NETDILIGENCE CYBER RISK SUMMIT 2026

KEY INSIGHTS & STRATEGIC TAKEAWAYS

Attendee: Dominic Hithon

Company: Aeren LPO

Designation: VP Business Development

Location: Miami, Florida

Executive Overview

The NetDiligence Cyber Risk Summit 2026 reinforced a critical reality: Cyber risk is business risk. Across discussions involving insurers, breach counsel, CISOs, regulators, and forensic experts, one theme consistently emerged — no organization is fully prepared for a breach. The differentiator lies in preparedness, defensibility, and leadership alignment.

Transparency & National Security

Transparency is increasingly viewed as both a governance obligation and a national security imperative. Organizations must protect legal privilege, operate under a structured Incident Response (IR) plan, and extract and mine data using defensible workflows with documented decision-making

AI in Cyber Response: Innovation vs. Risk

Artificial Intelligence is augmenting digital forensics and data mining, automating phishing detection and first-pass document review. However, concerns remain around evidentiary defensibility, chain-of-custody integrity, and regulatory scrutiny. AI will augment human oversight, not replace it.

Incident Response & Tabletop Exercises

Effective tabletop exercises are designed to expose vulnerabilities and test real-world breach scenarios. They assess escalation pathways, privilege protection, data extraction readiness, and governance controls such as retention schedules and multi-factor authentication.

The CISO Reality

Effective tabletop exercises are designed to expose vulnerabilities and test real-world breach scenarios. They assess escalation pathways, privilege protection, data extraction readiness, and governance controls such as retention schedules and multi-factor authentication.

Threat Profiling & Exposure Areas

Organizations are encouraged to create formal threat profiles assessing third-party exposure, remote workforce vulnerabilities, phishing campaigns, sensitive data types, and detection capabilities. Every organization has likely experienced compromise — impact depends on detection and response maturity.

Data Mining & Workflow Distinctions

Incident Response workflows differ significantly from traditional eDiscovery. IR requires custodian-level PII review, higher subjectivity, and faster defensible decision-making under time-sensitive conditions.

Litigation & Post-Breach Considerations

Class actions vary in exposure risk, particularly in healthcare and sensitive-data cases. Dark web circulation of breach data may lead to repeated claims. Identity monitoring and structured post-breach tools are becoming standard practice.

Insurance & Carrier Coordination

Brokers and carriers must collaborate closely based on claim size, regulatory exposure, and jurisdiction. Clear protocols, especially regarding AI use, are increasingly important.

Culture, Leadership & Risk Tolerance

Security culture follows leadership. Business models shape retention policies, data maintenance strategies, and authentication enforcement. Innovation must be balanced with organizational risk tolerance.

Industry Scale & Outlook

The cybersecurity market continues rapid expansion, with thousands of companies operating globally and significant growth projected. Despite scale, preparedness maturity varies widely.

Conclusion

NetDiligence 2026 highlighted that cyber preparedness is a strategic business function. Organizations that invest in structured IR frameworks, defensible data review processes, AI governance, and leadership-driven security culture will be better positioned to manage breach events effectively.