



CIONET UK • SEPTEMBER 2026

Beyond Cyber Security

Data Integrity, Resiliency,
and the Modern Enterprise

Part II

AN EXECUTIVE ROUNDTABLE

In association with Hitachi Vantara

For the second time this year, CIONET and Hitachi Vantara brought a group of senior IT and security professions together to explore the needs of their organisations, and to assess how those needs are changing over time.

At an event in July, attendees shared best practice advice, the merits of disaster recovery (described by one as the “Cinderella” service), and the impact of artificial intelligence (AI). During that discussion, another guest commended the application of AI during recovery because the technology removes the “emotion” from what can be a very fraught process.

Now, a late September executive roundtable allowed a second set of senior technology leaders to pick up those themes and move the conversation on. Here are some key takeaways.

All about recovery

Or rather, recoveries. Because recovery isn't a single event, nor is it applied to a single team. That means it is time, attendees were advised, to reconsider the recovery challenge and to be sceptical of vendors that offer simple solutions. Red flags should be raised if you are told that compromised data store can simply “return to production” or that “we'll recover it into the cloud” given “a shotgun cloud recovery is very unlikely to succeed.”

●

“a shotgun cloud recovery is very unlikely to succeed.”

When planning for an attack, assess what a minimal viable business would look like and ensure that the data you cannot do without is available, as back up, in immutable form. Assess, too, what constitutes an acceptable length of outage and work backwards from there in your recovery planning process. As you do so, acknowledge that there are likely to be six or seven teams (including compliance and legal) intimately involved in the recovery process. And remember, too, that a minimal viable business is likely to comprise hundreds of copies of data.

Testing, testing

Good recovery is dependent on a good, consistent, and regular testing regime. Testing might be a yearly exercise or a monthly exercise. The more you do it, however, the more pushback you are likely to get from your teams not persuaded by the benefits of additional work. To counter any resistant, security leaders should point to real life examples of cyberattacks, not necessarily within their own organisation but elsewhere, too. The impact of those attack and, more importantly, the ongoing work required post-attack should focus minds, argued one attendee.

Greater regularity of testing raises poses another question. Namely, in an era in which AI constantly alters the threat landscape what value does a monthly test provide? It is, argued one voice, little more than a “point in time”, out of date as soon as it is performed. To emphasise the dilemma, another attendee highlighted a noticeable reduction in air gapping as a means of security. The prevalence and persistence of artificial intelligence (AI) as applied to an organisation's attack surface renders even the shortest period of air gapping redundant.

In the spirit of finding solutions, another voice advocated that security professionals focus on what really matters. In other words, he said, identify five

most likely vulnerabilities and make those your priority.

The ‘human’ threat of AI

Many organisations around the table are still contemplating how best to combat the threat of AI. Few have a fixed approach, perhaps reflecting the relative immaturity of generative AI adoption. In the arms of a bad actor, AI vastly increases the volume of attacks and, potentially, adds a level of sophistication, too.

...treat AI models and agents as insider threats...

Meanwhile, AI deployed within an organisation—large language models and agents, alike—poses another threat if and when it becomes compromised. To address the danger, organisations need to stop treating this “non-deterministic” technology as “code”. Instead, treat AI models and agents as insider threats and apply the same behavioural metrics and vetting processes as you would when onboarding and overseeing a new member of the team.

Asked how AI can be the friend, not just the enemy, of the security professional, attendees pointed to its use in accelerating and expanding threat intelligence, creating comprehensive documentation of new and existing systems and environments, and in expanding employee awareness through the creation of more and more sophisticated (and targeted) phishing emails to test on the wider organisation.

Resilience in a time of flux

When one organisation is absorbing the people, processes, and technology of another post-merger or post-acquisition, cyber security, data integrity, and operational resilience are put at risk. “Discontinuity means something often fall between the gaps,” noted one attendee. Throw in the impact of AI which is escalating external attacks, and the risks intensify.

During periods of big change, due diligence must come to the fore. Similarly, companies absorbing another organisation’s technology stack must be confident in applying existing security frameworks, lean into secure-by-design principles, and quickly expand their monitoring capabilities. Another attendee had raised the challenge of dealing with “third, fourth, and fifth party risk”. When it comes to external parties, similar remedies apply.

Chaos theory. Redux

Returning to the merits of testing, two voices recommended deliberate disorder as a means of ensuring the regime remains challenging. One invoked Chaos Monkey, a tool designed to test system resilience and fault tolerance by randomly terminating production instances. By simulating unexpected failures, the tool is deployed to help organisations uncover and address potential weaknesses before they result in real-world outages.

In a similar spirit, a second voice warned against running tests on a weekday morning when the “A team” will inevitably be in the office. Instead, choose a day when half the team is absent in order to expose gaps in processes and to identify instances of tribal knowledge: the undocumented, unwritten information which—when unavailable to all—jeopardises recovery.

Those truly committed to implementing this form of chaos—and willing to lose the friendship of their team in the process—might even consider the random Christmas Day test.

Beyond Cyber Security: Data Integrity, Resiliency, and the Modern Enterprise—a CIONET executive roundtable in association with Hitachi Vantara—took place on Wednesday 30 September 2026 at South Place Hotel, London.



cionet.com