5G & IoT vs Cyber Security

Addressing the Elephant in the Room

Naman Agrawal & Neeraj Sinha

Image credit: Flickr

WITH hackers trying to break into a computer every 39 seconds on an average, cybersecurity continues to be the number one "external concern" for Indian policymakers and industry leaders, regardless of their industry. The annual costs of these attacks are expected to reach an incredible $6 trillion by 2021, according to Cyber Security Ventures (https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/).

As a result of this data privacy crisis, major companies are boosting internal investments in cybersecurity and collaborating with industry tycoons to protect their customers' data. Looking forward, 2020-21 promises to be the year when several cybersecurity trends converge. 5G and the Internet of Things (IoT) will also add billions of internet-connected devices into the world. Each of these is a potential target for hackers. Further, the tech talent crisis will continue to affect the data privacy sector disproportionately. That is because the number of job openings for cybersecurity experts is increasing faster than the supply of these specialists.

Image credit: Pxfuel

5G and IoT

The fifth generation of wireless technology is already here. Telecommunications companies like Reliance, AT&T and Sprint have begun testing and rolling out 5G service in major cities of the world, and consumers are expected to have full access to the technology by the end of 2021.

5G tech is important because it will make IoT a reality. This interconnected network of internet-enabled devices already exists. However, its potential is limited by the slow speeds of 4G wireless. The ultra-fast 5G network will allow these devices to transfer exponentially more information, with download speeds of up to 10 Gbps.

The upcoming 5G rollout is one reason why experts predict that more than 36 billion devices will be connected to the internet by the end of 2020 (https://www.pcr-online.

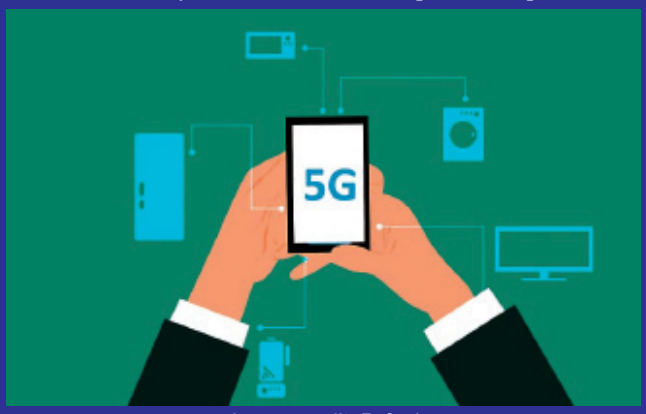

Image credit: Pxfuel

biz/2020/01/15/2020-will-be-a-smarter-year-for-retail/). Unfortunately, all of them will be exposed to security threats. In fact, research has found that the "first wave of IoT attacks" had already begun in 2016.

This makes the expanded IoT a nightmare for cybersecurity experts, who must figure out how to protect cell phones, security systems, vehicles, smart homes and more devices from being breached. The types of vulnerabilities and threats on IoT Devices include:

- **Cyber espionage:** It involves the utilisation of cracking techniques and malicious software to conduct surveillance on the targeted users to gain access to personal information on the existing systems.

Image credit: Pixabay

- **Instinctual force attack:** It simply means making attempts to guess users' passwords with the help of automated software, which makes multiple attempts unless it gets the right password to gain access.

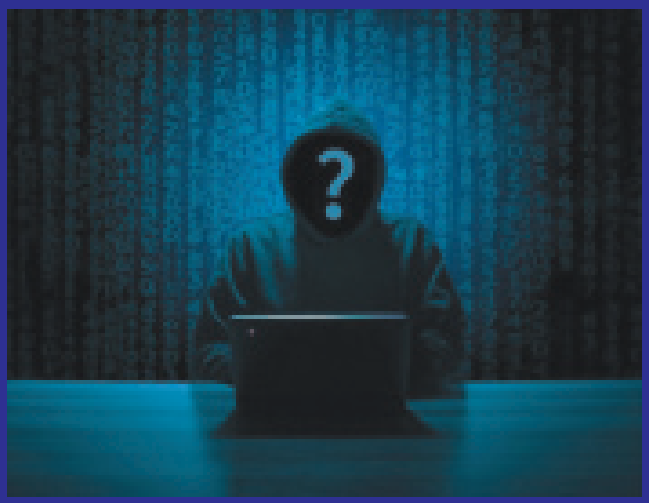

Image credit: Needpix

Software developers must respond to these threats by integrating security patches into the devices and waiting to release electronics until security has been fully tested and assured. Some of the most common types of attacks to prepare for are botnets, distributed denial of service, Radio Frequency Identity (RFID) spoofing, trojan viruses, malware and malicious scripts.

Protecting IoT Systems and Devices

IoT security methods vary depending on your specific IoT application and your place in the IoT ecosystem. For example, IoT manufacturers should concentrate on building security from the start, making hardware tamper-proof, building secure hardware, ensuring secure upgrades, providing firmware updates/patches and performing dynamic testing. A solution developer's focus should be on stable software development and reliable integration. For those deploying IoT systems, hardware security and authentication are critical measures. Likewise, for operators, keeping systems up to date, mitigating malware, auditing, protecting infrastructure and safeguarding credentials is essential.

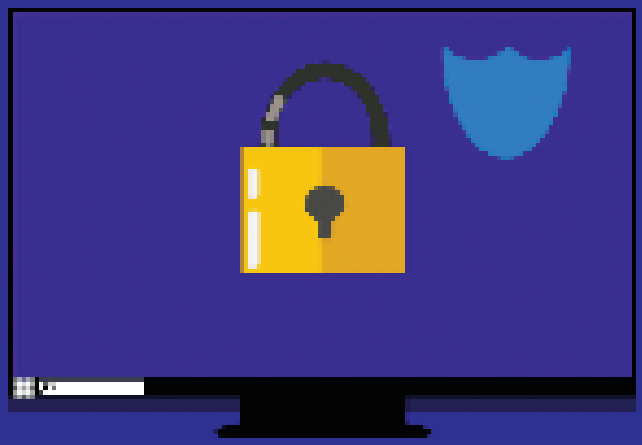

Image credit: Pixabay

Some common IoT security measures include:

- **Network security:** Protecting an IoT network includes ensuring port security, disabling port forwarding, and only supervised opening of network ports. Use of anti-malware, firewalls and intrusion detection system/intrusion prevention system, blocking of unauthorized IP addresses, and ensuring systems are always patched and are up to date.
- **Security gateways**: As an intermediary between IoT devices and the network, security gateways must have more computing power, memory and functions than the IoT devices themselves. In this way, they can implement functions such as firewalls to ensure that hackers cannot access the IoT devices to which they connect.
- **Strong encryption** measures are crucial for securing communication between devices. Data storage and transmission should be secured using cryptographic algorithms.
- **Inclusion of security measures in the design and production phase:** IoT developers should include security measures at the start of the development

of IoT devices. Ensuring system and data security by default is as critical as is deploying the latest operating systems and using secure hardware.

- **User sensitization**: Users must also be informed about the dangers of IoT systems and about measures that they can take to ensure security from time to time, which could be as simple as updating the default credentials and applying software updates.

International Data Privacy Regulations

With the development of extremely fast 5G networks and constantly improving smartphones, the enormous data generation presents significant security threats. Governments across the world are also responding to the global cyber security crisis by creating new regulations that govern the way companies handle and store valuable consumer data. This includes important information such as personal identification, banking, and credit card numbers, and purchase history.

The European Union, in particular, has been a leader in this field. One of its pioneering efforts is the General Data Protection Regulations (GDPR), which was passed in 2016 and went into effect in Spring 2018. It impacts all companies that do business with European customers, regardless of where the company is located.

The GDPR requires that companies receive consent from consumers before processing data, collect and store data anonymously, and notify the customers when their information has potentially been breached. It also requires large businesses to appoint a data privacy protection officer to oversee the implementation of the regulations.

Furthermore, while the U.S. federal government has yet to create a set of strong data privacy protections, several states have drawn up their legislation, including Hawaii, Massachusetts, Maryland, Mississippi, New Mexico, and Washington.

Though it is not a party to any convention on the protection of personal data, which is equivalent to the GDPR, India has adopted international declarations and conventions such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which recognize the right to privacy.

The Indian government also amended the Information Technology Act (2000) ("IT Act"), which gives right to compensation for improper disclosure of personal information. The Indian government subsequently issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, imposing additional requirements on commercial and business entities in India relating to the collection and disclosure of sensitive personal data or information.

Human Resource Crisis

Perhaps the most important cybersecurity challenge that will be faced by Indian corporates is the shortage of cybersecurity experts. Research conducted in the past year demonstrates that 53 % of IT workers report that their company is short on cybersecurity skills – an increase of 11% since 2016. What is more, 69% of cybersecurity experts said that their team is understaffed.

Today, more than 58% of cybersecurity experts have also reported that their organisation has unfilled information security roles. That's a major reason why Cyber Security Ventures recently estimated that the global shortage of cybersecurity would reach 3.5 million unfilled positions by 2021.

Unfortunately, there's no end in sight to this crisis. The number of cybersecurity openings continues to grow rapidly, while universities are still graduating the same, small amount of qualified information security experts.

Businesses must increase their compensation packages and other benefits in order to compete for the limited number of data privacy specialists. In addition, companies will have to focus on internal training programmes to develop cybersecurity experts in-house while simultaneously partnering with software outsourcing firms across the world to fill the talent shortage in the meantime.

Cyber Security – Top Priority

Cybersecurity is expected to remain the top priority for Indian policymakers and corporates over the next several years. That's because the number of data breaches is rising, and hackers are increasingly using sophisticated techniques like AI to break into well-protected systems. Countries such as India, which are riding a wave of digitisation, must brace themselves for the looming security challenges. Policymakers of the countries have to take proactive measures to develop innovative mechanisms to leverage the IT Potential of the country.

Image credit: Pixabay

Finally, the global rollout of 5G wireless technology, combined with the expansion of IoT, means that more vulnerable devices will be connected to the internet over the next several years. This will add up to the cybersecurity challenge and will need a dedicated response from all the stakeholders.

Mr Naman Agrawal (naman.agrawal@nic.in) is Senior Associate, NITI Aayog and Mr Neeraj Sinha is Adviser, NITI Aayog.