COLLECTIVE INTELLIGENCE

Munich Cyber Security Conference:

Five Insights for Business Leaders

Siobhan Gorman, Nicola Hudson and Michael Rogers

February 2024

This year's Munich Cyber Security Conference brought together the largest ever delegation of cyber professionals around the world from government, the corporate world, and civil society. The event, leading into the Munich Security Conference, wrapped up on Friday 16, 2024, with experts trying to chart a path out of what the conference called our current "cyber conundrum".

Five Takeaways

Brunswick took part in multiple panels at the event spanning the threat landscape, regulation, and what comes next. Here is why this year's conference mattered:

Outcomes are key

It's important not to confuse effort with outcomes. Over the last decade, cyberattacks and their consequences have been getting worse, not better. The key to fewer attacks and ones that have far less impact on organizations will be incentivizing the behavior that leads to those outcomes. There was also palpable concern over the U.S. government's increasing use of personal liability for cyber security professionals executing their jobs in an honest and forthright, yet admittedly imperfect, manner.

Cybersecurity has become business continuity

Without a major dent in cybercrime and attacks in the near term, organizations have to do much more now to be prepared to bounce back from an incident. The growing and unrelenting scourge that is ransomware continues to cause havoc on organizations and means businesses must assume "it's not if, but when" and plan accordingly. Companies need to share lessons across sectors, not just within them.

Implementation is the next big challenge for regulation

There has been an influx of regulation, including NIS2 and the Cyber Resiliency Act in Europe and the new SEC rules in the U.S. among others. Companies voiced exhaustion with the current pace of regulation and said we should stop generating further regulation until the private sector can fully absorb and execute what has been directed over the past 18 months. Several corporate leaders did note these regulations have elevated cybersecurity to the CEO and Board radar in a new, very real, way, which is a promising step in the right direction.

Geopolitics adds even more complexity

The connection between geopolitics and cybersecurity is intensifying rapidly. This dynamic - be it with Russia, China, Iran, North Korea, or others - makes it even harder for companies to understand what threats they are facing and how to defend themselves against them. Companies also do not know how to best interact with the various regulators, authorities, and national security agencies if attacked by a state.

AI's impact remains to be seen

AI may eventually transform the cyber landscape, but it hasn't done yet. For now, AI seems likely to elevate and accelerate the efforts of both the defender and the attacker, but it is not transformative yet.

The good news is there are a growing number of smart, experienced people around the world committed to developing solutions to these cyber conundrums – although a theme running through many of the discussions was the continued competition for talent. But it will still take considerable, and sustained work to get there with a continued focus how governments and business can work in concert to address these issues.

Get in touch with Brunswick

Siobhan Gorman

Partner, Cybersecurity, Data & Privacy Global Lead, Washington, D.C.

sgorman@brunswickgroup.com

Siobhan concentrates on crisis, cybersecurity, public affairs, and media relations. She worked on corporate crises and corporate reputation projects across a range of industries. Tapping her longtime journalism experience, she regularly advises clients on media relations issues and conducts media training for executives.

Nicola Hudson

Partner, Cybersecurity, Data & Privacy Global Lead, London

nhudson@brunswickgroup.com

Nicola has worked on hundreds of cyber security incidents and has deep expertise in cybersecurity issues and crisis management across both the public and private sector. Prior to joining Brunswick, she was a member of the Executive Board at the Government Communications Headquarters and Director of Policy at the National Cyber Security Centre.

Michael Rogers

Senior Advisor, Washington, D.C.

mrogers@brunswickgroup.com

Admiral Rogers joined Brunswick in July 2019 following a 37-year career in the U.S. Navy and is a senior advisor to the firm in the areas of cyber security, privacy, geopolitics, technology and intelligence as well as crisis management and the challenges of leading large organizations in a democratic society in the digital age.