MENLO SECURITY

Prevention is security's best hope against ransomware.

IT security professionals would like to prevent ransomware attacks but still think in terms of detection and response.

REPORT

Simply put, ransomware attacks are on the rise and show no sign of letting up.

The accelerated move to the cloud, the suddenly remote workforce, a shift to hybrid work environments and the sustained disruption that forever changed the way organizations do business have created significant security gaps that ransomware gangs are eager to exploit.

The uptick in ransomware attacks — Southeast Asia alone has seen a 600 percent increase in cybercrime[1] — has galvanized governments around the globe to become increasingly security conscious, joining forces to shore up defenses against malicious actors. Singapore, for example, expanded its existing cooperation on cybersecurity[2] with the United States to include critical technologies as well as research and development, while South Korea's Ministry of Science and ICT is offering small businesses data encryption, backup and restoration systems so they can bring their systems back online after ransomware attacks.

Alarmed by a string of aggressive and damaging ransomware attacks against the likes of FUJIFILM's Tokyo operations and the IT infrastructure of the Asian arm of global insurance company AXA, IT decision makers similarly sprang into action, investing in safeguarding their organizations and building resiliency.

During a recent virtual event, Menlo Security surveyed attendees, which included more than 400 IT practitioners in APAC-based organizations, on their views of the ransomware threat and their strategic priorities to vanquish it. The results reveal an eagerness to prevent attacks with clear dissonance between intent and action.

Key Findings

- Almost all decision makers, 94.3 percent, are concerned about the serious threat ransomware poses to their organizations.
- More than half have been victims of a successful ransomware attack in the previous 12 months.
- Just over two-thirds believe their organizations will be the target of successful attacks in the next year.
- Of respondents, 74.03 percent say the focus of time and resources should be on preventative solutions, though more than half are investing in after-the-fact solutions aimed at detection and incident response.
- Perhaps warned off by reports of companies paying up only to be double-crossed by attackers, about half say they would refuse to pay ransom if successfully attacked.

1. *United Nations Office on Drug and Crime, Ransomware attacks, a growing threat that needs to be countered*
2. *Cyber Security Agency Singapore, Singapore and United States Expand Existing Cooperation on Cybersecurity*

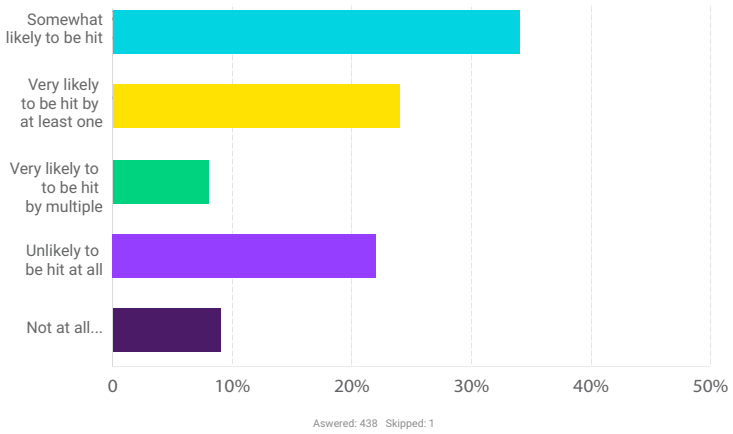
Insight #1:

The pace and aggressiveness of attacks have ramped up.

Ransomware gangs are leaving no stone unturned — regardless of size or industry, organizations can suddenly and without warning find themselves under siege, as cybercriminals and nation-states ramp up their efforts. And while the pandemic ushered in a new era of attacks with shifting techniques and aims, it seems that as the global pandemic wanes, the onslaught of ransomware will grow stronger as disruption and transformation of business continues. The introduction of new technology and a resulting lag in worker skills will only exacerbate security challenges and give attackers more opportunity for success.

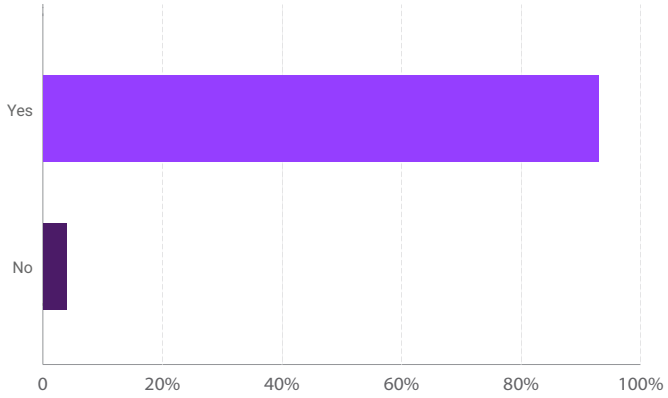
After a significant rise in attacks against companies big and small over the past two years, IT leaders have seen the writing on the wall — their organizations can't escape the crosshairs of ransomware gangs. Most, 68.27 percent, expect to be hit by at least one successful ransomware attack in the next 12 months and half of those are bracing for multiple attacks.

Which choice best describes your expectations for your organization to be hit by a successful ransomware attack in the next 12 months?



Aswered: 438 Skipped: 1

Do you believe ransomware poses a serious threat to your organization?



Aswered: 438 Skipped: 1

IT leaders agree: Ransomware attacks are inevitable and can do great damage. Regardless of company size or the industry served, nearly all decision makers, 94.06 percent, say their organizations are at serious risk from such attacks.

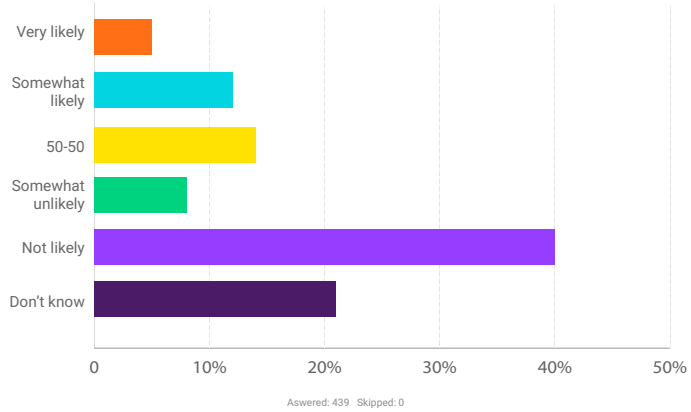
Insight #2:

Paying up is waning as a strategy for mitigating an attack.

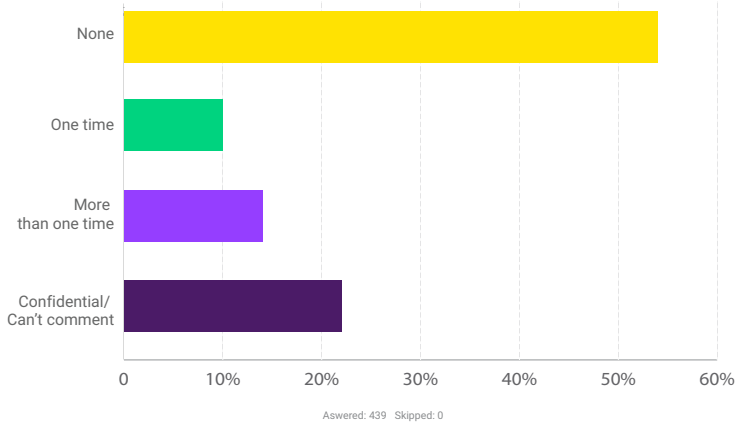
For all the high-profile reports of organizations paying ransom, making it part of a ransomware remediation, actually budgeting for it and even relying on insurance to cover the cost, ponying up to demands from malicious actors is a risky strategy. There is no guarantee that an organization will get its files back post-payment and gangs often come back for more, hitting the same company a second or third time. There is evidence, too, that payment just emboldens attackers to ply their trade elsewhere, perhaps with others in a victim's ecosystem.

For the majority (73 percent), at least 50 percent of their workforce is now working from home. Bucking a recent trend, half of decision makers will not pay a ransom if their organization falls victom to a ransomware attack, though just under 20 percent say paying up is a likely option and an almost equal number have no idea if they will pony up for a ransom demand.

Should your organization be hit by a successful ransomware attack in the next 12 months, what's the likelihood that your organization will pay the ransom?



How many times has your organization been affected by a successful ransomware attack in the last 12 months?



For well over half of respondents, the resolve not to pay has yet to be put to the test — nearly 54 percent say their organizations have not fallen prey to a successful ransomware attack in the year prior.

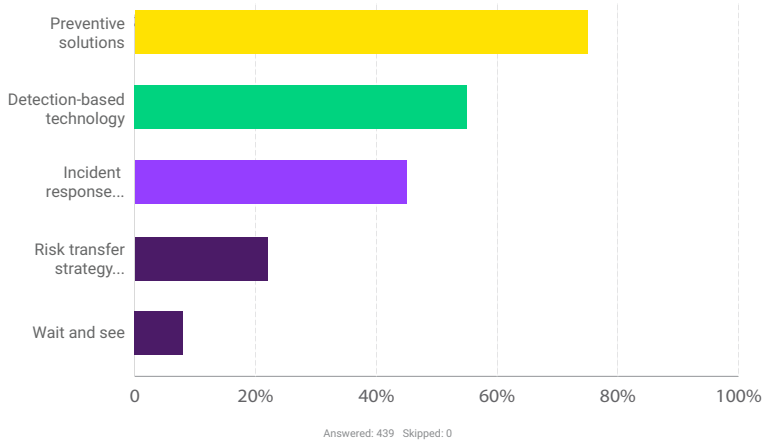
Insight #3:

Focus is on prevention, but investments in defensive measures run high.

As the idiom goes, an ounce of prevention is worth a pound of cure, and IT leaders are learning just how true that is when it comes to ransomware. They understand that preventing miscreants from getting into their systems can help them shake the defensive posture that so often characterizes security and will help protect their customers, partners and players in their supply chain from lateral attacks that ransomware actors are prone to make. Still, leaders revert to type, continuing to scoop up detection and incident response solutions that "protect" only after the fact.

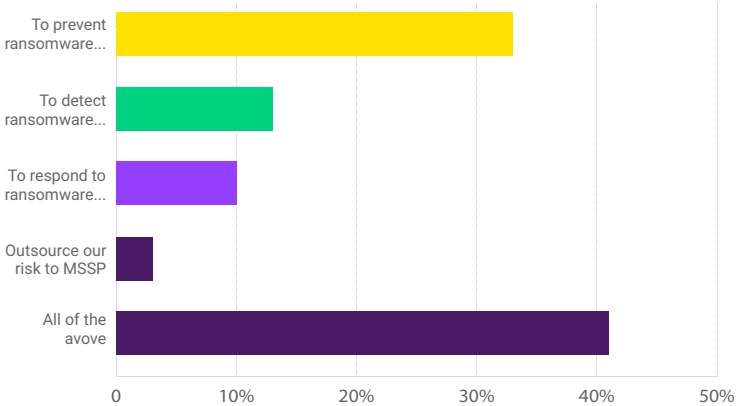
Leaders' beliefs are in the right place — 74.03 percent say organizations should invest in preventative solutions and measures — but their budgets are not. More than half, 56.25 percent, still put time and money toward detection, while 45.79 percent are investing in incident response.

Where do you believe organizations should focus their time and investments when it comes to combating ransomware?



Answered: 439 Skipped: 0

How would you classify your organization's security posture and strategy?

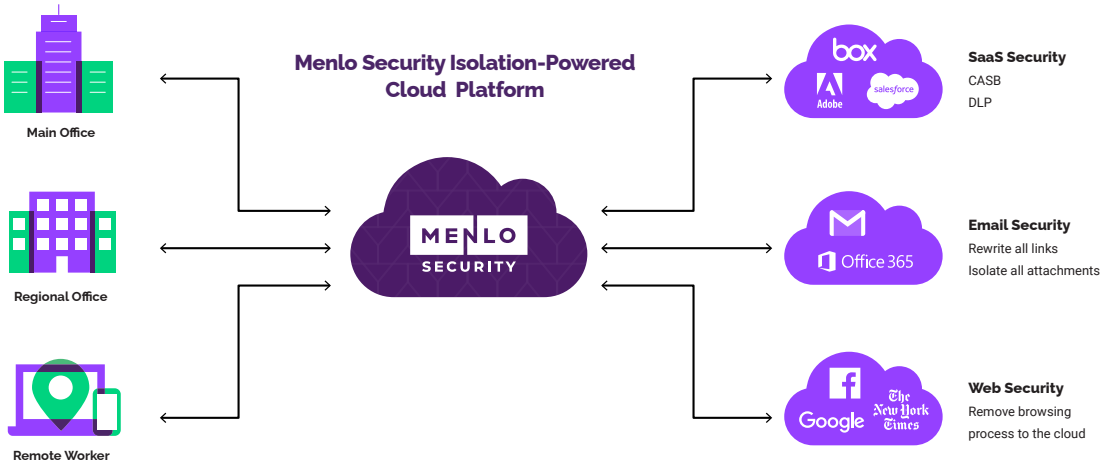


Answered: 439 Skipped: 0

While they clearly want to get out ahead of the dangerous antics of malicious actors, less than one-third of leaders, or 32.8 percent, believe their organizations are well-positioned to prevent attacks.

Prevent, don't react.

While no one would argue that detection and incident response measures are key elements of any security strategy, what if there was a way to keep malicious actors from penetrating systems in the first place? Endpoint protection is still necessary to protect organizations that are successfully penetrated by malicious actors, but what if miscreants could be kept out in the first place? Those organizations that move now to assume a preventative posture will greatly increase the odds that inevitable ransomware attacks won't succeed.



It's possible to shut the door on ransomware for good. Many organizations are doing this by taking a Zero Trust approach to cybersecurity. This is the only way an enterprise can make ransomware a distant memory. Coupled with isolation-powered security technology, a protective layer is created around users as they navigate the web, blocking not only known and existing threats, but unknown and future ones as well. Rather than responding to attacks after the fact, enterprises can prevent them from reaching users in the first place.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.