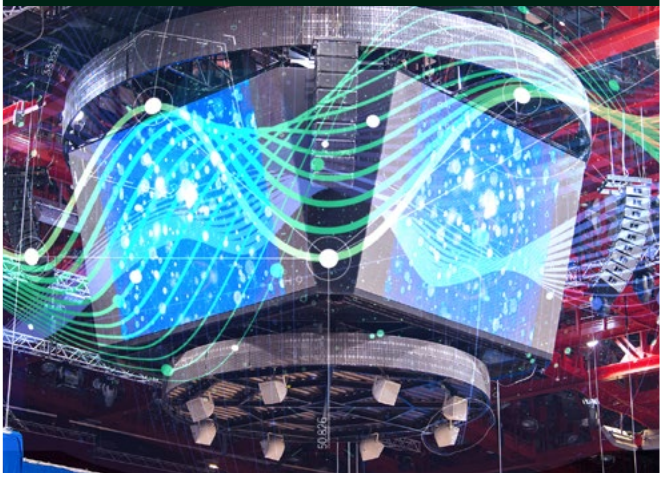
ECONOMIST IMPACT

EVENT SUMMARY

Cyber-security in the 5G era: mitigating risks and building resilience

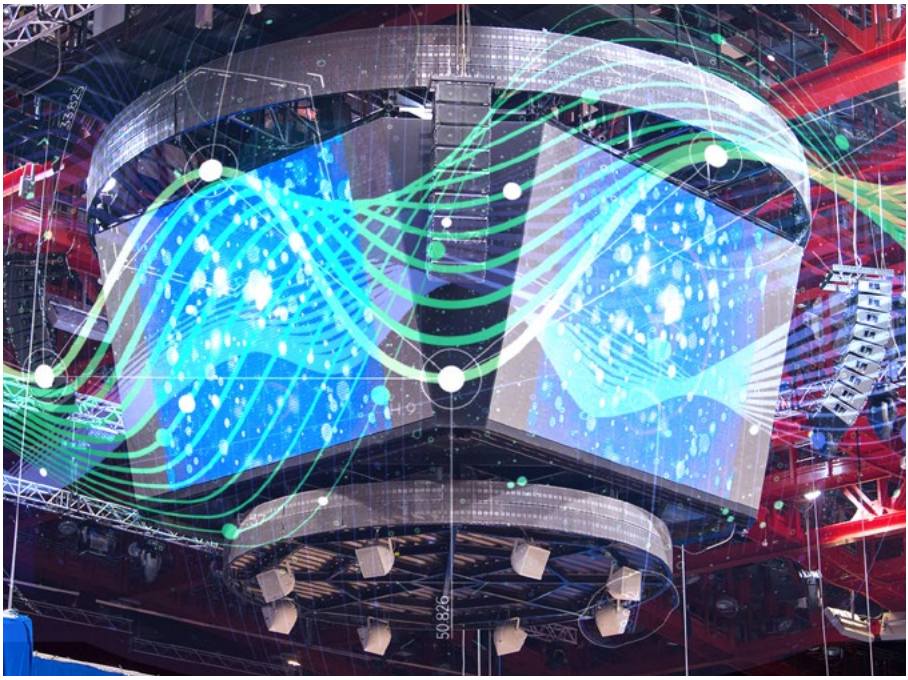
April 7th 2022



Sponsored by kyndryl

Event summary

Cyber-security in the 5G era: mitigating risks and building resilience



The digital transformation of society demands a new approach to cybersecurity. As we move from single connectivity points to more meaningful connectivity, many more players are involved in delivering IT services. These entities, more used to competing, now need to learn to collaborate to thwart malicious actors and protect the businesses they serve. This requires trust, openness and a willingness to share non-strategic information. Regulators have an important role to play in bringing stakeholders together to address cybersecurity, but it is important to avoid overreach. A light-touch approach is needed when it comes to developing cybersecurity standards and protocols, beginning with establishing a set of common denominators.

Executive Summary

Economist Impact convened a panel discussion sponsored by Kyndryl under the theme '**Cybersecurity in the 5G era: mitigating risks and building resilience**' to examine how fifth-generation (5G) wireless technology is changing the threat landscape for businesses and creating new challenges for mobile network operators.

The discussion was moderated by Dexter Thillien, lead analyst, technology and telecoms, Economist Intelligence Unit. The panel of experts comprised Todd Mason Scott, managing partner, Kyndryl; Michael Irizarry, executive vice-president and chief technology officer, engineering and information services, UScellular; and Mats Granryd, director-general, GSMA.

Business is Vulnerable

As the fourth industrial revolution, enabled by the faster speeds, lower latency and higher throughput capacity of 5G, propels us towards becoming a hyperconnected society, cybersecurity has become more important than ever.

The huge cost efficiencies and productivity gains offered by digital technologies such as the Internet of Things (IOT), cloud computing, artificial intelligence and data gathering mean connectivity has become critical for businesses. But this connectivity also makes businesses more vulnerable to malicious actors. With a up to 1 million IOT connections estimated to be in each square kilometre, the potential attack surface has dramatically increased.

"5G will not be all that it is capable of being if we stay in our silos."

Todd Mason Scott
Managing partner
Kyndryl

In an open network environment, full security is impossible to achieve. A network is only ever as strong as its weakest link. Robust cybersecurity involves more than just investing in technology; it requires people to be diligent, processes to be followed and the technology to be configured correctly, meaning cybersecurity is everyone's responsibility.

A team effort

Getting cybersecurity right has to begin at the very top of a company. The board and senior management need to be fully aware of the risks and understand the importance of investing in cybersecurity. Cybersecurity should be a team effort; it is not something that can be left to the company's security officer. Every employee needs to be educated about the risks, and cybersecurity needed to be embedded throughout all processes.

5G has been designed to support rapid growth in connectivity in order to facilitate the digital transformation of society. It has much stronger security features than previous generations of wireless technology including device ID authentication and encryption, and further cybersecurity innovations are under development, such as network slicing to isolate customer information transfers.

"Between now and 2025, it is estimated $600bn will be invested in mobile networks, and about 80-85% of that will go towards 5G and security and safety." Mats Granryd, GSMA

But digitalization also presents a new set of problems, requiring a different approach to cybersecurity. As the world moves from single connectivity points to more meaningful connectivity, many more players become involved in delivering IT services, and all these stakeholders - telecoms operators, vendors, cloud players, AI players and so forth - need to work together to mitigate security threats. The challenge is that all these players compete as businesses.

Collaborating with competitors

The industry will be better prepared to fight common threats if businesses are transparent about their experiences and share information on malicious actors in a timely manner. Businesses need to both compete and collaborate. This requires trust, openness and a willingness to share non-strategic information.

"If security is not a regular topic in the boardroom there is a problem."

Michael Irizarry
Executive vice-president and chief technology officer, engineering and information services
UScellular

Government also has an important role to play in bringing stakeholders together to address cybersecurity, but it is important to avoid regulatory overreach. Light-touch regulation is the ideal approach: regulators are most effective when facilitating information sharing between government and industry and working to create common guidelines and frameworks.

Common denominators

With different sectors and industry verticals having unique needs when it comes to 5G services, there cannot be a one size fits all approach to cybersecurity. Rather than trying to 'boil the ocean' when it comes to cybersecurity standards and protocols, regulators should adopt the approach taken with roaming and begin by focusing on a set of common denominators and later expand them.

Following a surge in high-profile hacks in recent years, company bosses are generally more attuned to cybersecurity than they were a decade ago, with more investment being directed towards technology and expertise. But we are still only in the early days of digitalization.

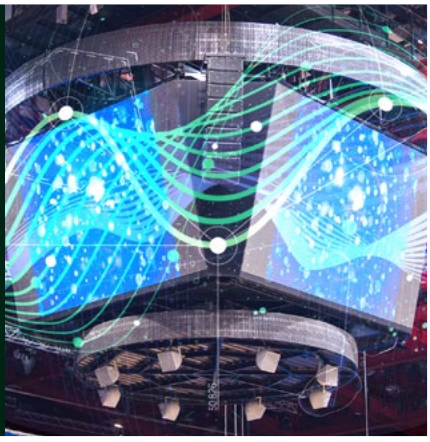
The enormity of the transformation that lies ahead as the full potential of 5G is realised and the cybersecurity challenge that this entails has yet to be fully grasped. The more connected society is, the more breaches, or attempted breaches, there will be.

"We compete as businesses, but the common threat is the malicious actor."

Michael Irizarry
Executive vice-president and chief technology officer, engineering and information services
UScellular

The task of cybersecurity is never done with, instead it needs to be constantly reviewed and revised. Companies should be testing their defenses as part of their day-to-day operations rather than waiting until an attack happens. If cybersecurity is not a regular topic in your boardroom, there is a problem.

Watch the webinar here



Economist Impact
Economist Impact is a part of The Economist Group, publisher of *The Economist* newspaper. Sharing *The Economist*'s commitment to informed, impartial and independent debate, we are recognised the world over as a leading provider of highly interactive meetings—including industry conferences, private gatherings and government roundtables—for senior executives seeking new insights into important strategic issues.

20 Cabot Square, London, E14 4QW, United Kingdom
events.economist.com