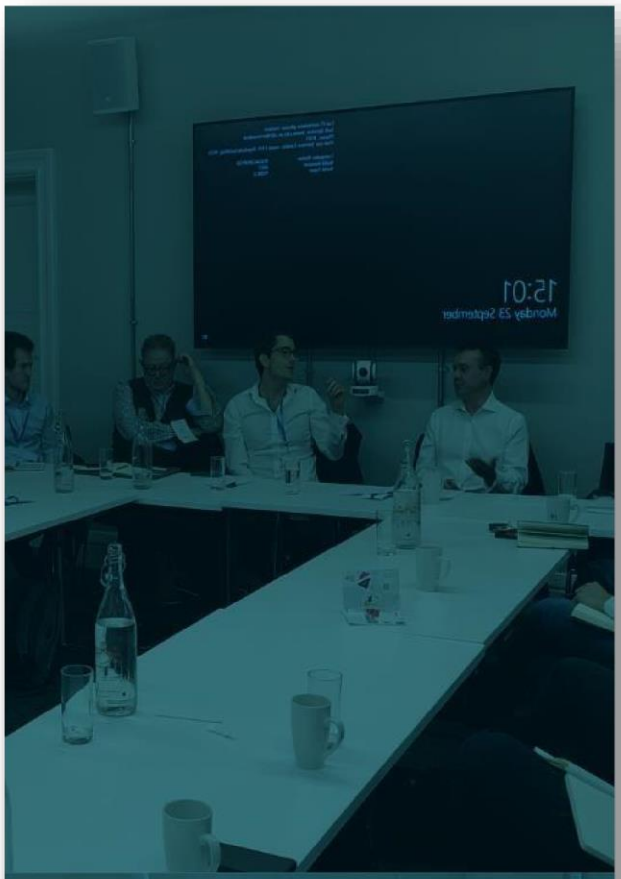
The Real Hon Stephen McPartland – Round Table Report 2024



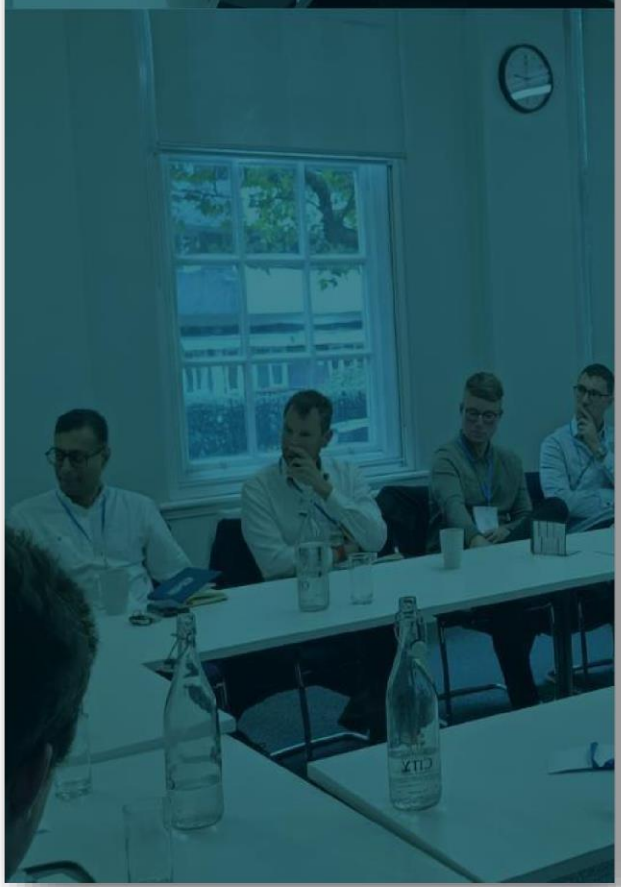


TABLE OF CONTENTS

CYBER.
LONDON

Date: 23/09/2024

Time: 14h00 – 17h00

Venue: Room AG04, City St George's, University of London

Number of Participants: 18

1. Introduction and Welcome

The roundtable event opened with welcoming remarks by Simon Newman, who highlighted the significance of the gathering and its purpose: to discuss the McPartland Review on Cyber Security as an Enabler of Economic Growth. The review outlines 16 key recommendations to strengthen the UK's cybersecurity landscape, with a particular focus on improving resilience and recovery in supply chains, supporting SMEs, and fostering a culture of cybersecurity awareness.

Introductions:

Each participant introduced themselves, providing insights into their professional background and perspectives on cybersecurity.

Simon Newman: A seasoned cybersecurity professional with extensive experience in strategic security leadership. Currently serving as a Senior Advisor and Consultant, Simon specializes in cybersecurity, crisis management, and organizational resilience. He is one of the Co-Founder of Cyber London. He served as the Chair of the roundtable, introducing the event and underscoring the critical need for a collaborative approach to cybersecurity.

Raj Rajarajan: Professor of Security Engineering and Director of the Centre for Cyber Security for Society at City St George's, University of London with a strong background in cybersecurity research and education. He is one of the Co-Founder of Cyber London. With over 20 years of experience in cybersecurity, he is recognized for his contributions to securing digital infrastructures and developing cybersecurity talent through academic leadership. He spoke about the academic perspective, emphasizing the role of universities in addressing the cybersecurity skills gap.

Izak Oosthuizen: CEO of Zhero Cybersecurity & IT Support, focusing on bespoke cybersecurity solutions for SMEs. He is also the Co-Founder and Director of Cyber London, recognized as the official Cyber Cluster for London, and the Founder of Winelands PASS. As a member of the Entrepreneurs' Organization, Izak actively contributes to the cybersecurity community with over 20 years of experience, bringing strategic insights and innovative solutions to the industry.

Rt Hon Stephen McPartland: Former member of Parliament with over 14 years of experience, specializing in economic development and national security. As a leading voice in cybersecurity policy, he has been instrumental in shaping discussions on the role of cybersecurity in driving

economic growth. Stephen led the McPartland Review, which outlines key recommendations to strengthen the UK's cybersecurity landscape. As the chief guest of the event, he outlined his motivation for leading the review, provided valuable insights into the report's findings, and emphasized the strategic importance of implementing its recommendations. He stressed the critical role of cybersecurity in driving national economic growth.

Craig Dunn: An experienced insurance professional specializing in cyber risk management and underwriting. Currently serving as an Underwriting Manager, he focuses on developing insurance solutions that address the evolving cybersecurity needs of businesses. Craig discussed the challenges and opportunities within cyber insurance, especially for SMEs.

John France: Chief Information Security Officer at the Global Forum for Cyber Expertise (GFCE), with extensive experience in cybersecurity, risk management, and resilience. He focuses on enhancing global cybersecurity capabilities and promoting strategic collaboration across sectors.

Stuart Nelson: Cybersecurity leader specializing in cyber strategy, threat intelligence, and risk management. He is known for his work in helping organizations enhance their security posture and manage cyber risks effectively. Stuart brings a wealth of knowledge on strategic cybersecurity initiatives and their impact on business resilience.

Danny Lopez: CEO of Glasswall, a company specializing in advanced cybersecurity solutions. With a background in technology, finance, and international trade, he is recognized for his leadership in driving innovation in the cybersecurity industry. Danny is focused on helping organizations protect against cyber threats through cutting-edge technology and strategic insights.

Laura: Associate Director of Third-Party Risk at Crossword Cybersecurity Plc, where she focuses on managing third-party risks and enhancing cybersecurity strategies. She also serves as the Head of ThirdParty Risk and has previously worked as a Managing Consultant in Third Party Assurance, bringing extensive experience in technology risk and relationship management.

Aneesh Banerjee: Senior Lecturer in Digital Innovation and Entrepreneurship at Bayes Business School, City St Goerge's, University of London. He specializes in digital transformation, fintech, and innovation management, bringing a strong blend of academic research and industry expertise.

Fiona Bail: Detective Chief Inspector and Head of Cyber PATH, focusing on tackling cybercrime and enhancing cybersecurity measures. She has extensive experience in law enforcement and cybersecurity strategy, leading initiatives to protect organizations and individuals from cyber threats.

Mark Child: Chief Executive at Quantum Evolve Business Enablement, where he focuses on driving innovation and strategic growth through advanced cybersecurity solutions. With a strong

background in cybersecurity and business transformation, Mark leverages his expertise to help organizations navigate complex security challenges and enable business resilience.

Richard Starnes: Non-Executive Director and Chair of the Advisory Board at the Cyber Resilience Centre in London. He brings extensive experience in cybersecurity leadership, guiding organizations on resilience strategies and risk management, while also contributing to cybersecurity education and policy through his advisory roles.

Steve Johnson: Head of Information Security at Risk Ledger, specializing in enhancing supply chain security through pragmatic risk management. With over three decades of experience from mainframe systems to modern cloud environments, he blends technical expertise with strategic business insights. Steve is also an international conference speaker and contributor to cybersecurity standards and best practices.

Tom Exelby: Head of Cyber Security at Red Helix, where he leads the development of Cyber Security Managed Services to protect businesses against cyber threats. With over 15 years of military experience, Tom is a seasoned leader known for building strong team cultures and strategic approaches to cybersecurity.

Scott Goodman: Account Executive at N-able, where he specializes in cybersecurity solutions, helping organizations streamline their IT and security operations. A high-achieving sales professional, Scott built a successful company while at university, generating over £1 million in revenue, and has consistently excelled in his roles, combining entrepreneurial drive with expertise in security and backup solutions.

Anthony Young: Founder and CEO of Bridewell, a leading cybersecurity consultancy specializing in protecting critical infrastructure. With over 20 years of experience, he has driven Bridewell's growth by focusing on quality, integrity, and partnership with clients. Anthony started his career in Governance, Risk, and Compliance before establishing Bridewell to set a new standard in cybersecurity services.

Carrie Meyers: Associate Professor of Criminology at City St George's, University of London, specializing in youth crime, victimology, and crime prevention. With a background in criminological research and education, she focuses on understanding the social impacts of crime and developing effective prevention strategies.

2. Setting the Scene – The McPartland Report **Summary:**

Rt Hon Stephen McPartland provided a comprehensive overview of the McPartland Review, which includes 16 strategic recommendations aimed at positioning the UK as a leader in cybersecurity. The report emphasizes the need for a Cyber Charter to build resilience into supply chains, Green

Cyber initiatives to align cybersecurity with environmental goals, and improved threat intelligence sharing between industry, academia, and government. McPartland highlighted the urgency of these recommendations, noting that while the government had initially welcomed the report, they have not yet issued a formal response following the July 2024 elections.

Key Recommendations from the Report:

Cyber Charter: Proposed to integrate cybersecurity guidance into business practices from the outset, particularly targeting SMEs through tax-efficient measures.

Green Cyber: Encouraged environmentally friendly cybersecurity practices to reduce carbon footprints in the tech sector.

Cyber in the Boardroom: Recommended the integration of cybersecurity awareness at the highest levels of corporate governance.

Skills and Education: Stressed the importance of embedding cybersecurity training at all educational levels to address the skills gap and promote diversity in the field.

3. Open Discussion

The open discussion section was the core of the event, with participants engaging in a dynamic exchange of views on the report's findings and recommendations. **Key Discussion Points:**

1. Attacks on National Infrastructure and Supply Chains:

Stephen McPartland opened the debate by highlighting the growing threat landscape, particularly the risks posed to national infrastructure and supply chains by state-sponsored actors and cybercriminals. He referenced recent attacks that have severely impacted global economies, stressing the importance of implementing robust security measures. The discussion covered how state actors are increasingly targeting digital assets, with no regard for geographical boundaries, emphasizing the need for heightened vigilance.

2. Challenges Faced by SMEs:

Craig Don elaborated on the vulnerabilities of SMEs, noting that 99.8% of UK businesses fall within this category and often lack sufficient cybersecurity defenses. The discussion touched on the difficulties SMEs face in implementing basic security measures, such as Cyber Essentials, due to cost constraints and lack of expertise. Participants agreed that a significant cultural shift is needed to view cybersecurity not just as a compliance issue, but as a critical business enabler.

3. Cyber Insurance and Its Role in Risk Mitigation:

The conversation highlighted the role of cyber insurance as a tool to mitigate risks for businesses. However, concerns were raised about the effectiveness of current insurance products, with Craig Don noting that many policies fail to cover the full scope of potential damages. There was a consensus on the need for more robust and clearly defined insurance offerings that could better protect SMEs against cyber threats.

4. Global Cybersecurity Landscape and Quantum Cryptography:

The participants explored the global cybersecurity landscape, including the emerging challenges posed by advancements in quantum cryptography. Mark discussed parallels with GDPR and how the evolving technological environment is complicating efforts to achieve true cyber resilience. The conversation acknowledged that as technologies advance, so do the tactics of cybercriminals, necessitating continuous innovation in defense strategies.

5. Education, Skills, and the Cybersecurity Workforce:

There was significant discussion around the skills gap in the UK's cybersecurity sector, identified by Raj. He highlighted the critical need for targeted education and training programs to address the shortage of skilled professionals. Aneesh stressed the importance of attracting a diverse range of candidates, including women, disabled individuals, and career changers, to broaden the talent pool. The group called for universities to work more closely with industry to ensure that graduates are adequately prepared for real-world challenges.

6. Cybersecurity Legislation and Regulation:

Participants discussed the role of legislation in shaping a secure digital environment. Simon noted that the UK is lagging behind other countries in implementing comprehensive cybersecurity regulations. There was a call for a balanced approach that includes both technical and cultural guardrails to foster a more resilient cybersecurity ecosystem.

7. Behavioral Change and Cybersecurity Culture:

The need for cultural transformation within organizations was a recurring theme. Participants agreed that cybersecurity must be embedded into the DNA of companies, from the boardroom to the frontline employees. Discussions underscored the importance of proactive measures, continuous education, and the role of leadership in driving this cultural shift.

Key Questions Raised:

Funding and Implementation of Recommendations: Richard inquired about the financial feasibility of the proposed recommendations and the timeline for their implementation.

Global Comparisons: The group explored international best practices, questioning what the UK could learn from other nations that are further ahead in cybersecurity.

SMEs and Cyber Essentials: A key question was raised about how to make Cyber Essentials more accessible and attractive to SMEs, given the existing barriers to adoption.

4. Summary and Next Steps

Closing Remarks:

Rt Hon Stephen McPartland and the Chair of the Roundtable Simon summarized the key insights from the discussion, reiterating the need for ongoing collaboration between the government, private sector, and academia. They emphasized the importance of implementing the report's recommendations to strengthen the UK's cybersecurity posture and drive economic growth.

Action Items:

White Paper Development: A white paper will be drafted to consolidate the recommendations and outline a strategic roadmap for future actions.

Enhancing Cybersecurity in Supply Chains: Efforts will be made to integrate cybersecurity practices within supply chains through collaboration with large financial institutions and the wider business community.

Education and Skills Training: Initiatives to bridge the skills gap will be prioritized, including the development of mentoring programs and partnerships between universities and industry.

Legislation and Policy Advocacy: The group will explore ways to advocate for stronger cybersecurity legislation and regulatory frameworks that address the evolving threat landscape.

Proposed Next Steps:

Further Roundtable Discussions: Organize additional events to deepen the dialogue on specific issues such as cyber insurance, skills training, and regulatory challenges.

Engage with Stakeholders: Foster closer collaboration with policymakers, industry leaders, and educational institutions to drive forward the implementation of key recommendations.

Monitor Progress: Establish a mechanism to track the progress of the recommendations and measure their impact on improving the UK's cybersecurity landscape.

Acknowledgments:

The event concluded with a message of gratitude from Rt Hon Stephen McPartland, who commended the participants for their valuable contributions and encouraged them to continue supporting efforts to enhance cybersecurity in the UK.

5. End Note:

Simon Newman, as the Chair of the roundtable, concluded the event by thanking all participants for their valuable insights and active engagement. He emphasized the importance of the discussions in shaping the future of cybersecurity in the UK, particularly in the context of the McPartland Review's recommendations. Simon acknowledged the diversity of perspectives shared during the session and highlighted the collective responsibility to drive forward the initiatives discussed. He expressed appreciation for the collaborative spirit and encouraged everyone to maintain this momentum as they work together to strengthen the nation's cybersecurity resilience.

Simon closed by underscoring the critical need for continued dialogue and action, urging participants to stay connected and involved in the ongoing efforts to enhance cybersecurity across sectors. He expressed optimism about the impact of their contributions and the potential for significant progress in the months ahead. Simon thanked everyone for their dedication to the cause and looked forward to future collaborations that would build a more secure digital landscape for all.

CYBER.
LONDON