LOGICALIS
Architects of Change

Managing Risk in Cybersecurity

Tales from the field

Mike Fry, Security & Cloud Business Unit Director, Logicalis UK&I

In this session, Mike Fry delves into the reality behind the statistics. What's really going on out there? What are organisations actually concerned about? And what's stopping them addressing the challenges and vulnerabilities they know they have?

Drawing from recent research and statistics in our 10th anniversary CIO Report:

- An alarming **83%** of CIOs reported falling victim to cyber hacks in the past year.
- Nearly all respondents suffered business ramifications as a direct consequence.

Despite concerted efforts, less than half of those surveyed express confidence in their readiness to mitigate another major security breach.

This session promises to equip attendees with practical insights, messages, and actions to navigating the complex cybersecurity terrain, arming them with real-world knowledge, essential for safeguarding their organisations against emerging threats.

Key Takeaways:

- Malware and ransomware remain top threats, exploiting vulnerabilities in organisational defences.
- Data breaches pose significant risks to data integrity and privacy.
- Phishing attacks persist as a prevalent threat vector, targeting unsuspecting users.
- Technology Leadership: In today's security environment, a proactive stance is essential, requiring a level of hypervigilance between intense curiosity and paranoia.

At-A-Glance

"You're Fired": we take a look at the changing Governance Risk and Compliance Landscape, real examples of security maturity assessments, and what's stopping organisations getting to get grips with their regulatory obligations and protecting their organisations.

"Everyone has a plan, until…": explore how organisations need to shift from a mindset of 'if' they are breached to 'when', and what they do to improve their resilience.

"Are you ready…really?': how prepared an organisation is, *ahead* of when a breach occurs, makes a huge difference in responding to and recovering from a successful attack. Here, we highlight thew critical components of robust Incident Readiness.

"What next?": Mike share's his thoughts on what 2024 will bring, and beyond, including the evolving threat landscape and how AI will play a role in both offence and defence.