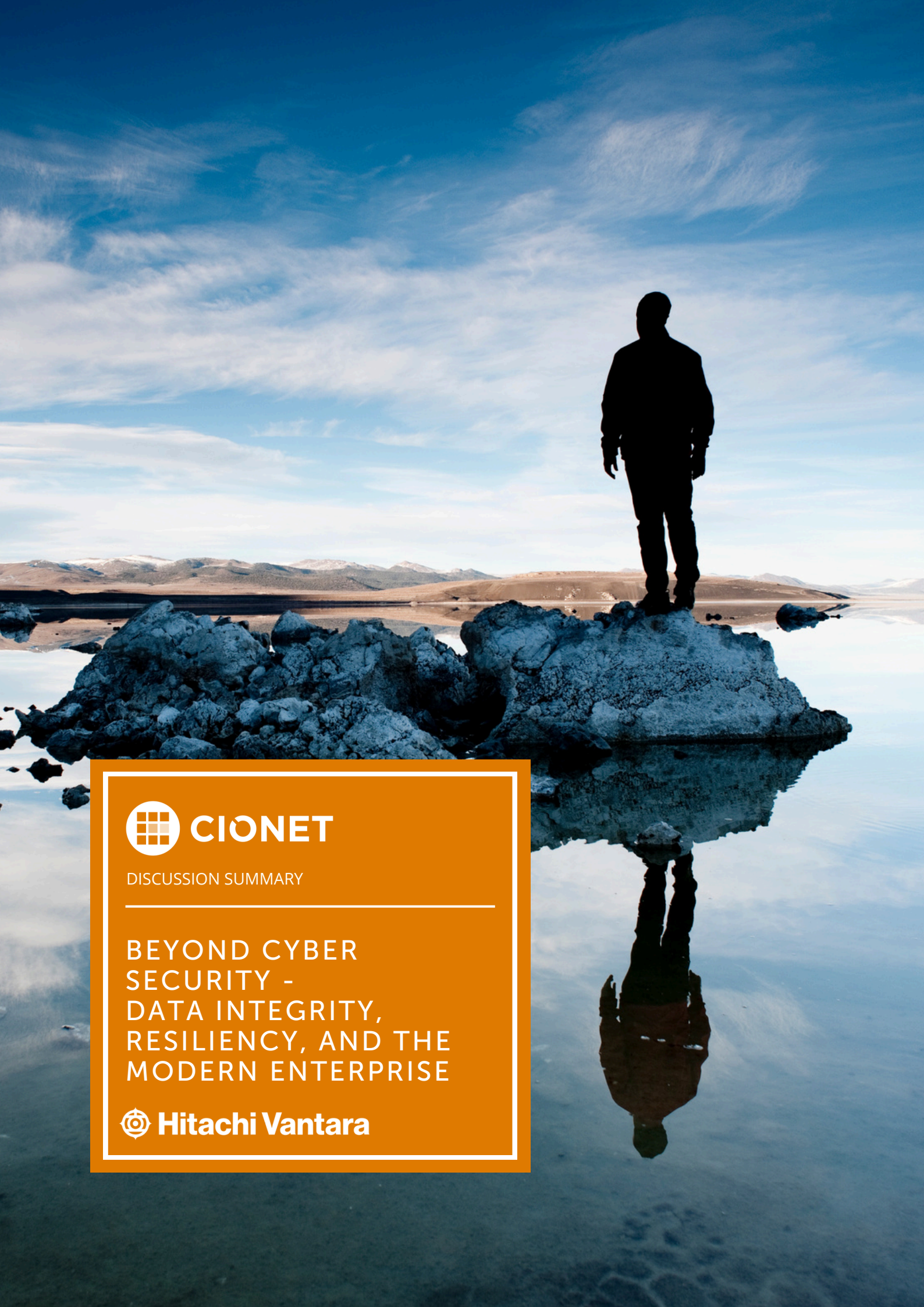

CIONET

DISCUSSION SUMMARY

BEYOND CYBER SECURITY - DATA INTEGRITY, RESILIENCY, AND THE MODERN ENTERPRISE

Hitachi Vantara

For today's organisations, cyber threats such as ransomware remain top concerns but resilience goes beyond security. It's about ensuring data availability and integrity even during moments of disruption. It's about planning and recovery. It's about continuity in times of crisis.

In this mid-July executive roundtable from CIONET and Hitachi Vantara, senior IT and security professionals explored how to embed resilience into the modern enterprise. Among the issues up for discussion were ways of identifying risk and responding to attack, the importance of data integrity as much as data protection, and immutable storage among other technology solutions enhancing speed of recovery.

Here are some of the main takeaways from a night of lively discussion and professional insights.

Disaster recovery: the 'Cinderella' service

More than one voice around the roundtable observed how disaster recovery (DR) has been sidelined by organisations more interested in implementing the latest cyber tools, always "shiny" and increasingly AI-derived. While DR – broadly defined as putting in place a set of practices for restoring access to IT infrastructure and critical business data following a catastrophic event – might appear a fundamental building block of resilience, many organisations appear reluctant to commit. Indeed, many are only convinced of the importance of DR when the consequences of downtime are experienced close at hand. Or to put it another way, only once disaster strikes.

Moreover, even organisations that claim to have a DR plan in place are giving insufficient thought to how that process would work in practice. For example, argued one voice around the table, those that insist that they will "recover back to production" or "recover back to the cloud" are failing to recognise the consequences of their choices. Both options should raise a "red flag". The former because any organisation operating in a regulated industry is going to experience a significant period offline while they satisfy the regulator that their data is "clean". Naturally, the downtime will have material commercial consequences. The latter because cloud means a "bunch of different things" – private cloud, hyperscalers, infrastructure as a service, software as a service – and that any of these often prove difficult and time consuming to return to operational health.

Consider, too, that a notional minimum viable business might be made up of 50 applications. To get those back into production, even with serviceable back up in place, is likely to take the best part of a month.

Another attendee urged organisations to make sure that DR planning aligned with an active business continuity strategy. The two should work in tandem. Senior executives must be fully cognisant of the consequences of downtime and ask themselves how long their business will last without key systems in place. Some downtime is an almost inevitable consequence of a successful attack however effective a DR plan might prove.

AI: enemy or friend of cyber security and resilience?

One organisation represented around the table observed that the volume and sophistication of attacks on her business have increased dramatically over the last 12 months or so. She put this down to "programmatic attacks driven by AI". Asked about increased sophistication, she noted how generative AI tools allow bad actors to trawl the internet and social media at speed for every last detail of an individual so they can better "impersonate" them when prepping for an attack.

To meet increasing volume and sophistication requires ramping up the protocols in place to protect the network. In turn, these protocols – tighter access to payroll data, for example – add to the burden of security teams and introduce unwanted bureaucracy facing the internal users of those systems. Inefficiencies are likely to prevail.

Offering a more positive perspective of artificial intelligence, one attendee argued that AI allows firms to combat the actions of bad actors in kind. In other words, the increased volume and sophistication of attacks can, and must, be met with an increasingly fast-paced and intricate response. Both are possible through the effective adoption of AI tools when aligned with coherent security and resilience planning.

Another potential benefit of AI comes when deploying it during the recovery process. The period following an attack will often prove far more stressful than even the most well-designed war gaming and scenario planning. By deploying AI agents – allied with the necessary human supervision – to carry out recovery, organisations can "take the emotion" out of the process.

Frameworks, planning and other good practices

"Have a plan and think hard about recovery." That was the closing advice of one roundtable voice, capturing the essence of earlier conversations. Another attendee observed that a surprisingly high number of organisations have missed a trick by failing to implement security frameworks as part of their security and resilience efforts. Existing frameworks – such as the National Institute of Standards and Technology (NIST) cybersecurity framework – provide the necessary architecture with which to build a robust response, he said.

NIST, by way of example, is organised around six key functions – govern, identify, protect, detect, respond, and recover. Among the advantages of deploying this or similar frameworks, the attendee argued, is that they offer a common language in which to talk about risk and protection, and that they tend to be outcome focused. Those without a framework lack the underlying architecture to assess risks, to agree the shape and size of a viable business post attack, and to coalesce around a shared route to security and resilience.

Beyond Cyber Security: Data Integrity, Resiliency, and the Modern Enterprise – a CIONET executive roundtable in association with Hitachi Vantara – took place on Thursday 16 July 2026 at Great Scotland Yard Hotel, London.

About CIONET

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.