Smart Diaspora 2025 – Workshop 14 Cybersecurity

TOP 5 CYBERSECURITY RISKS IN 2025: PANEL DISCUSSION

DIANA MOLDOVAN, ASOS, UK

MOLDOVAN.DIANA1987@GMAIL.COM

Ransomware 2.0 & RaaS



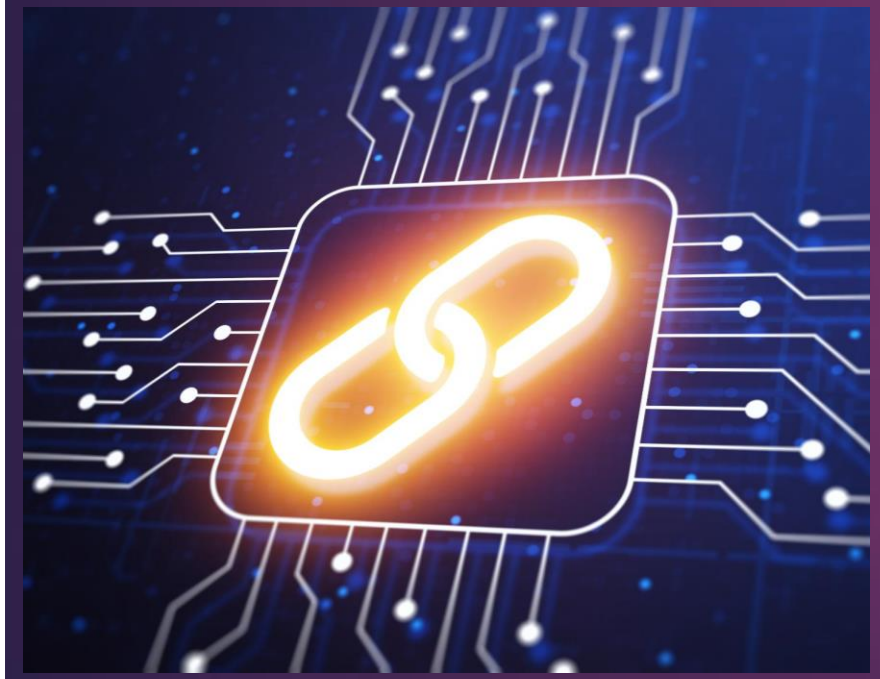
Ransomware groups are becoming more organised, offering "franchise models" to affiliates, and using data theft ("double extortion").

Questions

1. Ransomware attacks are not slowing down — they're evolving. How have threat actors professionalised in 2025 compared to just a few years ago?

2. What's the most overlooked defense measure organizations ***still*** fail to implement against ransomware?

Supply Chain & SaaS Vulnerabilities



The SolarWinds legacy continues; in 2025, breaches often come through trusted third-party tools or cloud integrations.

Questions

1. We've seen that attackers no longer go through the front door — they go through your suppliers. How can organizations realistically secure the digital supply chain?

2. Should software vendors and SaaS providers bear more responsibility for downstream security failures?

3. With so many SaaS apps integrated into enterprise workflows, is a 'Zero Trust' model enough — or do we need a new approach?

AI Powered Threats & Deepfake Phishing



Generative AI has made phishing and impersonation far more convincing and scalable.

Questions

1. AI is now a tool for both defenders and attackers. What's the scariest way you've seen AI used maliciously in 2025?

2. How can organizations build employee awareness when deepfakes and synthetic voices make social engineering so convincing?

Data Breaches & Privacy Erosion



Massive multi-billion record leaks (like the 2025 SaaS breach) show that personal data exposure is growing exponentially.

Questions

1. Are we losing the battle on data protection — or just fighting it with the wrong weapons?

2. What role should governments and regulators play in enforcing stronger data protection standards?

Critical Infrastructure & Nation-State Attacks



Government agencies, telecom, and energy providers are increasingly targeted by state-sponsored operations.

Questions

1. Nation-state cyber operations are becoming more frequent and disruptive — what's driving that escalation?

2. How can public and private sectors collaborate more effectively to defend critical infrastructure?

Wrap-Up

