CYBERSECURITY

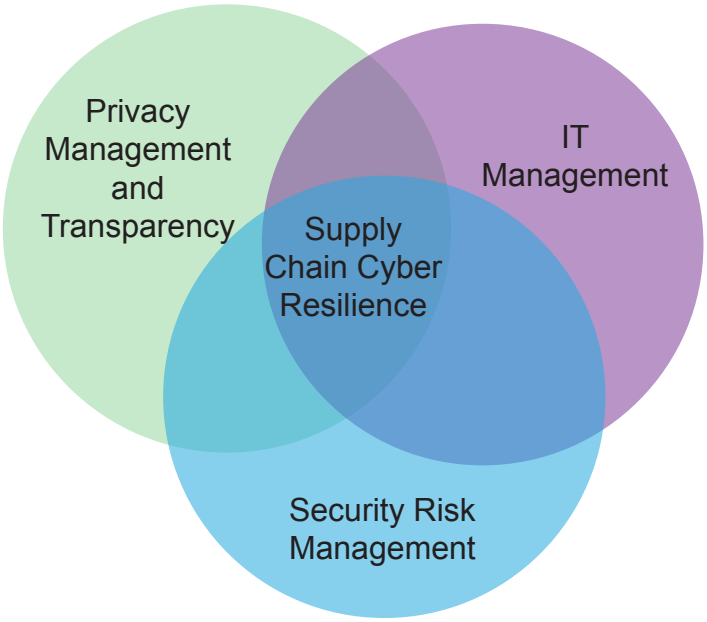
Fernando Ambrosetti

At present, leading economic countries across the globe are competing in a sort of arms race to dominate the 5G telecommunications industry. Therefore, it is no longer a question of if 5G will be implemented, but when. Ushered in with the incoming 5G era will be a plethora of inherent cybersecurity risks which will be a major obstacle for first-mover telecommunications companies in the German and Austrian 5G markets. 5G networks will undergird a host of critical functions such as autonomous vehicles, smart electric grids, factory automation, telemedicine, and smart cities. With the proliferation of massive machine-to-machine communications, or IoT, billions of devices will connect with one another in a web-like environment. As such, 5G will provide a critical function in the global economy and in society at large. However, accompanied with this increased dependency on 5G networks will be an increased vulnerability to the theft of sensitive data navigating the network, and to cyberattacks that disrupt the network and connected devices.[i] With 5G, the telecommunications system will become so central to everyday life that it will become a more appealing target for malicious actors, which may undermine the technology's utility.[ii] Therefore, it is in the interest of telecommunications companies to proactively respond to cybersecurity risks. First, this section of the report will provide a synopsis of the most concerning cybersecurity-related risks in the 5G industry. Subsequently, mitigation strategies to the identified risks are presented, which will give 5G providers a competitive advantage over their competitors and will situate them well for the 5G era.

SUPPLY CHAIN COMPLEXITY

Operators of communications infrastructure often depend on technology from other suppliers and the supply chain which provides ICT (Information and Communication Technology) equipment is becoming increasingly global.[iii] Associated with the increasingly complex supply chain are several major security risks. For instance, Nokia and Ericsson both have factories and subcontractors within China, which could become vulnerable to government pressure due to bias and speculation. The supply chain risk stretches far beyond the specific example of China. At large, offshore manufacturing facilities and products sourced from abroad open telecommunications companies up to greater security risk. First, the overall risk of influence by the country where production is located increases with a more complex supply chain. Notably, the clarity of cooperation agreements on security or if it is committed to the fight against cybercrime and data protection is unknown and troubling.[iv] Second, every manufacturing facility, depending on its location will have security protocols which may or may not live up to those of the EU. The supply chain that makes up 5G consists of everything from radio networks, to the integrated

chipsets in that network and the devices that will use the network (not just phones, but also billions of IoT devices).[v] The increased scale of supply chains makes it more difficult for operators to guarantee that network components are free from all vulnerabilities. At any level of the supply chain, individuals could insert 'backdoors' without the knowledge of the final vendor and even the subcontractor, either independently or on behalf of a malicious state or non-state actor.[vi]



MITIGATION:

Collaboration and Data Protection

Securing supply chain management processes depends on collaboration given the large number of actors and stakeholders involved. The amount of trust that an organization places on another, will eventually feed into the risk assessment process and subsequent introduction of appropriate security controls. Addressing the complexity and the risks involved in large supply chains is a matter of identifying how much trust one can afford to place, and what residual risks it can accept in order to define appropriate levels of security.[vii] Additionally, securing the collaboration between two entities is not sufficient, when such collaboration is only part of a wider supply chain.[viii] End-to-end security is a prerequisite for ensuring a secure supply chain. Therefore, holistic management of security across the supply chain is necessary.

In accordance with the ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, data processed by a third-party must be protected by a data processing agreement. Telecommunications companies should only share consumers' personal data with third parties after obtaining the express consent of the consumers, unless otherwise required and limited for the use of service operations or product features. Furthermore, it is necessary to adopt cyber supply chain risk management policies and communicate specific security requirements to suppliers and partners.[x]

5G PERSONNEL EXPERTISE

A lack of security has the potential to significantly affect business continuity. For example, in 2017 the NotPetya attack caused $10 billion in corporate losses. The combined losses at FedEx, Merck, and Maersk alone exceeded $1 billion.[xi] Although 5G networks did not exist at that time, the attack illustrates the high cost of such incursions, and can even be considered small in comparison to the attacks that could occur in a 5G society. Human injury or loss of life will become far more likely results of cyberattacks in the 5G era where the digital and physical realms will mesh as a result of advancements such as smart cities and autonomous vehicles. Clearly, the personnel needed to achieve adequate cybersecurity will be a critical asset to telecommunications companies entering the 5G market. However, 5G will allow for the emergence of several new, far more complex digital capabilities such as the IoT and Industry 4.0. Cybersecurity personnel will require expertise over several areas, for example, network security, embedded systems, OT security, and IT security just to name a few.

Therefore, it is becoming increasingly difficult to find qualified specialists who are aware of the imminent security issues at a time when they are needed most. Unfamiliarity with the new technologies associated with 5G raises concern for whether employees (and in turn, 5G telecommunications companies as a whole), possess the new competences that are essential for maintaining secure telecommunications networks.[xii]

MITIGATION:

Advance Cybersecurity Training and Implementation of AI Security Solutions

Telecommunications firms should invest in state-of-the-art dedicated cybersecurity training which covers all necessary aspects of IT/OT security convergence.[xiii] Furthermore, firms should consult with regulatory/standardization bodies such as ENISA and ETSI in order to address cybersecurity issues more efficiently. Cybersecurity can be an important competitive advantage for telecommunications companies as it leads to reliable, secure, and trustworthy products. Which means investment in cybersecurity should not be seen as only a cost,

but an important business opportunity. Further mitigations can be taken through the introduction of automation and AI-driven security solutions. Given the need for massive efficiencies in detection, provision of situational awareness and real-time remediation of threats, AI serves as an invaluable complement to human labour in cybersecurity. Machines' ability to synthesize unstructured data allows them to make connections that may not be immediately obvious to the human eye. Fatigue, which can lead humans to miss a potential exploit or vulnerability will no longer be a factor with automation and AI.[xiv] Therefore, in addition to modern training of cybersecurity employees, it is advised to adopt the same cutting-edge technologies which will be used to attack 5G in an attempt to defend it from those attacks.

Telecommunications companies around the globe are preparing for the inevitable 5G telecommunications era. As such, these companies are seeking to maximize their share of the 5G market as it is the future of the industry. However, with the valuable advancements which 5G brings are an abundance of security concerns. Therefore, proper implementation of 5G networks means the implementation of secure and reliable networks. In order to achieve secure and reliable networks telecommunications companies must overcome the challenges of the complex 5G supply chains and the scarcity of 5G security personnel. It is in the interest of 5G telecommunications companies to offer networks secure from cyberattacks as that is what consumers and governments demand. Telecommunications companies should therefore view cybersecurity as a top priority, and the associated costs as a necessary investment for entering the lucrative 5G market.

---

[i] Robert, Williams, "Securing 5G Networks", Council on Foreign Relations, July 15, 2019, https://www.cfr.org/report/securing-5g-networks

[ii] John D. McKinnon, "5G Wireless Technology Raises Security Fears." The Wall Street Journal, Dow Jones & Company, September 12, 2018, https://www.wsj.com/articles/5g-wireless-technology-raises-security-fears-1536804240.

[iii] "Commission Recommendation – Cybersecurity of 5G Networks." European Commission. European Union, March 26, 2019. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks, 4.

[iv] "Commission Recommendation", 4.

[v] Tom, Wheeler, "5G in five (not so) easy pieces." Brookings, The Brookings Institution, July 9, 2019. https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/.

[vi] "The EU Assesses Cyber Security and 5G Networks." RUSI, Royal United Services Institute, Cyber Threats and Cyber Security, October 25, 2019, https://rusi.org/commentary/eu-assesses-cyber-security-and-5g-networks.

[vii] Dr. Apostolos Malatras, Christina Skouloudi, and Aggelos Koukounas. "Industry 4.0 Security: Challenges & Recommendations." The European Union Agency for Network and Information Security, May 20, 2019, p.9. https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.

[viii] Malatras, Skouloudi, and Koukounas. "Industry 4.0 Security," 9.

[ix] "Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures," The European Union Agency for Network and Information Security, November 20, 2017, p.48. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[x] "Baseline Security Recommendations for IoT," 48.

[xi] Tom Wheeler, and David Simpson, "Why 5G Requires New Approaches to Cybersecurity." Brookings, The Brookings Institution, November 25, 2019. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/amp/.

[xii] Malatras, Skouloudi, and Koukounas. "Industry 4.0 Security," 3.

[xiii] Malatras, Skouloudi, and Koukounas. "Industry 4.0 Security," 4.

[xiv] Meg King, and Jacob Rosen, "AI Raises the Risk of Cyberattack – and the Best Defence Is More AI," World Economic Forum / Wilson Center, April 4, 2019. https://www.weforum.org/agenda/2019/04/how-ai-raises-the-threat-of-cyberattack-and-why-the-best-defence-is-more-ai-5eb78ba081.