Filling the Gap: The Need for Comprehensive Cybersecurity Strategies

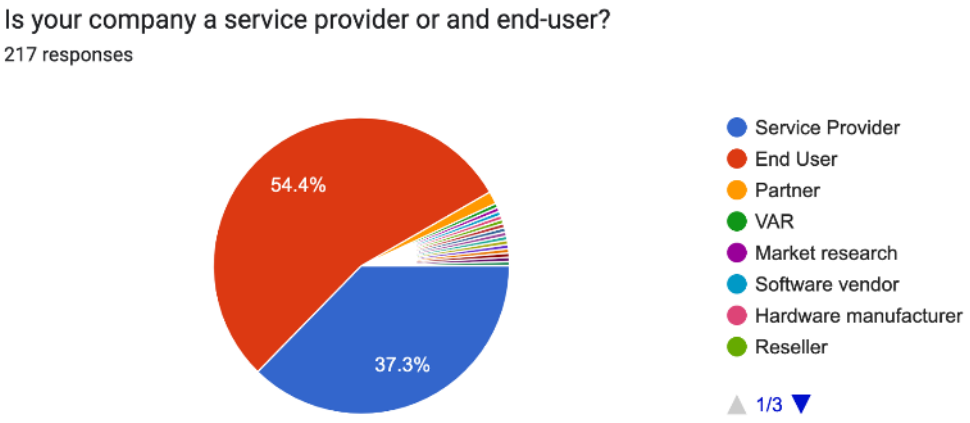
Intro

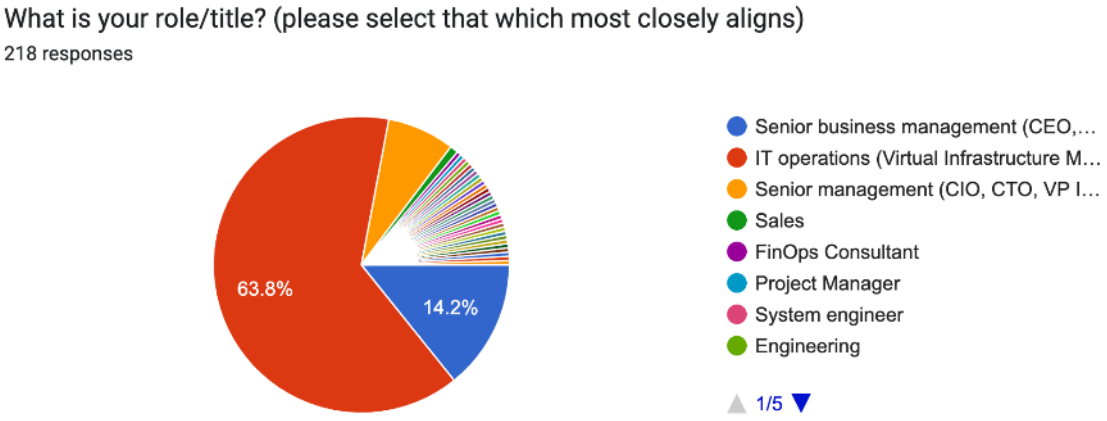
Every company relies on data to perform day-to-day operations. Business can't function without it, so it's important to adapt internal strategies as new cyberthreats and challenges emerge or existing data threats grow more dangerous. Most companies correctly start by building a robust prevention strategy focused on thwarting attacks. However, as attacks become more sophisticated and capable of breaching prevention security, prioritizing recovery must be a key part of a modern, multi-layered approach.

This survey sought to understand, at a high level, how companies view their security posture. Are they invested in keeping malicious actors out, having the ability to recover their data in the event of a breach, or both?

Respondents

The survey received responses primarily from end users and service providers (92%). Across those groups, 87% of respondents had experience working with corporate IT. This indicates that both groups held an in-depth, personal understanding of data protection strategies.

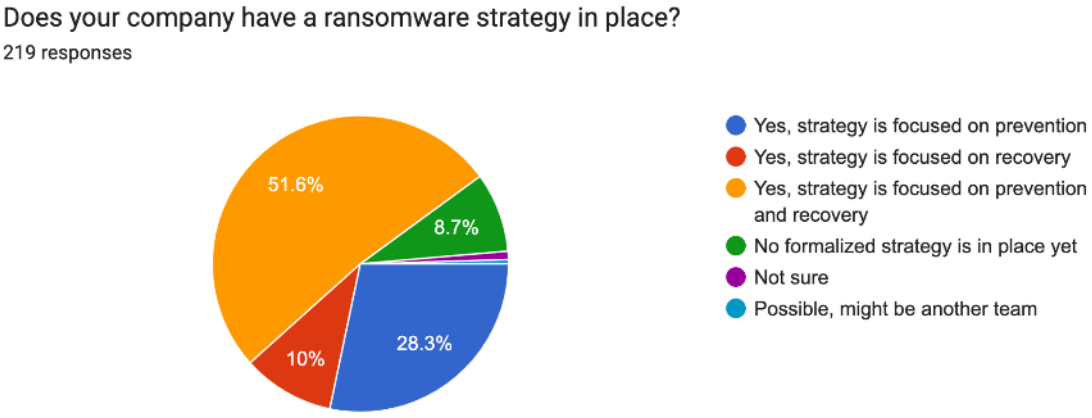




Ransomware strategies as they are

Ransomware can impact a business in many ways. As found in a recent IDC report, sponsored by Zerto, the impact of these attacks is extensive. The cost to people can be high with employee overtime, lost employee productivity, the direct cost of recovery (i.e., the engagement of consultants or specialists), and unrecoverable data being notable issues. However, there are even more significant impacts like lost revenue, damaged company reputation, and permanent loss of customers.

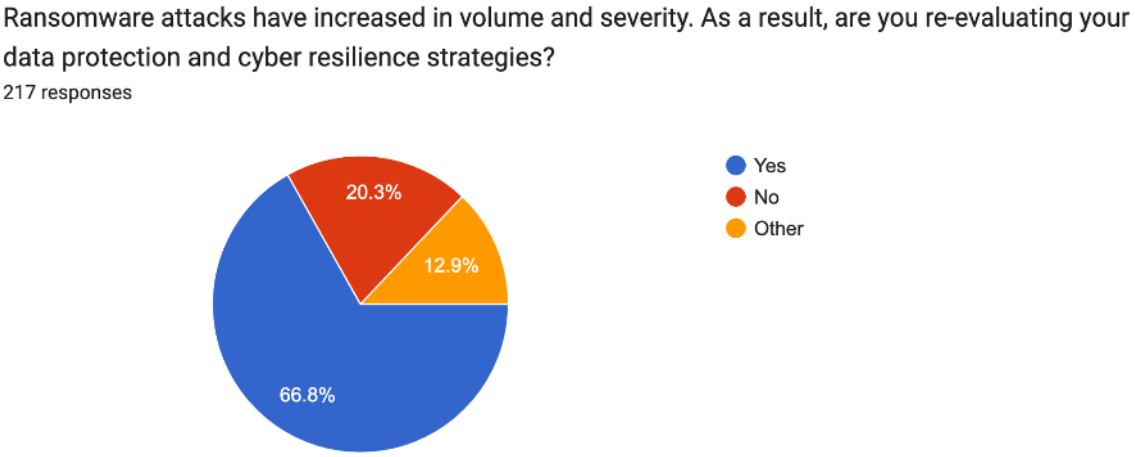
That is why cyberthreats are part of most businesses' high-level strategy, but how organizations prepare for them varies. Only half of the companies surveyed focus on both recovery *and* prevention. This indicates that a holistic view is far from the norm amongst those surveyed. Interestingly, over a third of respondents (37%) do not have a strategy in place that focuses on recovery. They either have a sole focus on prevention or, alarmingly, have no formalized strategy in place yet (8.7%). This is dangerous because as ransomware actors become more capable of impounding data, businesses will suffer wide-ranging consequences if they can't get back up and running immediately on their own behalf.



Reevaluating ransomware strategies

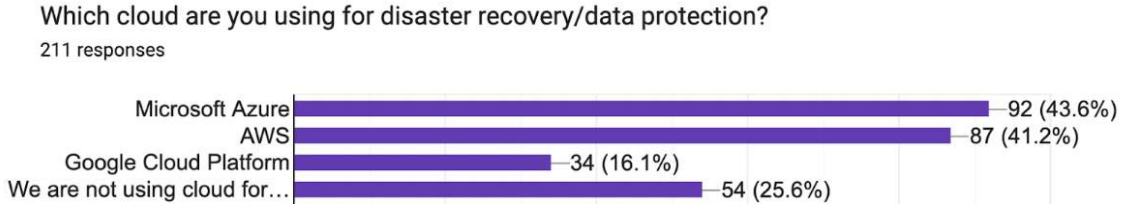
Ransomware can be combated with proper recovery strategies, but as the previous response indicated, not all companies have a formalized recovery strategy in place. The upside is that companies are reevaluating their data protection and cyber resilience strategies. In the survey, 66.8% deem their strategy in need of further examination; meanwhile, 20% are satisfied with the plans in place.

It's concerning that two-thirds of respondents indicated they aren't comfortable with what they have in place—especially considering the current cyberthreat landscape. This may signal that prevention is not enough and that legacy data protection is failing. As companies reevaluate their strategies, those that haven't yet put a focus on recovery will benefit by leaning in the direction of continuous data protection, which offers a continuous stream of recovery checkpoints that allow them to rewind to a time within seconds prior to an attack.



Using cloud as part of disaster recovery/data protection strategy

Nearly three-quarters (74.4%) of respondents are using cloud as part of their disaster recovery (DR)/data protection strategy. This points to the recognition of security in the cloud. Certainly, DR in the cloud is cost effective and simple to use, and it opens the door to cloud adoption as companies can off load on-premises preccesse to the cloud.



Methodology

The research team surveyed 220 people in person at VMware Explore in San Francisco, August 29 to 31, 2022. All were attendees of the VMware Explore conference. All data was collected in a span of three days. Responses were recorded anonymously, but company and job/title information was collected.

Wrap up

In an era of relentless cyberthreats, strategies to combat attacks can't remain idle, and they must be multi dimensional. Cyber attackers 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 a 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 not worth taking.

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.