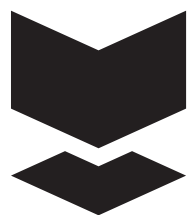


Post event report



Strategic Sponsors



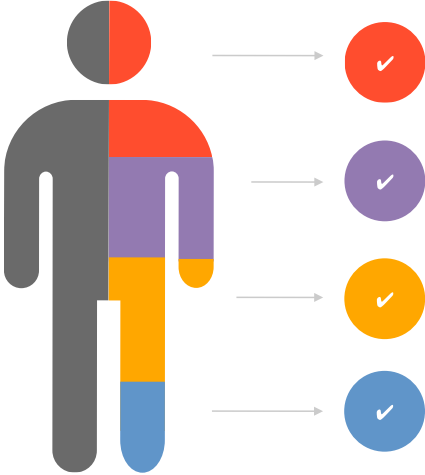
Silverfort



TRUSTMARQUE

Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda

Key themes	Speakers
Securing legacy technology	Alex Harris, Head of Future Cyber Capability Cabinet Office
The ultimate third-party problem	Dr Emma Philpott, Director and CEO IASME
Securing Arm’s Length Bodies – a systemic issue	Gerard Thompson, Chief Information Security Officer North Tyneside Council
Developing a risk-based approach to the Cloud	John Keegan, Deputy Director, Head of Digital Security Department for Work and Pensions (DWP)
A better approach to outsourcing cybersecurity	Matthew Holland, Incident Response Team Lead Royal Navy
Upskilling security teams	Peter Batchelor, Regional Director UK&I Silverfort
	Elliott Morgan, Cyber Lead for the NHS and Regional Services Trustmarque (on behalf of Silverfort)
Who attended?	
<div><div><div>Cyber-security We have a 20-year track record of producing the events cyber-security professionals take seriously</div><div>Risk Management We attract senior risk officers with responsibility for information risk assessment and mitigation</div><div>Fraud, Audit, Compliance We provide the go-to events for fraud prevention and compliance owners at the world’s key corporates</div><div>Data Protection & privacy We are a key venue for decision-makers with budget and purchasing authority</div></div></div>	

Agenda	
09:30	Chair's welcome
09:35	Improving public sector resilience at scale A representative from NCSC <ul style="list-style-type: none"> Improving cyber decision-making and increase cyber-accountability Resilience against common threats through Cyber Essentials Addressing identity issues through increasing the uptake of strong authentication, such as FIDO authenticators including passkeys
09:50	Building a new approach to government and public sector cybersecurity Alex Harris , Head of Future Cyber Capability, Cabinet Office <ul style="list-style-type: none"> An honest review of the current state of government and public sector cybersecurity Creating a joined-up approach to government and public sector cybersecurity Meeting the cyber-challenges of the future
10:05	Rapid NCSC CAF Compliance: Deploying Enterprise PAM in days with Silverfort Peter Batchelor , Regional Director UK&I, Silverfort; Elliott Morgan , Cyber Lead for the NHS and Regional Services, Trustmarque (on behalf of Silverfort) <ul style="list-style-type: none"> See proven public sector results with case study examples of how Trustmarque and Silverfort have helped government teams achieve CAF compliance with minimal disruption and cost Learn how to extend MFA 'everywhere' to legacy systems, on-premises environments Learn how to automatically detect and protect service accounts and cloud non-human identities Learn how to deploy Just-in-Time, access – Enforcing time-bound privileged access that meets CAF controls without the overhead of legacy PAM Learn how to deliver identity zero trust, stop lateral movement, and protect against 3rd party/supply chain cyber-attacks
10:25	From reactive to resilient: Cyber-resilience for public sector operations Shifting the mindset from prevention to resilience in cybersecurity Gerard Thompson , Chief Information Security Officer, North Tyneside Council <ul style="list-style-type: none"> Why resilience matters more than ever in critical public services Integrating continuity planning, cyber-hygiene, and adaptive security Metrics for resilience: What should leaders actually measure? Real-world frameworks for building institutional muscle memory
10:30	Comfort break
10:40	To 'DAIR' is to do – Rethinking incident response frameworks for modern teams Matthew Holland , Incident Response Team Lead, Royal Navy <ul style="list-style-type: none"> Explore PICERL – Gain insights into the current industry-standard incident analysis framework, understanding both its strengths and its limitations Discover DAIR – Introduce a modern, agile alternative designed to enhance collaboration, adaptability, and continuous learning Compare & apply – Analyse a real-world incident through both lenses to reveal how DAIR can drive deeper insights and more effective outcomes than PICERL
11:00	Evolving from Secure-by-Design to Secure-by-Default – improving cyber-resilience John Keegan , Deputy Director, Head of Digital Security, Department for Work and Pensions (DWP) <ul style="list-style-type: none"> Operational and architectural shifts required to move from Secure-by-Design to truly enforceable Secure-by-Default implementations Integrating Secure-by-Default principles into CI/CD pipelines, infrastructure-as-code, and zero trust enforcement at scale How Secure-by-Default enhances resilience by reducing attack surfaces, enforcing least privilege, and eliminating insecure defaults across complex environments
11:20	Cyber Essentials: Simple steps, stronger security Dr Emma Philpott , Director and CEO, IASME <ul style="list-style-type: none"> What's it all about? Effectiveness and impact Overcoming challenges for large organisations meeting such a prescriptive standard Using Cyber Essentials as a supply chain tool
11:40	Chair's closing remarks