services institutions, and large governmental institutions. Menlo Security is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Mountain View, California..

© 2022 Menlo Security. All Rights Reserved.