Podcast Title: HCLTech and Cohesity Supercharging Cyber Resilience Together

Host and moderator: Avinash Agarwal, Sr. Product Marketing Manager, Cohesity
Speakers: Kapil Tiwari, General Manager-PMG, Hybrid cloud Business Unit, HCLTech and Haris Shah, Global Technical Account Manager, Cohesity

The volume and value of business data has increased exponentially over the years. This is has given an opportunity to innovators and enterprise leaders to extract insights from data and use these insights to empower companies and industry transformations.

But at the same time, cybercriminals are exploiting digital information for significant gains.

Having said that, we'd like to start today's podcast with Kapil and Haris. So, my first question is to you Kapil. As per you, what are the key data security and management challenges that your customers face during their digital transformation journey?

Thank you for the warm introduction, Avinash. It's' great be here. So, to answer your question, let me begin by saying that today, cloud is driving the business transformation journey for most organizations across the world. And why not…by moving systems to the cloud, enterprises enjoy the benefits of agility, cost effectiveness, collaboration and accelerated time to market.

So, this cloud-first thinking has been truly transformational.

But as you rightly mentioned, it has also introduced fresh concerns regarding data that enterprises need to address if they want regular gains. Here's the obvious reason: increased cloud adoption has led to data fragmentation. After all, adopting multiple clouds means multiple systems in multiple locations, multiple regions where your data is generated and stored.

Now for all the benefits of a new cloud model, old-fashioned data silos can be hard (and costly) to manage, analyze and protect. And now we're experiencing a new hybrid work reality, post pandemic era, which is increasing cyberthreats and compliance requirements than ever before.

Also, want to highlight that the digital transformation journey exposes customers to potential cyber threats. The increased connectivity and reliance on digital platforms create opportunities for cybercriminals to exploit vulnerabilities and gain unauthorized access to customer data.

Also, want to highlight the challenges related to data recovery, something that's really important to point out here. For example, the increase in the scale of data which has made it difficult to optimize and restore large and critical data pools, which is obviously increasing the burden on IT budgets.

And Haris, what do you feel about Kapil's views? Do you also see the similar challenges with your customers too?

Thanks, Avinash. Well, I totally echo with what Kapil mentioned. What we see is that enterprises are looking to rapidly transition from legacy data protection solutions to a modern Data security and management solution, the reason is the outdated legacy products are creating major roadblocks in their transformation journey.

As we have recently seen that organizations are struggling in adapting legacy protections to prevent cybercriminals from exploiting both traditional and modern data sources such as databases, cloud-native apps, and containers. They're also facing the challenge of determining the optimum way to incorporate artificial intelligence and machine learning (AI/ML) technologies for more proactive threat detection.

To overcome these obstacles—we need to look at new frameworks and solutions.

Now, for achieving a high degree of data isolation, the conventional 3-2-1 air gap model results in slow recovery times when you're experiencing a cyberattack. And this negatively impacts your recovery service-level agreements (SLAs).

Don't forget that the failure to meet SLAs can damage your company's reputation, even if your business can successfully retrieve all its data. So, enterprises that are looking to increase the security of their data and backup solutions through data vaulting, these enterprises face the dual challenge of protecting not only data, but also improving agility to meet recovery SLAs. .

Thanks a lot for telling us about the depth of these challenges, Harish. So, that compels me to ask that how does HCLTech VaultNXT powered by Cohesity is helping customers become cyber resilient here?

Sure, Avinash. See, VaultNXT is an end-to-end cyber recovery solution that protects and recovers enterprise data against ransomware attacks.

This framework helps you strengthen your overall cyber resilience posture. So, it acts as the last line of defense…and safeguards business-critical data.

And **this** enables you to leap from threat detection to a **holistic** cybersecurity strategy.

I'll explain a bit more on how this works.

You see, VaultNXT strengthens data protection while boosting agility. It integrates modern Cohesity data security and data management platform, with HCLTech's proven assessment, consulting and build services, and ongoing operations—for end-to-end cyber recovery.

There are a few more things which our audience should know in this direction, which is that…

VaultNXT powered by Cohesity, also empowers enterprises to transition from disjointed threat prevention approaches to a holistic cyber security strategy.

And we have like more than 500 trained skilled resources support this effort. So, these resources, they assess the objective of your enterprise and its current maturity against cybersecurity threats to formulate, build and support the end operations of customer environment.

Our experts and consultants help enterprises chose flexible service options through the VaultNXT framework, so you know enterprises can develop a customized cyber-resilient architecture that is driven by the Cohesity Data Cloud platform—which furnishes you with robust data protection and management solutions.

Perfect, and if you can through some more light on this framework, how exactly it works and how it benefits the customers.

Sure, I'll cover this in brief, it has primary three main key towers that I'm explaining here.

The **first** is its ability to assess.

This includes the consulting and discovery of the customer infrastructure and understanding of their overall environment to identify the risks and governance associated with their business objectives, and conducting end-to-end assessments and planning of their environment. Outcome of this is going to help in the designing and building the solution.

So, we're talking about benefits such as finalizing the solution design, designing security and processes, and identifying the end-to-end cyber recovery process. So that's the more about the build solution phase.

Finally, the third is VaultNXT's ability to help you operate things. So, when we say this, we're talking about the execution of test and recovery plans, monitoring and reporting, and performing breach simulation.

Awesome. That's really sounds interesting, but why Cohesity? What do you think is unique about this partnership with Cohesity?

I think there are a lot of factors involved. So, Cohesity is not a new partner. We've been working with their ecosystem to make digital transformation a reality for our customers.

And our partnership with Cohesity helps our customers accelerate their digital transformation initiatives in the face of rising data volumes and cyberattacks. Cyberattacks which have, you know, compelled organizations to rethink the role of data and data management solutions.

Now when we speak to our customers, they tell us that they want modern and cloud-native data protection and management solutions. And, we see that Cohesity ticks all the boxes there.

Most importantly…

Cohesity supports seamless solution integration. Add the flexibility and scalability that it brings, which make it super easy to integrate with our various solution frameworks.

Of course, there're– three key points I really want to highlight here;

First - As Cohesity is built for cloud. So, it helps you adopt a cloud-centric and digital-first operating model.

Second- It provides you with simplicity at scale while reducing your business cost.

And third and the most important is that it's based on Zero Trust security principles to protect, detect and defend data from ransomware threats.

Sounds great, Kapil. Now when you've said this, are there any real customer stories that you can share with us. Haris, if you could answer that for us, you know, without naming the customer.

So, we have a joint customer, who's a leading Swiss insurance service provider, who I'd like to mention here. The best part is that they're already benefiting from our joint VaultNXT solution.

I mean before they had VaultNXT, they were facing a number of challenges: around modernizing their legacy data backups, you would be surprised to know that they had five different backup vendors in their datacentre and they had challenges around deploying strategy for their future workload protections, and most importantly adding ransomware recovery capabilities to their existing multi-vendor environment, everything was a challenge for them. And it was eating up their time, energy and money.

So we reached out to them and proposed a unified data protection and cyber recovery vault solution, in a flexible consumption model.

This simple, secure, and scalable solution helped the Swiss insurer simplify its approach to modernize and consolidate their secondary data landscape and strengthen the security

posture through immutable air-gapped vault, along with adding end-to-end ransomware protection capabilities.

As a result, they benefitted at multiple fronts:

- Improved RPO / RTO
- Significant reduction in data management costs, and
- Achieved faster restoration of data

Wow, that's an awesome story. And I believe that it'll definitely help a lot of listeners better understand how HCLTech VaultNXT can help them in their transformation journey.

With this, I'd like to conclude this podcast.
Thanks, Kapil and Haris for joining me and contributing to today's episode. It was a pleasure discussing with you the data security challenges that we see around in these times, how VaultNXT, powered by Cohesity, kind of empowers us in this direction.

I hope that our listeners got some real great insights from this episode. And it benefits them in supercharging cyber resiliency.
So, that's it from this episode of podcast on a such a critical topic. Of course, if you want to learn more about our joint solutions and capabilities, feel free to visit our websites—www.hcltech.com or www.cohesity.com.

Till then, have a good day. And keep listening to us.