Cyber Security Risks of 5G IoT Demand Proactive Measures

The fifth generation of mobile networks, or 5G, promises to revolutionize the way we communicate and live. With faster speeds, lower latency, and massive connectivity, 5G provides the perfect environment for IoT devices and applications. But the significant cyber security risks of 5G IoT require organizations to evolve their security strategies accordingly.

5G Expands Capabilities for IoT

By delivering high bandwidth and real-time connectivity, 5G enables new applications such as self-driving cars, telemedicine advances, and smart cities. These applications involve massive deployments of IoT devices. In fact, some estimates suggest that by the end of 2023, over 17 billion IoT devices will be connected to the internet.

For example, 5G enables powerful, life-saving advances in medicine. Wearable devices allow for remote monitoring of a patient's vital signs, glucose level, and medication adherence. Robotic surgery provides rural patients access to specialized surgeons in faraway cities. And highly infectious patients can have substantive doctor visits without entering the clinic or hospital.

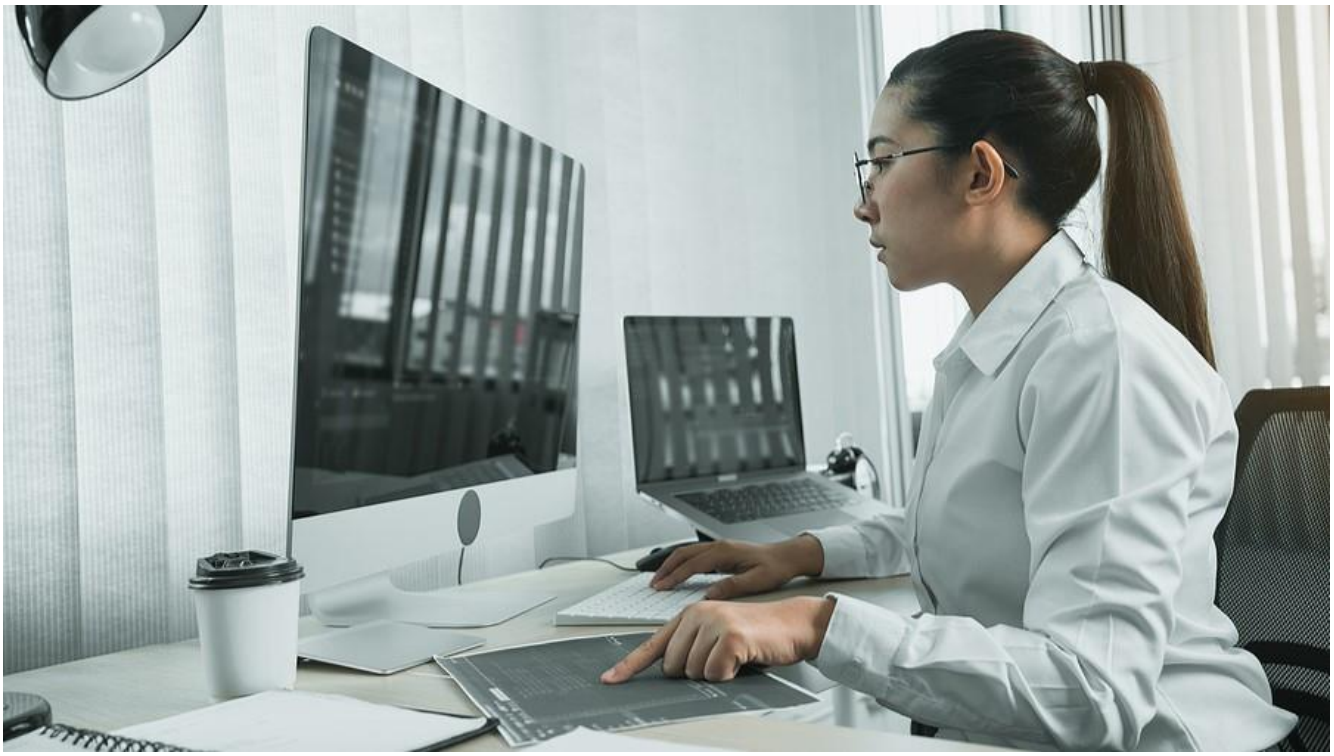
Likewise, 5G IoT expands the capabilities of smart cities. For instance, by supporting real-time data collection from traffic cameras, sensors, and vehicles, 5G helps to optimize traffic flow and prevent accidents. It can also enhance public safety by enabling faster emergency response and providing both video surveillance and facial recognition.

Hyperconnected Environment Introduces Security Challenges

However, the very real benefits of 5G IoT also introduce increased cyber security risk. In the first place, each new IoT device adds another potential entry point for attackers, greatly increasing the

attack surface. And because IoT devices are typically always on, they present particularly appealing targets.

Secondly, IoT devices are designed for function rather than security. And consumers typically neglect to change default configurations or install updates. Thus, hackers can often easily insert backdoors or zero-day malware into the network through the device. Additionally, devices frequently have too liberal access by default, access hackers will not hesitate to exploit.



For example, distributed denial of service (DDoS) attacks aim to overwhelm a target system with a large volume of traffic, making it unavailable for legitimate users. Attackers take advantage of the weak security of IoT devices to create large-scale botnets and launch attacks on 5G networks.

The weak security of IoT devices also increases the risk of supply chain attacks. If developers neglect to implement strict quality control and security by design for their devices, hackers can introduce vulnerabilities before the device has even been installed.

Additionally, 5G IoT generates, transmits, and stores a huge volume and variety of data. This often includes sensitive data such as personal health information. Without strong encryption and careful access control, organizations run the risk of significant data breaches.

Holistic Approach Mitigates Cyber Security Risks of 5G IoT

A comprehensive, multi-layer security approach will help reduce the risks posed by 5G IoT. Some cyber security best practices in this environment include the following:

- Choose IoT devices carefully – When choosing devices to add to the organization's network, look for devices that provide the ability to customize settings and features. Also choose devices

with the ability to receive regular security updates and patches. And stick to providers that make security a priority in the products they develop.

- Enforce strong password and authentication policies – Always replace the default passwords on IoT devices with strong passwords. And invest in strong device authentication.
- Install device firmware updates in a timely fashion – If devices cannot receive automatic updates, monitor device status and apply patches as soon as possible.

- Update device configuration and access – Before enabling an IoT device, disable any risky or unnecessary features. For instance, disable remote access unless necessary for the device to complete its job. Enable security features, including antivirus and firewalls.
- Implement network segmentation – Segment IoT devices away from the rest of the network. This allows for increased IoT security and ensures that hackers cannot use IoT devices to gain access to the rest of the network.
- Educate users at all levels – Everyone from network operators to end users needs to understand the security risks and best practices associated with the IoT. Update security policies and training programs regularly to cover 5G IoT concerns.

Partner with Cyber Security Experts

While 5G presents critical opportunities for growth and innovation, companies must balance new technologies with a proactive approach to security. Work with the security experts at eMazzanti to implement comprehensive cyber security designed for safe computing in a 5G world.