3 cybersecurity risks for 5G networks – and how to mitigate them

- Title ideas – 3 cybersecurity risks for 5G networks – and how to mitigate them
- Potential cybersecurity loopholes in 5G networks
- Why 5G networks are disrupting the cybersecurity industry
- Why do 5G networks require a new cybersecurity approach?

A major wave of change is coming to the wireless world. 5G mobile towers are cropping up in cities from Boston and Seattle to Dallas and Kansas City. This 5th Generation wireless network is touted to bring a new level of speed and reliability to the mobile browsing experience. With the exponential growth of smart devices and the Internet of Things, current 4G networks are straining to meet bandwidth demand. 5G promises to deliver increased capacity and energy efficiency, at a fraction of the cost.

However, the adoption of any new technology is always fraught with challenges. The transition to 5G will not happen at the press of a button. Initially, 5G will work in parallel to 4G networks, as physical infrastructure is overhauled. Devices and network technology will need hardware upgrades to adapt to the new system. Eventually, 5G will be released as an all software network that can be maintained like any other digital system today.

"The race to 5G is on and America must win," President Donald Trump said in April. While politics and media have defined this race as which nation gets 5G built first, the tougher race is to retool and secure this network. Because of the cyber vulnerabilities of software, the ecosystem of 5G devices and applications could pose a serious security risk, not just to individuals but also to the nation.

Let us look at three key cyber security risks for 5G Networks and what can be done to minimize them.

Risk factor 1 - Exponential increase in attack surface from 4G

A network's attack surface is the total of access points that can be exploited by a hacker. 5G's dynamic software-based systems have far more traffic routing points than the current hardware-based, centralized hub-and-spoke designs that 4G has. Multiple unregulated entry points to the network can allow hackers access to location tracking and even cellular reception for logged-in users. This new architecture also makes current cybersecurity practices redundant, opening up the network to dangerous attacks.

Risk mitigation – Early planning and investment in security infrastructure upgrade

5G technologies require a complete rethink of network security, which is not possible without significant funding and executive support. This is a shared responsibility between both governments and 5G businesses. Government policies need to take into account where current market-based measures and motivations fall short and how they can be addressed. We need to invest now before we become dependent on insecure 5G services with no sustainable cybersecurity plans in place.

Risk factor 2 - Nonexistent security standards for IoT devices

Many IoT devices are being manufactured with minimal or non-existent cybersecurity measures. These devices are already being used by hackers as entry points to enterprise networks. We may soon live in a world where billions of everyday devices, from toothbrushes to coffee machines, could be connecting to the Internet automatically. In the future, such unsecured IoT devices could easily allow for Man-In-the-middle attacks. A cybercriminal could intercept and change sensitive communication over 5G - causing espionage, civil unrest, or even war.

Risk Mitigation – IoT manufacturer incentive and consumer education

Just like the FCC (Federal Communications Commission) grades radio systems, we could have a new regulatory body to oversee IoT devices. But it is important to plan for a scenario where IoT manufacturers may still not comply with new regulatory frameworks. This especially holds for low-end IoT brands, which just may not be able to afford the added cost of production. Incentives like market monopoly or logistics support for complying brands will be required to effectively regulate the IoT market.

Moreover, 5G security is only as strong as its weakest links. Despite regulation, a wide variation in security quality may still exist. Customer education on how to choose and use IoT devices safely will be crucial. For example, labeling standards may need to be introduced to indicate which devices are secure and which are not.

Risk factor 3 – Dynamic Spectrum Sharing make network partitioning more complex

Current 4G systems use network partition methods to limit cyber attacks. Networks are subdivided by hardware to prevent the existence of a single point of failure. If one node of the network is attacked, it can be 'quarantined' to limit the attack, without acceding control of the whole network. On the other hand, 5G uses short-range, low-cost, and small-cell physical antennas within the geographic area of coverage. Each antenna can become a single point of control. Botnet and Denial of Service (DDoS) type attacks can bring down whole portions of the network simply by overloading a single node.

Also, 5G uses Dynamic Spectrum Sharing, a telecommunication system that breaks data packets into 'slices'. Each 'slice' from different, parallel communications, is sent over the same bandwidth. Each slice thus contributes to its cyber risk degree.

Risk Mitigation – Artificial Intelligence and Machine Learning in network management

The dynamic nature of 5G's network architecture requires a dynamic and fast learning management system. Software-based and Intelligent computing solutions are required for effective countermeasures. AI-powered cyber solutions will continue self-learning and updating themselves. AI and machine learning can serve as powerful tools for 5G cybersecurity.

Best cyber security practices for adopting 5G networks

If you plan to switch to 5G networks, here are some things you can do to protect data misuse and system tracking from your devices.

1. Use a VPN when connecting any device to the Internet. You can do this by implementing VPN routers in your home.
2. Set up complex passwords for all personal devices. Change default passwords on any IoT devices you may have at home.
3. Update your computer, phone, and other devices regularly. Set up and use anti-virus software and critical devices.