Infosys®
Navigate your next

VIEW POINT

5G: NEW CYBERTHREATS

As 5G networks begin to be deployed, nations are scrambling to have a stake in its development. For all its promise, like any technological advancement, 5G will not be without risks. Businesses will have to carefully consider their initial steps toward adopting this new technology.

Infosys® | Knowledge Institute

5G: new cyberthreats

A new network standard, 5G, is at the epicenter of a geopolitical storm. Superpowers are battling over implementation of this new technology, and political frictions among traditional allies are increasing. Beyond the politics, however, there are grounds to be concerned about the new cyberthreats that could emerge as 5G is adopted and new applications, services and use cases are designed. If the 4G generation is any indicator, businesses and consumers need to prepare for unexpected impacts affecting infrastructure, information and even social structures.

Is 5G causing a global conflict?

Since the beginning of 2019, the United States has expressed fear that the Chinese government could employ Huawei's 5G wireless hardware in espionage operations abroad. While Huawei rejects these allegations, the United States has taken steps to ban the use of Huawei's equipment. Australia, Japan and New Zealand have followed suit.

Despite Huawei's fervent denial that it acts for the Chinese government, various U.S. officials have raised concerns that there is, nevertheless, a possibility that Huawei could be forced to turn over information and to work with Chinese state intelligence agencies.

Whether Huawei's close ties with the Chinese government are part of a conspiracy or not, it is undeniable that the battle over 5G technology development is a new source of international tension.

Global conflict has always evolved hand in hand with technological advancement. The 20th century saw automated weapons replacing manual rifles and cavalry on the battlefield. Today, cyberspace presents a new front for conflict with technological instruments that can silently, and in a matter of seconds, disrupt infrastructure.

The 5G networks are a new battlefield where countries see a strategic opportunity to demonstrate their influence.

While these political frictions continue, do businesses and consumers need to be concerned? It is impossible to predict all 5G-related threats, but it is worth assessing the following three categories of risk: infrastructure, information and societal.

5G is at the epicenter of a geopolitical storm

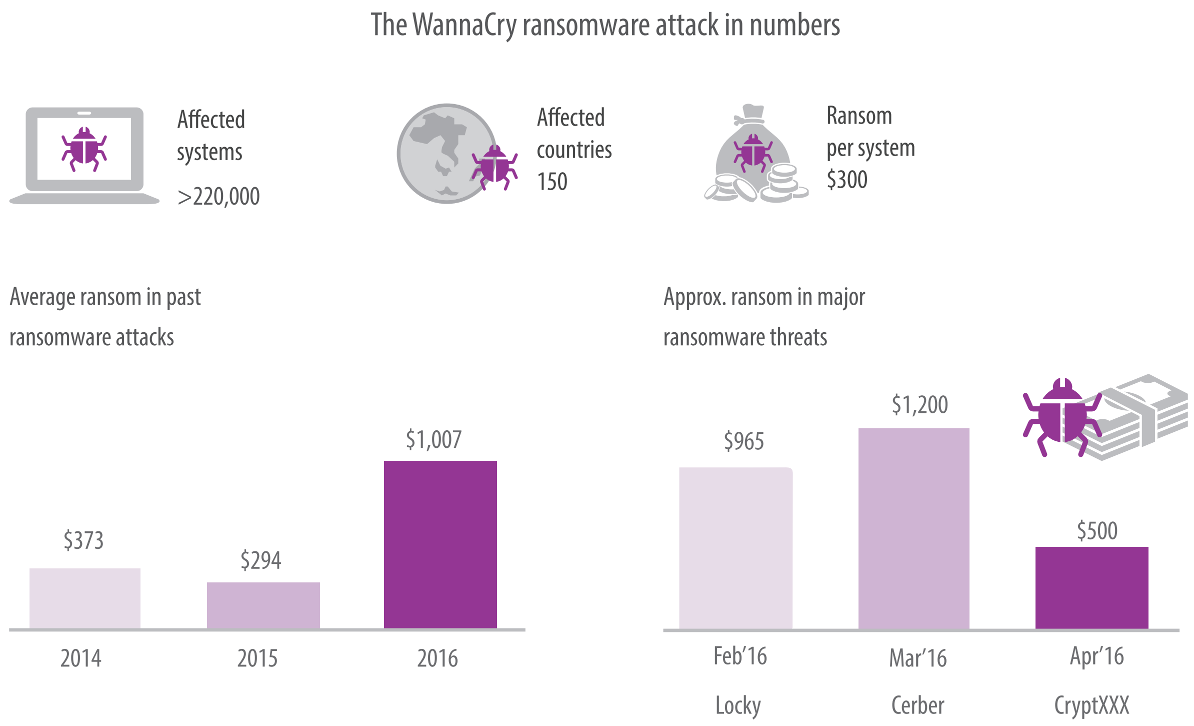
Infrastructure risks

In the modern world, people increasingly rely on technology and have become more interconnected through internet of things (IoT) devices. Such devices can be monitored remotely through software applications. But as IoT platforms become more popular, integration of machinery with upgraded software becomes tricky, and sometimes even lethal. For instance, it is widely believed that software-hardware integration issues were potential causes of the Boeing 737 Max jetliners' tragic crashes in October 2018 and March 2019.

Besides the software-hardware integration issues, the most destructive threat to critical infrastructure is the possibility of an unexpected cyberattack. With 5G providing the opportunity for additional critical equipment to go online, the risks of a catastrophic blackout will grow. An incident in 2016 involving a Ukrainian power outage connected with a cyberattack not only demonstrated the vulnerabilities of existing infrastructure systems but also showed a real-life scenario in which hackers took control of a country's power grid. Implementation of 5G networks could theoretically increase the number of connected devices, and the complexity of providing security to the system would grow exponentially.

Furthermore, the development of malware requires significant resources and research available only to national governments. In previous years, the world saw state-sponsored cyberattacks, and in the 5G era they could become more frequent. Take, for example, the 2017 WannaCry ransom attack.

Figure 1: The impact of the WannaCry and other ransom attacks globally



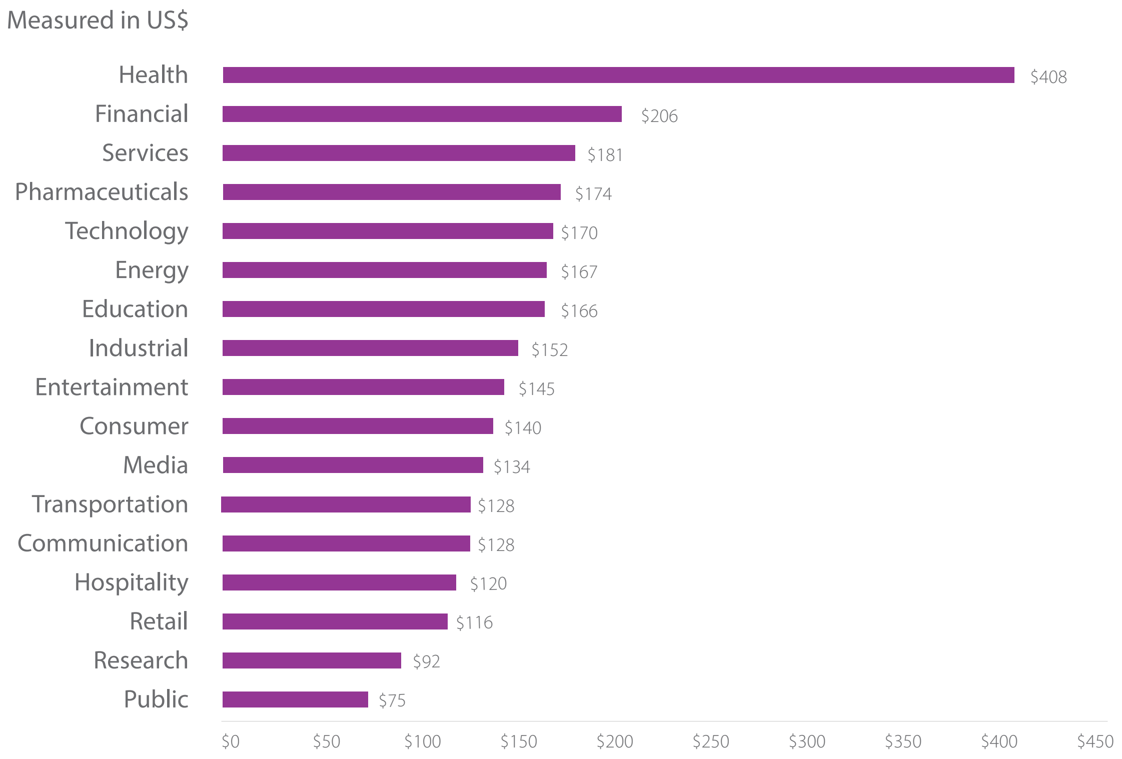
Source: Statista

The virus affected computers in 150 countries across North America, Europe and Asia, and the attack was the largest ransomware delivery campaign to date. The cyberattack hit over 200,000 computers worldwide, including those of the National Health Service in the UK.

Another example of malware is Stuxnet, an Israeli-American computer worm that caused disruption in nuclear power plants in Iran. The virus, which was designed to produce physical damage, found its way to the Natanz uranium enrichment plant and caused the failure of several centrifuges. As tensions between China, the U.S. and other countries continue to escalate beyond trade wars, businesses and governments should expect more and more reports of subtle cyberattacks.

As more infrastructure components get connected faster and more often through 5G, the risk of design errors increases, as does the complexity of defending against outside attack.

Figure 2: The large per capita costs of data breaches by industry



Source: 2018 Cost of a Data Breach Study: Global Overview[1]

Information risks

The past few years have shown how the availability and access to data cause significant informational risk. In particular, the current 4G wireless networks have, in recent years, already presented significant struggles for cybersecurity, partially as a result of the ease of maneuverability in cyberspace. Hackers and the like can remain anonymous and be located in any part of the world.

The evolution of 5G networks makes governments and businesses more vulnerable because of increasing connectivity and lower latency (response times).

For instance, hospitals are utilizing more IoT devices to deliver better patient experiences and facilitate workflow. The IoT prompts medical devices to collect valuable data, provide remote care and monitor health. Patients can receive care without leaving their homes. Importantly, telehealth will benefit rural communities. But along with the benefits exist real threats: compromised privacy and medical identity theft. IoT devices will store personal data, which will increase information risks by creating more attack vectors.

The health care industry is especially attractive to cybercriminals who know that patient data is a matter of life and death. By gaining access to patients' records, a malicious actor can manipulate sensitive information that could change crucial diagnostics.

Figure 2 shows the costs of data breaches by industry. Health care is clearly the most heavily impacted, though its costs are also significantly larger than other industries because of the high notification costs and the steep penalties in the U.S. for health care information mismanagement.

An increasing number of ways to penetrate a network will likely increase the risks of distributed denial-of-service attacks (DoS). In October 2016, the world saw an attack by a botnet that targeted Dyn, a major DNS provider, and compromised IoT devices. The attack disrupted sites like Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit and GitHub. The resolution of the attack took place within one day; however, one may wonder how quickly an attack would be resolved in a 5G-connected world.

Figure 3: Wireless networks have evolved to deliver faster downloads at lower latencies

	1G	2G	3G	4G	5G
Approximate deployment date	1980s	1990s	2000s	2010s	2020s
Theoritical download speed	2kbit/s	384kbit/s	56Mbit/s	1Gbit/s	10Gbit/s
Latency	N/A	629 ms	212 ms	60-98 ms	< 1 ms

Source: GSMA: Mobile Broadband: The path to 5G[2]

Societal risks

Fourth-generation, or 4G, wireless networks paved the way for smartphones. The 4G networks outperformed 3G networks and improved the user experience on social media, allowing users to share ideas and views through pictures, videos and music.

But together with increased download speed and lower latency, 4G also created more unknown societal risks by enabling political mobilization and manipulation from the use of instant and video messaging to organize protests that culminated in the Arab Spring, to the use of forums and social media to distribute alt-right ideologies. Today's society is being changed by people's access to data on the move.

And it is not just on the extreme ends of the political spectrum where this has occurred. For example, in 2015 Cambridge Analytica, a data analytics firm, harvested information from millions of Facebook profiles of U.S. voters in an effort to predict election results and alter voting behavior.

"We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on,"[3] said whistle-blower Christopher Wylie.

Another example of societal risk is the 2016 story that Russian hackers tapped into emails of John Podesta, Hillary Clinton's presidential campaign manager, and leaked information to Wikileaks. Wikileaks, in turn, made information available for public usage. The cyber episode is a vivid example of the penetration of a secured systems and extraction of highly sensitive information. Through actions in cyberspace, it is now possible to alter public opinion and change the course of political events.

When 4G promised to enable Facebook to engage more closely with people's lives, few would have envisaged that information previously thought to be private on the platform might be used to manipulate their opinions. 5G could provide for more, yet unknown, ways to spread propaganda.

Cybersecurity is key

Most of the above-mentioned risks occurred as a result of gaps in cybersecurity. To manage early detection and effectively respond to the risks, it is crucial to have a proactive cybersecurity approach.

"Most businesses have a reactive approach toward security, not thinking about it at all until they get compromised or breached," says Vinod Muniyappa, head of Infosys's security practice. "Looking at the past data, the cost of a security breach today is ten times higher than it used to be. To be protected from cyberattacks, companies need to be secured by design. Today, cybersecurity is no longer only about regulatory compliance. It involves many elements — how to secure the enterprise, how to secure custom and employee information."

As the development of a fifth-generation network will inevitably present more opportunities for abuse, it is of major concern to businesses and consumers to eliminate, as far as possible, incidents of weakness in cybersecurity.

Will 5G greatly affect cybersecurity and create more risks?

Innovation in any technology and business model always comes with risks, explains Mr. Muniyappa.

“While 5G is promising great benefits, we will be able to identify the risks it presents only after it is in use. But cybersecurity will evolve, and has always done so. Two years ago, there were concerns about the insecurity of the cloud. But today the cloud is a very good option, and vendors have been able to address the risks. They may have not mitigated the threats entirely, but they continuously strive to improve and make it more secure.”

Without risk there is no reward. 5G is becoming a new battlefield, and today we are witnessing global superpowers taking their place in the cyber arena.

New 5G networks are intended to be 10 to 100 times faster than an ordinary wireless connection and have significantly reduced response time.

More services mean more risks that need to be taken into account when considering potential threats. Just as any new technology is fraught with possibilities of misuse, 5G will also attract its share of abuse by those seeking to take advantage of the increasingly wirelessly connected world. Thus, enterprises need to shift their business priorities by identifying risks and trends and look at security proactively instead of dealing with it when it’s too late.

To learn more about the capabilities and limitations of 5G wireless networks, read our report “Is the Hype Around 5G Real?”[4]

References:

1. https://www.ibm.com/downloads/cas/861MNWN2
2. https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf
3. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
4. https://www.infosys.com/about/knowledge-institute/insights/Pages/hype-around-real.aspx

Authors

Samad Masood

Senior Principal – Infosys Knowledge Institute
Samad.Masood@infosys.com

Yulia De Bari

Consultant – Infosys Knowledge Institute
Yulia.Debari@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next