SATORI CONSULTING

5G WILL INCREASE CYBERSECURITY RISK

As the world anticipates the roll out of the 5G technology, consumers and businesses alike are looking forward to the new opportunities in communications and operational improvements that this will bring. At the same time, many are concerned that the myriad of the newly connected devices and higher data transmission speeds may mean new cybersecurity risks. In Satori's opinion, they are correct to be worried. For businesses, information security is especially important as many mission-critical processes may become reliant on 5G in the future. In this paper we discuss how 5G will likely impact the cybersecurity landscape.

Satori CONSULTING

New York, 212.918.4560

info@satoriconsulting.com

5G IS COMING

5G Roll-Out is Around the Corner

Global cellphone networks are preparing to bombard the public with advertising regarding the benefits of the latest innovation in cellphone technology: 5G, the fifth generation of the equipment and protocols on which their networks will soon run. So far, the 5G roll-out has been happening incrementally mostly using 4G equipment, with the first large-scale and fully fledged implementation planned for Tokyo during the 2020 Olympics. As protocol standards are finalized, spectrum is allocated and the equipment manufacturing and related security issues addressed (including the ongoing concerns relating to Huawei), the eventual wide-spread use of 5G appears inevitable.

Benefits for Consumers

For the public, the benefits sound compelling – most significantly, access to ~20x increase in data transfer speed and extremely low (0.1 millisecond) latency. This means, for example, that it should be possible to watch high-definition television broadcasts in real-time from your smart phone. However, the reality is likely to disappoint many, at least in the short-term, with high-bandwidth rollouts initially confined to first world cities with the highest population densities. Even then, a number of challenges are yet to be resolved, such as the difficulty, for some part of the spectrum, of transmitting through walls, which may make performance spotty within buildings.

Benefits for Business

For businesses, 5G implementation offers an opportunity for a true paradigm shift rather than an incremental improvement from 4G. In fact, when combined with other technologies such as Global Positioning System (GPS) and Internet of Things (IoT), 5G will allow a plethora of new solutions to be developed. For example, a private IoT at a manufacturing facility could increase productivity and safety by operating and tracking industrial robots. Other solutions will collect immense volumes of data from sensors and cameras that can be subjected to big data analysis and artificial intelligence (AI) applications to derive new insights on various aspects of customer behavior and business operations.

New Risks

Every major technology advance introduces new risks. We live in an age of increasing cybersecurity risk, and 5G is likely to introduce new challenges for businesses and Information Security professionals looking to stem the tide.

SATORI 5G FRAMEWORK

When considering the positive and negative impacts of 5G, Satori uses the model shown in the figure below.

Same Business Activity – Potential Improvement in Effectiveness/ Efficiency

In the medium-term, 5G will reinforce the move towards a Digital economy, attracting more and more business to the mobile platform. Consumers will continue to increase their time online and become even more comfortable with transacting on mobile, from the micro- to the macro-scale. While this may appear to be business-as-usual for businesses that are mobile enabled, it will ultimately change the risk factor – are you ready for a world where >90% of your business is mobile? What would be the impact of an outage of a few hours or even days? Could you afford a massive fine due to a data breach?

SATORI 5G CYBERSECURITY FRAMEWORK

Many businesses are already using the Internet of Things (IoT) for industrial control or to track product within the supply chain and/or once it has been delivered to customers. 5G will have the potential to transmit much richer data (more meta data) in both directions, allowing better control and tracking from early stages of production through to end of useful life. The downside, of course, is that IoT has historically been weak on security, and this needs to be fixed before businesses increase their reliance on it. Are your IoT devices making confidential information available to third parties? Are you opening up product and systems to control by unauthorized users?

Finally, 5G is likely to reinforce the Millennial generation trend towards different choices in work-life balance. It will become even easier to work from anywhere, facilitated by video links and near-instant data transfers. Gig working will also likely increase, as will Bring-Your-Own-Device (BYOD). Devices will become primarily conduits for communicating with the cloud where all the data storage and processing will occur (the Google Chromebook is a good early example of this). How will you control confidential data in a world of ultra-short-term contracts with equipment and data you don't directly control?

Same Cyber Threats – More serious Consequences

The bad news is that 5G will help bad actors as much as good ones. A particular concern will be the increased effectiveness of botnets, which have many applications in cyber-crime, including Distributed Denial of Service (DDOS) attacks, unauthorized cryptocurrency mining, and password cracking. 5G will increase the number of devices available for botnets, as well as allowing transfer of much higher data volumes to make their attacks more effective.

The impact of attacks of known types is also likely to increase, with infection rates from viruses and ransomware accelerating due to the higher bandwidth. When breaches do occur, it will be possible to exfiltrate much more data before being detected.

New Business Activities/Opportunities

Smart businesses will "Be Digital" and rapidly roll out new products and services that take advantage of what 5G has to offer. The risk is that in the rush to be first to market, security takes a back seat, with the business expecting to fix it in subsequent releases. The anticipated proliferation of bad actors makes this a highly risky strategy. There's no point in being first to market if you're also the first to have a major data breach!

Security needs to be a recognized and required element of the Minimum Viable Product (MVP) and this can only be achieved if the business adopts Security by Design and Privacy by Design principles up-front.

New Cyber Threats with As-yet-unknown Consequences

It's highly likely that bad actors are also looking at what 5G has to offer and inventing entirely new threats. These are "unknown unknowns", and therefore very difficult to protect against in advance.

Powerful actors, such as organized crime and state-sponsored hackers are well funded and can actively research new attacks – generating zero-day exploits known only to them. In addition, there is concern that states will be able to coerce suppliers into adding back-doors into 5G infrastructure.

Meanwhile, 5G will be built into entirely new products that have capabilities far beyond existing IoT devices. Self-driving cars and trucks are on the horizon, and there are many other opportunities where automation, Artificial Intelligence, and 5G networks will drive advances. Hacking these machines could cause chaos in the real world, or (less apocalyptic) make near unlimited computing power and bandwidth available for brute-force cyber-attacks.

We can be certain that cybersecurity will become even more important in the future. Businesses must prepare by ensuring that they have a well-considered and sustainable cybersecurity program that is able to detect and respond to a wide variety of threats.

IN CONCLUSION

While it's still early days, it is possible to predict that 5G will reinforce several social and business trends and interact positively with other technologies to transform many aspects of the way we live and work:

- Reinforcement of the Digital economy with greater reliance on online and mobile, including many entirely new products and services
- Increases in "work from anywhere" and BYOD
- Remote control and tracking embedded into everyday objects and devices.

Satori's Recommendations

While 5G will offer new business opportunities, they need to be implemented carefully in order to minimize the inevitable increase in cybersecurity exposure. In addition, businesses must be prepared for more effective and new cyber-attacks, intensified by the new technology.

To address these issues, we recommend:

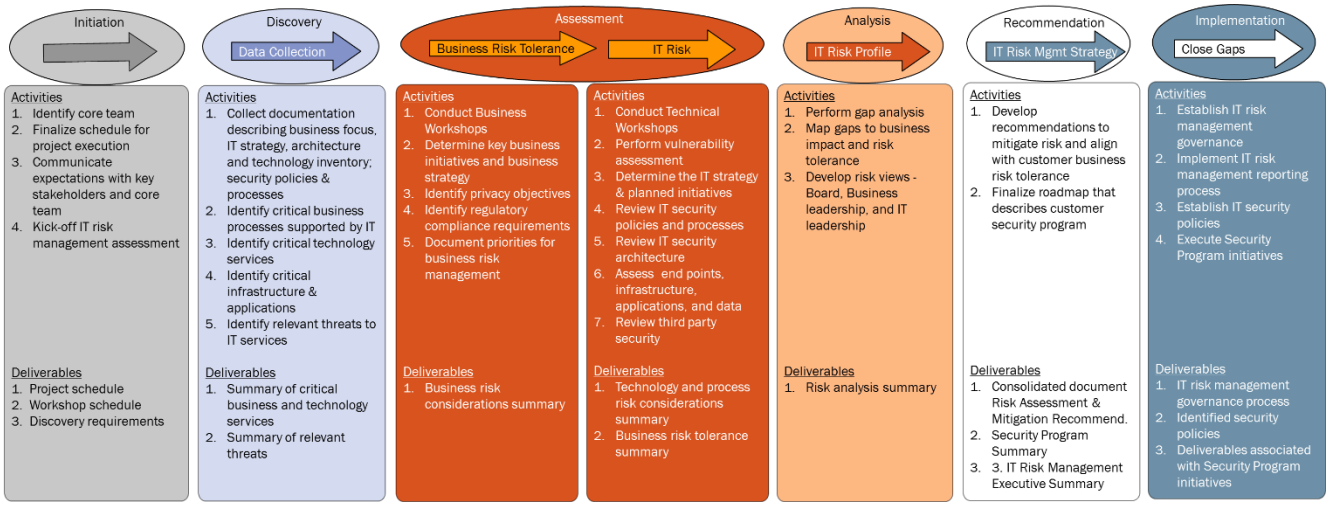
- Ensuring that a robust and effective cybersecurity program is in place before 5G becomes widespread
- Strengthening existing protections against attack, especially on externally accessible products and services
- Automation of cybersecurity monitoring and reporting in order to handle the increased volume of attacks
- Implementing policies and supporting technologies to ensure safe remote working and BYOD
- Assessing any existing IoT implementations and performing necessary hardening
- Implementing secure software development practices before developing products or services that exploit 5G.

With an effective cybersecurity program in place, businesses can be optimistic about the opportunities that 5G will afford.

HOW SATORI CAN HELP

Satori is a leading international management consulting firm with offices in New York, Chicago, Boston, Washington DC, and London. We have a dedicated cybersecurity practice that assesses, designs, and implements cybersecurity programs for many types of businesses across multiple industries. We deliver:

1. A proven methodology for assessing current cybersecurity capabilities and recommending improvements
2. A comprehensive set of cybersecurity policies and procedures, which can be adapted by program maturity, alternative business sizes, and industries
3. Seasoned practitioners with real-life experience of cybersecurity programs in a variety of contexts
4. Strong understanding of standards such as NIST and ISO, and how to apply them to ensure effective risk management and compliance with regulations (e.g., GDPR and HIPAA)
5. A collaborative working style and an emphasis on developing strong long-term working relationships.



Satori's Cybersecurity Program Stages

At Satori Consulting, our mission is simple—to work side-by-side with clients to discover opportunities and solve problems. We strive to provide both comprehensive and expert service, mindful of every client's unique needs. Our team of highly skilled management consultants brings a wealth of industry and functional experience to provide wide-ranging services in project and program management, risk management, change management, organizational effectiveness, strategy and advisory, business process engineering, performance management, and infrastructure and technology.

48 Wall Street
Suite 1100
New York, NY 10005

Phone 212.918.4560
Email info@satoriconsulting.com

www.satoriconsulting.com