Comprehensive Cybersecurity Strategies Can Provide Confidence Against Threats

Introduction

Ransomware attacks are on the rise and inflicting an increasingly adverse impact on businesses — not only in the form of direct financial impact from the attacks but also from perceived threats that affect business strategy, budget priorities, and IT preparedness.

A recent Enterprise Strategy Group (ESG) report, co-sponsored by Zerto, found that ransomware has become a top concern for businesses and is being perceived as "an existential threat to the viability of any business." This points to the increasing need for businesses to adapt their internal strategies as the likelihood and complexity of cyberthreats increase and grow more dangerous.

It is natural for companies to start by building a robust prevention strategy focused on thwarting attacks. However, as attacks become more sophisticated and capable of breaching prevention measures, prioritizing recovery must be a key element of a modern, multi-layered approach. It's just as crucial as prevention, if not more, in the current threat environment.

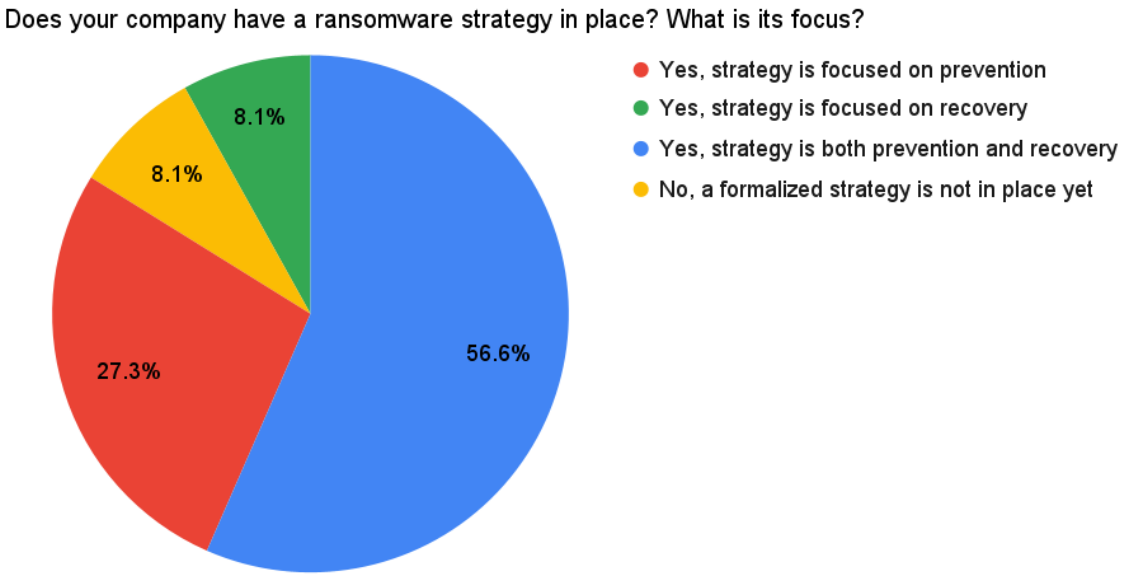
This survey sought to understand at a high level how companies view their security posture. Are they more invested in keeping malicious actors out, having the ability to recover their data in the event of a breach, or both? What steps do they take to mitigate the impacts of these attacks? In addition, respondents were asked their opinions on cyber insurance, another option for businesses to protect themselves against financial loss in the ransomware era.

What the survey found is that more than one third of companies still do not have a well-rounded, holistic ransomware strategy in place, and despite having many tools at their disposal, they are not getting what they need from their data protection and cyber resilience strategies. Because of that a majority of companies surveyed are reconsidering their solutions.

One in three companies still are not prioritizing recovery

The perceived and real threats of cyberattacks are why ransomware preparedness is part of most businesses' high-level strategy but how organizations approach their strategies varies. Alarmingly, more than one third (35.4%) of companies surveyed are not prioritizing recovery-. Add to that, as will be shown later, a clear majority are reevaluating their data protection solutions (66.2%) to strengthen their defenses, and we are seeing that protection, while important, is not a comprehensive solution strategy.

In all, just over half of the companies surveyed (56.6%) focus on both recovery *and* prevention. This indicates that a holistic view is far from widespread amongst those surveyed. As noted, over a third of respondents do not have a strategy in place that focuses on recovery at all. They either have a sole focus on prevention or, unfortunately, have no formalized strategy in place yet (8.1%). This is dangerous because, as ransomware actors become more capable of impounding data, businesses will suffer wide-ranging consequences if they cannot recover and get back up and running immediately on their own behalf.

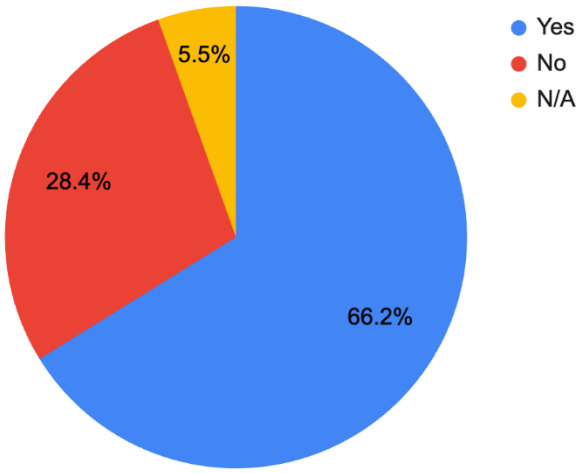


Reevaluating ransomware strategies: Companies continue to struggle

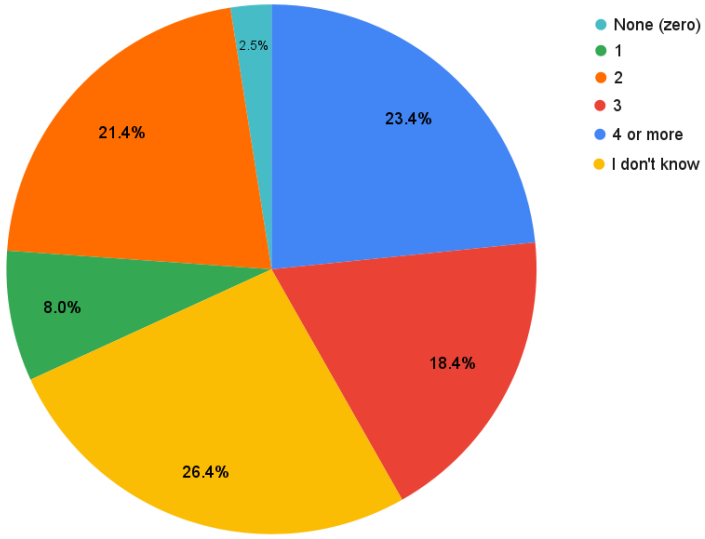
Ransomware can be combated with proper recovery strategies, but as the previous response indicated, not all companies have a formalized recovery strategy in place. The upside is that companies are reevaluating their data protection and cyber resilience strategies. In the survey, 66.2% deem their strategy in need of further examination; meanwhile, 28.4% are satisfied with the plans in place. This is a trend we've seen since last year when this same survey was conducted and 66.8% of respondents stated that they were reevaluating their data protection and cyber resilience strategies. With all the so-called, 'ransomware messaging fatigue' out there, companies are still struggling to align their priorities to match the threats they are facing.

The fact that companies are reevaluating strategies they have in place, especially considering that nearly two thirds (63.1%) of those surveyed have multiple data protection and ransomware detection tools at their disposal, signals that prevention is not enough and that legacy data protection falls short. As companies rethink their strategies, those that haven't yet put a focus on recovery will benefit by moving in the direction of continuous data protection, which offers a streaming set of thousands of recovery checkpoints that allows them to rewind to a time within seconds prior to an attack. It provides a peace-of-mind that operations can be restored quickly and effectively in the wake of a disruption.

Ransomware attacks have increased in volume and severity. As a result, are you re-evaluating your data protection or cyber resilience strategies and tools?



How many solutions does your organization use for data protection and ransomware detection?

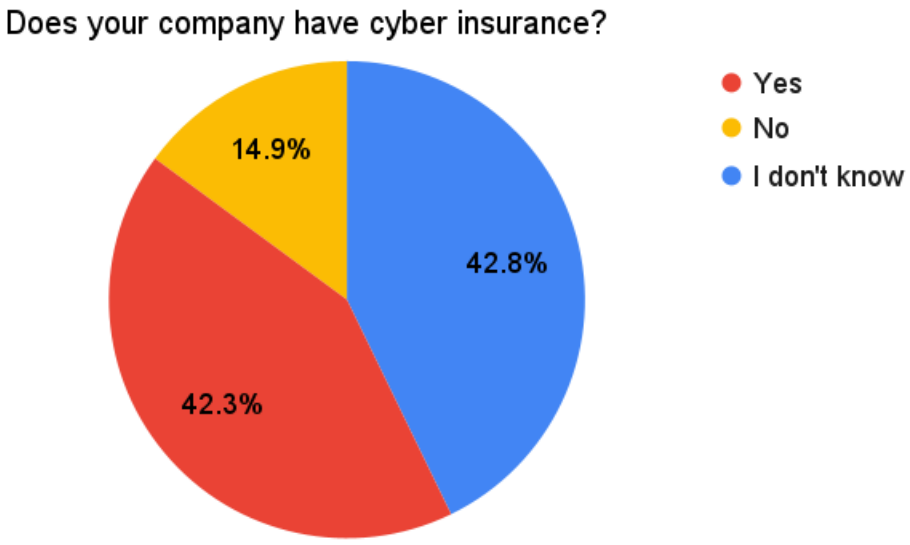


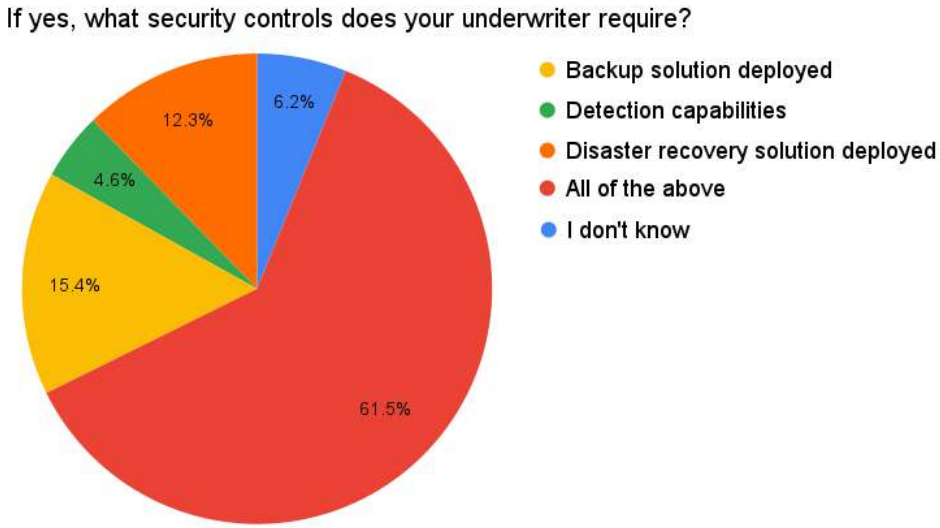
Cyber insurance requires a holistic approach

With the threat of ransomware being top of mind for so many, the concept of cyber insurance services was something this survey sought to better understand. More than 40% reported working for companies that utilized cyber insurance, while an almost equal amount did not know if their organization carried a cyber insurance policy. This leaves only 14.9% providing a definitive 'no' to having cyber insurance. This might point to the possibility that it remains a positive option that businesses are

evaluating but haven't fully embraced. It might also point to the fluidity of companies when it comes to their approach to cyber threats.

Of those that have cyber insurance, we found that they run up against a number of requirements to get policies approved. Insurance is a useful measure to offset the effects of ransomware, but it may not be available if your cyber strategy is not holistic. The survey found that for those utilizing cyber insurance, the underwriters that evaluate applicants require backup, disaster recovery, detection, and data vault capabilities to approve policies. This shows that those who are in the business of financially protecting against ransomware threats require policy holders to protect their data in a comprehensive fashion.





Wrap up

In an era of relentless cyberthreats, strategies to combat attacks can't remain idle, and they must be multi-dimensional. One solution that companies are considering is isolated cyber vaults that can employ a secure architecture to protect data and thwart ransomware. To elaborate, in this survey, it was found that respondents preferred an on-premises cyber vault to one in the cloud by a margin of three to one, pointing to the future of data protection as being one that includes cyber vaults as a key part of any organization's ransomware resilience strategy. Cyber insurance policies, local and federal regulatory bodies, and industry associations are increasingly requiring fully separated data vaults that cannot be infected by ransomware. These options of last resort are critical during large-scale ransomware attacks.

Cyberattackers have proven that they can breach fortified security structures, so companies need a plan in place for what to do once bad actors are in. If the goal is to keep business running and operating, a recovery strategy is required. It's positive that many companies have multifaceted strategies in place, but completely protecting the business requires recovery capabilities.

To that point, it's encouraging to see that organizations are reevaluating their ransomware strategies. For companies that have not put a focus on recovery, this is a step in the right direction toward a more holistic ransomware strategy. Organizations should not rely on protection alone. That is a risk that can't be alleviated by insurance or preventative measures and is not worth taking.

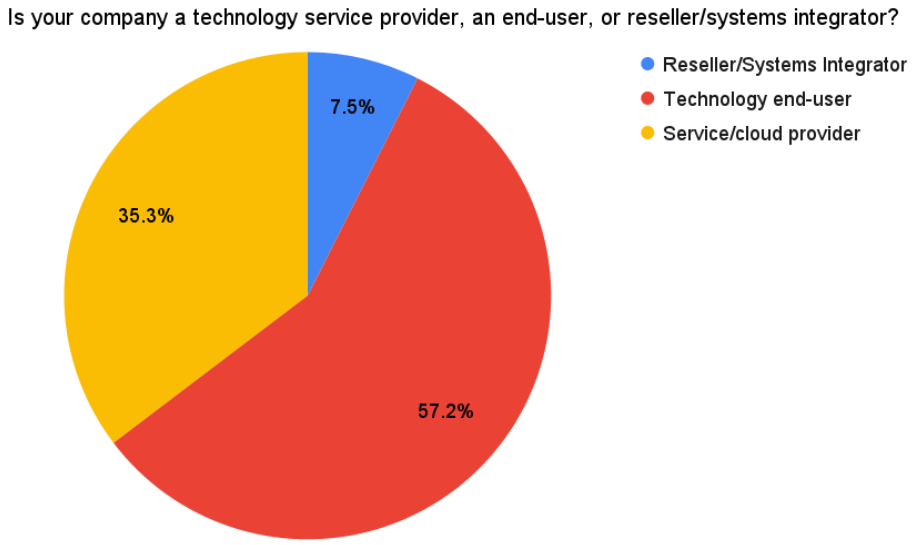
Methodology

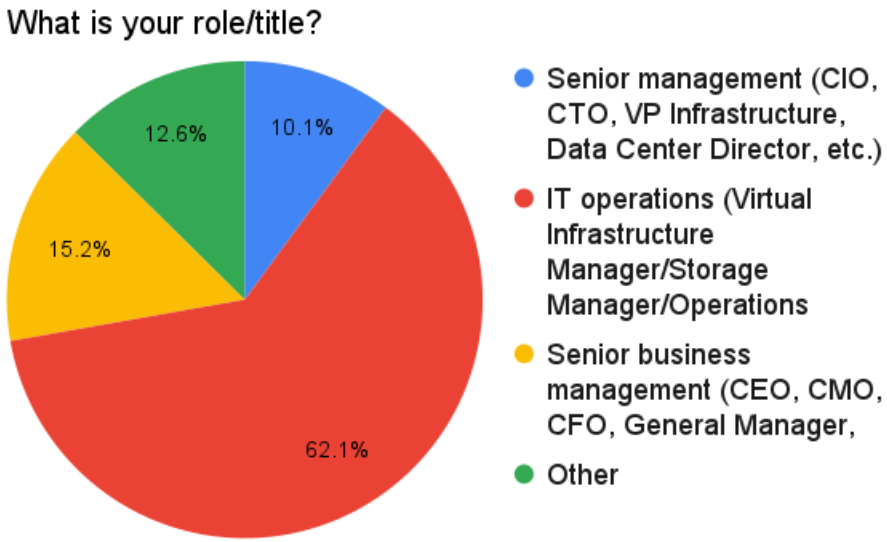
The research team surveyed 201 people in-person at VMware Explore in Las Vegas, August 26 to 29, 2023. All respondents were attendees of the VMware Explore conference. All data was collected over

three days. Responses were recorded anonymously, but company and job/title information were collected.

Respondents

The survey received 201 responses primarily from end users, service providers, and resellers (92%). Across those groups, 94% of respondents had experience working with corporate IT. This indicates that both groups held an in-depth, personal understanding of data protection strategies.





About Zerto

Zerto, a Hewlett Packard Enterprise company, empowers customers to run an always-on business by simplifying the protection, recovery, and mobility of on-premises and cloud applications. Zerto eliminates the risks and complexity of modernization and cloud adoption across private, public, and hybrid deployments. The simple, software-only solution uses continuous data protection at scale to solve for ransomware resilience, disaster recovery and multi-cloud mobility. Zerto is trusted by over 9,500 customers globally and is powering offerings for Google Cloud, IBM Cloud, Microsoft Azure, Oracle Cloud, and more than 350 managed service providers.

###