TECHPLUS MEDIA Publication

ITPV

Connecting with Solution Provider in
EMERGING MARKET

Vol XII | Issue 8 | December 2022 | Pages 32

▪ Northern ▪ Eastern ▪ Maharashtra ▪ Gujarat ▪ MP & Chattisgarh ▪ North East ▪ Southern ▪ UP & Uttarakhand ▪ Bihar & Jharkhand

CYBER SECURITY IN THE 5G ERA: WILL SUPERFAST MEETS SUPERSECURE EXPECTATIONS?

Vishak Raman
Fortinet

Debasish Mukherjee
Sonicwall

Jaspreet Singh
Grant Thornton

Nilesh Gupta
3i Infotech

Dipesh Kaura
Kaspersky

Sonit Jain
GajShield Infotech

Stanislav Protassov
Acronis

Manoj Paul
Equinix India

Sakshi Grover
IDC India

Dhananjay Ganjoo
F5

Anurag Singh
Ingram Micro India

TECHPLUS MEDIA

Toner Box Series

Smartest choice for your business.

brother
at your side

WHY COMPROMISE, WHEN YOU HAVE A CHOICE. CHOOSE GENUINE. SAY NO TO NON-GENUINE.

GET QUALITY, WARRANTY, DURABILITY, LONGEVITY.

With ORIGINAL TONER COST 33 Paise* Per Page

2600 PAGES YIELD

₹940 MRP

TONER TNB021

34 Pages Per Minute

Duplex Printing

250 Sheets Paper Tray

2,600 Pages Inbox Toner

Cost Saving Toner Box Technology

SUPERIOR RANGE OF MONO LASER PRINTERS

DCP-B7535DW	HL-B2080DW	DCP-B7500D	HL-B2000D	MFC-B7715DW
MRP ₹ 25,290/-*	MRP ₹ 15,990/-*	MRP ₹ 18,990/-*	MRP ₹ 13,990/-*	MRP ₹ 26,990/-*

www.brother.in

FOR SALES ENQUIRIES: • WEST BENGAL & ASSAM : Raja Banerjee - 9007135395 / Soumavo Nandi - 8583010825, • **BIHAR :** Deepak Singh - 9771403031 / Amit Kumar - 9308475768, • **ORISSA :** Saroj Nayak - 9438362634, • **JHARKHAND :** Dilip Santra - 9334794315

*T&C Apply | Original toner cost per page is calculated on toner yield of 2600 pages (as per ISO/IEC 19752) at ₹846 | MRP mentioned above is for 1*unit and subject to change without prior notice

CONTENT

COVER STORY

IN CONVERSATION

NILESH GUPTA
Chief Cloud Officer, 3i Infotech

DEBASISH MUKHERJEE
Vice President APJ, Sales, Sonicwall

DIPESH KAURA
GM, South Asia, Kaspersky

ANURAG SINGH, Director,
Head of Advanced Solutions, Ingram Micro India

VISHAK RAMAN, Vice President, Sales,
India, SAARC and Southeast Asia, Fortinet

JASPREET SINGH, Partner, and Clients and Markets Leader – Advisory Services, Grant Thornton

Cyber Security in the 5G Era: Will Superfast Meets Supersecure Expectations?

5G is likely to usher in a new wave of opportunities for businesses, unlocking the next level of growth for the country. However, 5G may also open doors for new cyber threats. The high speed of data transfer may allow hackers to infect more data packages and spy on companies without being noticed. This cover story will analyze the unforeseen threats, cyber security risks, and risk management framework that enterprises must be aware of

Amit Singh

With the recent 5G launch in India, the digital revolution is well underway and in the coming decade it will take on even more significance as connectivity comes to underpin every aspect of our lives, from industry to utilities. Indeed, 5G promises to deliver increased capacity and energy efficiency at a fraction of the cost.

Faster connectivity speeds, ultra-low latency, and greater bandwidth are bound to advance societies, transform industries, and dramatically enhance day-to-day experiences. However, when it comes to security, the 5G platform is yet to prove itself as a truly resilient system.

“5G private networks are rarely entirely isolated from the enterprise IT environment or external environments (partners, integrators, public cloud, etc.) and may be exposed to internal and external attacks and risks.”

VISHAK RAMAN, Vice President, Sales, India, SAARC and Southeast Asia, Fortinet

“5G software-defined network does not provide for chokepoint inspection and control as such activities are pushed outward to a web of digital routers. Further, a shift from physical appliances to virtualization will make the network vulnerable to attacks.”

DEBASISH MUKHERJEE,
Vice President APJ, Sales, Sonicwall

High stakes on 5G

Enterprises are putting high stakes on 5G as they line up their priorities over

“Researchers have identified shortcomings in 5G NSA installations that enable downgrade attacks, in which a phone’s connection is altered to downgrade to older networks, providing cybercriminals with access to vulnerabilities in 3G and 4G services.”

JASPREET SINGH, Partner, and Clients and Markets Leader – Advisory Services, Grant Thornton

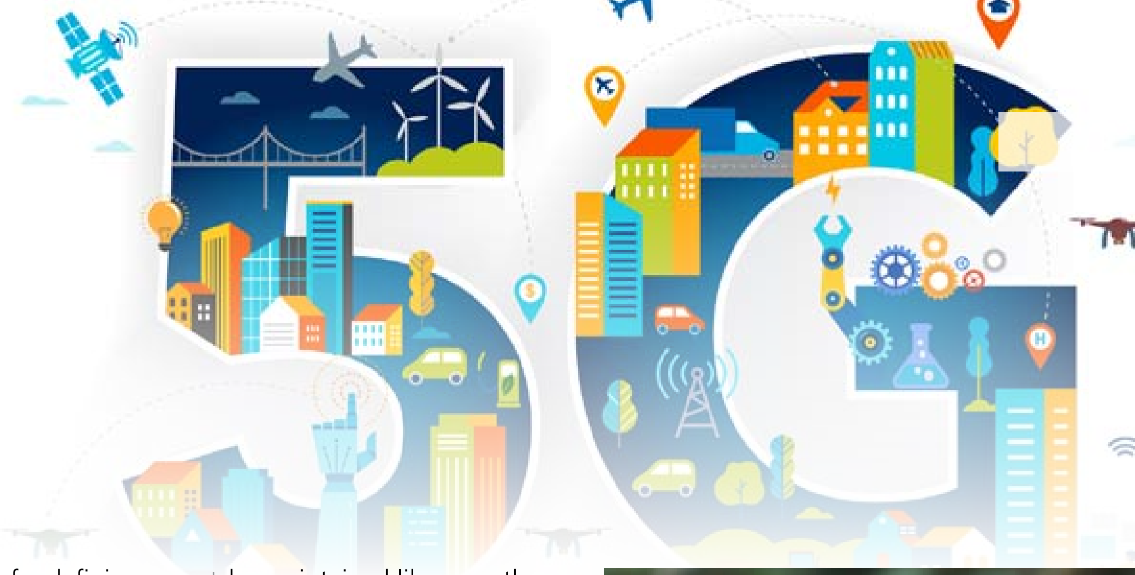
the next couple of years. As per IDC’s Asia/Pacific Connected Enterprises Survey, 62 percent of enterprises in India mentioned that network flexibility especially network slicing makes 5G more attractive to them than previous radio generations. This is followed by 55 percent that mentioned that significantly higher speeds than 4G seems to be an attractive point.

Another report from EY says that as many as 70 percent of enterprises are expected to make the highest investment in 5G in the next three years as compared to other emerging technologies. Smart manufacturing, immersive content, and cloud gaming will be the top 5G use cases, it said.

Interestingly, half of the enterprises surveyed said that they have limited clarity on 5G policy and regulations. The report highlights the

“We need a 5G network service that is built on an open, programmable, reliable, and software-driven Intelligent Cybersecurity Mesh that treats the internet (IP) itself as Zero Trust and relies heavily on strong encryption for all data transmitted, processed, or stored anywhere on it.”

NILESH GUPTA, Chief Cloud Officer, 3i Infotech



significance of redefining cyber security strategies as vulnerabilities get heightened by the distributed and virtualized nature of 5G networks.

The need for strengthened security is further intensified by a recent Fortinet survey around security in enabling 5G adoption in business verticals. Almost 90 percent of respondents stated that the mobile network operator's security capabilities are either critical or very important for success in vertical industry use cases. More than 80 percent consider native 5G security features as important. Moreover, 54 percent of respondents believe operators should offer a shared responsibility model; over 86 percent believe operators should offer full-stack security.

Challenging traditional approaches in cyber-security

The adoption of any new technology is always fraught with challenges. During the transition to 5G, it will initially work in parallel with 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.

While 5G capabilities continue to advance, the realization of a connected future hinges on ensuring trust and security. As networks become increasingly software-based and decentralized, their attack surface will widen and the number of potential entry points will expand, introducing new threat vectors and vulnerabilities. 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.

The biggest challenge will be the sudden, exponential growth of the attack surface due to the rapid expansion of IoT devices and edge-based computing says Vishak Raman, Vice President, Sales, India, SAARC and Southeast Asia, Fortinet. "This will be followed closely by the fact that these devices won't necessarily be connected to a central network in a traditional hub-and-spoke configuration. With literally billions of IoT devices interconnected across a meshed edge environment, any device can become the weakest link in the security chain and expose the entire enterprise to risk," he adds.

> “DSS works by broadcasting 4G LTE and 5G NR cellular wireless over the same frequency to allocate more spectrum resources to new technology as more users switch to 5G. For DSS to work, both technologies need to cooperate in tandem, creating added complexity.”
>
> DIPESH KAURA, GM, South Asia, Kaspersky

In addition, higher speed and more devices used by the 5G network will create a deluge of data which will increase the network traffic and attack surface. "It would result in lower network visibility, which might attract cybercriminals and escalate data extraction. Additionally, high throughput

5G networks open doors for network and application layer attacks risking the protection of sophisticated networks of connected devices, where compromising one device can infect the whole network," shares Dhananjay Ganjoo, Managing Director, India & SAARC, F5.

Jaspreet Singh, Partner, and Clients and Markets Leader – Advisory Services, Grant Thornton elaborates that data exfiltration attempts on 5G networks are more lucrative for cybercriminals since a lot more data is transferred in a given amount of time. "An aspect of weakness is also the software's integrity, particularly when it originates from open sources and the entire software distribution network. The significant increase in bandwidth that enables 5G also opens up new attack vectors. Small-cell antennas with a short range and low budget that are widely used in urban areas are now deemed critical threats," he says.

> 5G aims to improve the authentication between the base stations and the core network as well as further strengthen subscriber protection against man-in-the-middle attacks over the radio.

STANISLAV PROTASSOV,
Co-Founder & Technology President, Acronis

> DSS has a marginally negative 25 percent and 15 percent influence on the performance of 4G LTE and 5G NR, respectively. The performance hit is often well worth having the entire spectrum accessible to both networks.

SONIT JAIN, CEO, GajShield Infotech

Further, network slicing and each segment being

accessed by multiple vendors all at once leads to improper network management, and also a potential security risk with 5G implementation, which can lead to the presence of untrusted and malicious core components to edge networks. "The proliferation of connected end-user devices and increased connectivity can lead to the exposure of encryption keys resulting from lack of stringent configurations and data governance policy violations. Apart from this network virtualization by-pass, API exploitation, and lateral movement within the core network can steer the way to expanded attack surfaces such as radio access network threats, core network threats, network slicing, NFV-SDN threats, and user equipment threats, to name a few. At the same time, dealing with the existing vulnerabilities of legacy 4G infrastructure is an added and significant risk for enterprises," details Sakshi Grover, Research Manager, IDC India.

Raman of Fortinet adds that many organizations assume that a private 5G network will inherently keep them safe, which is not necessarily always the case. "5G private networks are rarely entirely isolated from the enterprise IT environment or external environments (partners, integrators, public cloud, etc.) and may be exposed to internal and external attacks and risks."

Hence, in preparing to use 5G, organizations should pay close attention to the software-defined aspect of 5G infrastructure. It is very different from the Wi-Fi and 4G networks in use today. Implementing 5G network security requires a risk management framework that adapts to the flexibility and programmability of network services and traffic flows in software-defined networks.

How 5G security concerns differ from 4G

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.

One of the inherent vulnerabilities in 4G and LTE networks is that a subscriber's unique identifier is unencrypted. 5G fixes that and helps identify and defend against 'man-in-the-middle' attacks. In addition, 5G's unified authentication framework improves usability, connectivity, and endpoint security by allowing open and network-agnostic authentication with 4G, LTE, Wi-Fi, and cable networks.

However, cyber threats impacting 5G won't be because of its architecture but rather because of implantation flaws in 5G and the new technologies that started because of 5G. In fact, 5G could be more vulnerable to cyber-attacks compared to its predecessors. 5G uses a distributed software-based digital routing, unlike its predecessors, which utilize centralized hardware-defined switching.

"The previous generations of networks are based on hub-and-spoke designs, in which all issues converged at choke points and were cleaned away during cyber hygiene maintenance. However, the 5G software-defined network does not

> "Traditionally, network security solutions assumed a single defensive layer for all services and content included within. This method is no longer suitable as a network's perimeter grows more distributed and linked."
>
> MANOJ PAUL,
> Managing Director, Equinix India

provide for chokepoint inspection and control as such activities are pushed outward to a web of digital routers throughout the network. Further, a shift from physical appliances to virtualization (like in the 5G case) will add to complications and make the network vulnerable to attacks. Also as the 5G network operates on software, the chances of hackers gaining access to the network are pretty high therefore protecting software vulnerabilities within the network may not be the most efficient way to provide overall security," highlights Debasish Mukherjee, Vice President APJ, Sales, Sonicwall.

In addition, researchers have identified shortcomings in 5G NSA installations that enable downgrade attacks (also known as cross-protocol attacks), in which a phone's connection is purposefully altered to downgrade to older networks, providing cybercriminals with access to vulnerabilities in 3G and 4G services, says Singh of Grant Thornton.

As 5G is a totally different architecture and is built ground up, it will require a lot more than just a security solution that is stitched to meet these requirements. The earlier generation of cellular networks relied on Signaling System 7 and Diameter protocols. 5G uses common internet protocols (IP) such as HTTP and Transport Layer Security (TLS). These open web protocols lower the entry barrier not only for operators but also for predators and hackers.

"What we need is a 5G network service that is built on an open, programmable, reliable, and software-driven Intelligent Cybersecurity Mesh that treats the internet (IP) itself as Zero Trust and relies heavily on strong encryption for all data transmitted, processed, or stored anywhere on it," says Nilesh Gupta, Chief Cloud Officer, 3i Infotech.

" Organizations must invest in real-time monitoring of network health and check the behavior of distributed environments along with maintaining centralized policy management over 5G wconnected core elements and sensitive and critical data residing both on-premises and in the cloud environment. "

SAKSHI GROVER, Research Manager, IDC India

Complexity in network partitioning with dynamic spectrum sharing

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 ceding 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.

While 5G is built for efficient network slicing, which allows customers to segregate sensitive and more generic data and provide precise security and privacy controls in the different slices; however, each slice from different, parallel communications is sent over the same bandwidth. Hence, each slice contributes to its cyber risk degree. "Dynamic spectrum sharing (DSS)

works by broadcasting 4G Long Term Evolution (LTE) and 5G New Radio (NR) cellular wireless over the same frequency. DSS technology automatically allocates cellular resources between the two networks based on demand. It allows mobile network operators to allocate more spectrum resources to new technology as more users switch to 5G. For DSS to work, both technologies need to cooperate in tandem, creating added complexity," details Dipesh Kaura, GM, South Asia, Kaspersky.

While DSS will bring significant benefits to mobile network operators (MNOs) enabling them to expand 5G coverage, we need to ensure synchronization between 4G and 5G systems while making measurements for DSS. "They must remain synchronized in the time and frequency domains to prevent resource block misalignment. The other key aspect to pay attention to is the fast coordination rate between the LTE and NR packet schedulers which is essential to handle the dynamic allocation of resources," highlights Mukherjee of Sonicwall.

In order to maximize capacity, service providers will need to take DSS into account in relation to their spectrum holdings and technological advancement strategy which is a complexity posed by the network partitioning. The major obstacle to any cooperation or cohabitation between networks is the extremely varied pilot and synchronization signals needed by devices to coordinate and access the network in the two systems, highlights Singh of Grant Thornton.

However, few experts opine that the benefits of DSS outweigh the drawbacks in most situations. "DSS has a marginally negative 25 percent and 15 percent influence on the performance of 4G LTE and 5G NR, respectively. The performance hit is often well worth having the entire spectrum accessible to both networks. Due to their inability to understand the sub-frames, older LTE devices will not be able to access DSS networks employing MBSFN. Modern LTE devices with beam-forming capabilities can do so without any issues," says Sonit Jain, CEO, GajShield Infotech.

Cyber resilience in the 5G platform

5G expands cyber risks due to factors like network decisions (switching and routing), which are more distributed. A shift from hub-spoke security to distributed security of telecom infra, the introduction of billions of devices, Session Description Protocol (SDP) based networks, etc. are making things more complex.

However, the ecosystem surrounding 5G can be better protected than that of previous generations, with security controls from stronger encryption to privacy protections built into networks by design.

As per experts, 5G

> "One of the best technologies to manage networks in the 5G era is AI/ML; it can be used for planning and dimensioning decisions taken prior to network deployment. AI can help in obtaining insights to run the network better and dynamically reconfigure the network at different time scales."
>
> DHANANJAY GANJOO,
> Managing Director, India & SAARC, F5

has overcome many confidentiality and integrity challenges with previous networks like 4G/3G/2G as it has adopted 'Secure by design principles.' For example, UE (User Equipment like mobile or tablet) identity in 4G is sent over radio networks without encryption. Although a temporary identifier may be used to hide a subscriber's long-term identity, researchers have shown that it has a flaw. 5G is designed in security controls to address these issues like mutual authentication capabilities, enhanced subscriber identity protection, and additional security mechanisms, states Gupta of 3i Infotech.

Stanislav Protassov, Co-Founder & Technology President, Acronis, highlights that the 4G protocol faced an issue with core network trusting base stations, which became a problem with the proliferation of nano base stations often installed indoors in locations making them available to malicious intruders. "5G aims to improve the authentication between the base stations and the core network as well as further strengthen subscriber protection against man-in-the-middle attacks over the radio," he adds.

In fact, 5G may not provide 100 percent security but is more secure than its previous generation for comparable services and functionality. 5G provides better user authentication services as compared to 4G. In a 4G network, a SIM card is used to authenticate users, and considering the world of IoT devices today, it is difficult for a single SIM to cope with the requirements. Whereas in a 5G network user authentication, unique identities are assigned to individual devices, eliminating the requirement of SIM, and shifting the responsibility to an individual service provider, shares Ganjoo of F5.

He further adds, "Another area in which 5G excels from its previous generation is encryption. 5G uses 256-bit encryption as opposed to the 128-bit standard used by 4G, making it difficult to identify or locate from the moment users get on the network."

In addition, some of 5G's cyber resilience features allow it to provide better security:

- **Protection of User-plane integrity:** Unlike the previous generation, in a 5G network, the user-plane, which carries the network traffic is integrity protected.
- **SEPP (Security Protection Proxy):** 5G solves the security concerns of roaming interconnect, the SEPP ensures secure traffic among the 5G networks.
- **Unified Authentication:** 5G is known to connect various technologies such as IoT devices, WiFi, cloud platforms, etc. The mighty 5G brings in a unified authentication solution for access to these various technologies in the network. This feature of 5G will allow networks to control the authentication of the device.
- **Enhanced Encryption:** 5G

“5G can be a key enabler to drive AI/ML integration into the network edge. Embedding ML and AI into 5G networks can improve automation and adaptability, facilitating effective orchestration and dynamic network slice provisioning.”

ANURAG SINGH,
Director and Head of Advanced Solutions,
Ingram Micro India

provides enhanced security with better encryption, which conceals the identity of the user.

Although 5G has some built-in security, organizations will still need to integrate a larger cybersecurity strategy to confidently move to 5G applications. They need a solution that will provide comprehensive protection at 5G speeds without compromising end-to-end visibility, automation, and enforcement throughout the ecosystem's attack surface.

Until then, enterprises are more inclined toward private 5G which can be expensive, complex, and lengthy to implement and maintain. On the other hand, consuming public 5G is significantly more cost-effective and rapid but offers less control and customization. "It is likely that private and hybrid (a combination of private and public 5G consumption) 5G networks will be the popular 5G enterprise consumption form. In fact, recent studies show that some organizations would rather use private 5G networks than public ones due to the critical and sensitive nature of industrial environments, processes, and operations," says Raman of Fortinet.

Relook at network security in the 5G era

Traditionally, network security solutions assumed a single defensive layer for all services and content included within. "This method is no longer suitable as a network's perimeter grows more distributed and linked, so a more complicated and multi-dimensional approach is necessary to augment or replace conventional firewalls with a larger zero-trust framework," highlights Manoj Paul, Managing Director, Equinix India.

Experts opine that many existing and traditional security solutions can reduce the risk of the potential 5G security threat vectors, including security solutions created to validate user identities, edge resource identities, endpoints, location-aware identity and access management solutions, malware or incident response, encryption, and IPsec tunneling. "Organizations must also invest in real-time monitoring of network health and check the behavior of distributed environments along with maintaining centralized policy management over 5G connected core elements and sensitive and critical data residing both on-premises and in the cloud environment," suggests Grover of IDC.

Further, businesses today depend on APIs for service and business integration. Lack of authentication or inadequate authorization can leave APIs vulnerable to attacks as they have the potential to introduce additional threat vectors into the network. To avoid this, businesses must use API Gateway solutions to ensure that 5G services achieve their requirements for low latency and other performance parameters.

Further, 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. Hence, AI and machine learning can serve as powerful tools for 5G cybersecurity.

"Businesses must protect and manage every node of the network to efficiently leverage the benefits of 5G. One of the best technologies to manage networks in the 5G era is AI/ML; it can be used for planning and dimensioning decisions taken prior to network deployment. Artificial intelligence can help in obtaining insights to run the network better. It can also be used to dynamically reconfigure the network at different time scales," shares Ganjoo of F5.

In fact, 5G can be a key enabler to drive ML/AI integration into the network edge. Embedding ML and AI into 5G networks can improve automation and adaptability, facilitating effective

orchestration and dynamic network slice provisioning, adds Anurag Singh, Director and Head of Advanced Solutions, Ingram Micro India.

"The most effective approach would be to migrate from traditional, isolated point defense products to a security fabric designed to be integrated, automated, and open using open APIs and common standards. This approach must also combine single-pane-of-glass management and control with security technologies that can move seamlessly across traditional, SD-WAN, multi-cloud, and highly mobile endpoint and IoT devices for consistent visibility and control," concludes Raman of Fortinet.

In fact, 5G technologies require a complete rehaul of network security, which isn't 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 the market falls short and how it can be addressed. We need to invest now — before we're caught with no sustainable cybersecurity plans in place.

Security will be at the Core of 5G: 3i Infotech

NILESH GUPTA
Chief Cloud Officer, 3i Infotech

Nilesh Gupta, Chief Cloud Officer, 3i Infotech, in a brief conversation with Amit Singh, interprets the security challenges in the 5G era. He noted that privacy and identity management will be a primary threat that will need continuous and utmost importance to people that use 5G

As most of the employees work in a hybrid work environment which necessitates decentralization of access, how has it affected the security landscape and strategies for enterprises?

Earlier this year, one of the major workplace consulting research companies surveyed possible workers returning for work shortly. Based on the results, it was very clear that they were not returning to the same workplace full-time that they left in March 2020. More than half responded that they wanted a hybrid model of work environment with other major parts working only remotely. Less than 10 percent responded to returning to the office full-time.

So, what this means is that the traditional way of security landscape for a company is not a viable solution. They need to look into the aspects:

1. Unsecure networks (working from home or away): Borderless workforce often uses unsecured networks like home, coffee shops, open Wi-Fi connections, and many other options that do not have secure and protected network protection.

2. More cyber-attacks: Since a greater number of these workforces use open networks or networks that do not have the right protection as per security standards, they are often the victim of back-door entries and are at mercies of these hackers.

3. No patching standardization: Since there is no IT or shadow IT is not very effective, proper updates take a miss and again provide each access for not-so-updated systems. They are more vulnerable based on the scans.

4. Open access to install anything: Since no proper mechanism to monitor these systems or networks, cyber-attacks are built around the efficient exploitation of vulnerabilities when unwanted software is installed that could lead to a malicious hacker getting into the systems. Shadow IT teams are always at a disadvantage because they must defend all possible entry points, while an attacker only needs to find and exploit one weakness or vulnerability.

Enterprises are upbeat about the 5G launch in terms of a new wave of opportunities for

businesses and unlocking the next level of growth for the country. However, 5G may also open doors for new cyber threats. What are the security challenges you interpret in the 5G era?

The world was rejoicing when 4G was launched, it was like a great leap forward in the history of cellular networks, primarily because we were on the cusp of transformation and every industry and vertical was reworking their digitalization framework of services. While 4G allowed many industries to focus on technology betterment, what took the industries by storm is online streaming – which was way faster and seamless at the speed it provided when compared to 3G. But 5G is designed to connect many more types of such devices than just smartphones – it connects just about anything. 5G opens doors to just about anything - from machines becoming your best friends, we will be spending most of our time in a virtual world made up of metaverses.

That's why, I relate 5G to human connection, and hence when humans matter– t hat is you and I and our younger generation that will use 5G services, security will be the very core of 5G and its usage. Privacy and identity management will be a primary threat that will need continuous and utmost importance to people that use 5G. We love to say who we are, what we do, and where we are, but 5G will also pave the way to several types of predators as well.

As 5G is a different architecture and is built ground up, it will require a lot more than just a security solution that is stitched to meet these requirements. The primary reason is that earlier generation of cellular networks relied on Signaling System 7 and Diameter protocols. 5G uses common internet protocols (IP) such as HTTP and Transport Layer Security (TLS). These open web protocols lower the entry barrier not only for operators but also for predators and hackers.

> “We need a 5G network service that is built on an open, programmable, reliable, and software-driven Intelligent Cybersecurity Mesh that treats the internet (IP) itself as Zero Trust and relies heavily on strong encryption for all data transmitted, processed, or stored anywhere on it.”

What we need is a 5G network service that is built on an open, programmable, reliable, and software-driven Intelligent Cybersecurity Mesh that treats the internet (IP) itself as Zero Trust and relies heavily on strong encryption for all data transmitted, processed, or stored anywhere on it. This approach enables secure and private end-to-end connectivity and provides the ability to securely operate anywhere and anytime, regardless of the environment, even on underlying networks that may be compromised.

How do 5G security concerns differ from previous generations?

5G is not a mere technical upgrade from 4G but it will enhance our connected devices/lives and pave the way for new kinds of innovations and solutions. This also means that every human would be connected in some form or other which would need a 5G security architecture to be built from the ground up as well. We need to have a 5G security framework to support connected humans on the 5G network. This means a lot of privacy issues will be at play giving way to unsolicited attacks. For example, with Intelligent Emergency Response Systems, the elderly can be equipped with a wearable device that can detect falls as soon as they happen through a 5G network and relay the precise location of the elderly person to emergency services in real time. But what could happen if this information is in the wrong hands? What we need is a clean network that is rooted and accepted by digital trust standards and utilizes only trusted hardware, software, and cloud infrastructure. A globally distributed robust

overlay architecture treats the internet itself as Zero Trust and relies heavily on strong encryption for all data transmitted, processed, or stored anywhere on it.

How can enterprises relook at their cyber security/ network security strategies in the 5G era?

Enterprises need a 5G-powered Zero Trust that integrates network and security with real-time threat detection and response. Enterprises need an end-to-end full-stack cloud-native solution to transform how security and performance are consumed and managed. A solution that will integrate networking and security in a single, autonomous platform that efficiently connects users, offices, devices, and their applications regardless of their locations.

With cyber threats growing and new types of threats emerging, we should be able to stop tomorrow's threat today! This can only happen when we bring in an element of combining the two most powerful subjects that are very popular and widely discussed in technology – Artificial intelligence and Machine Learning. We need these to help us to predict what possibly can happen based on past events and correlate them based on learnings. These learnings can help in possible root causes, self-remediate, and predict when possible. Such incidents can happen based on past experiences.

An intelligent cyber security mesh can help with complete 5G core integration Converging SASE and 5G to have significant performance synergies, as drawing security to the edge of the network will allow 5G-enabled end-users to securely access applications on the go no matter what device or network they connect with.

The Concept of ‘5G Security’ Still Lacks an Official Definition: Sonicwall

DEBASISH MUKHERJEE
Vice President APJ, Sales, Sonicwall

Debasish Mukherjee, Vice President APJ, Sales, Sonicwall in a brief conversation with Amit Singh highlights the security challenges and complexities in the 5G regime as he speaks about the best practices to face these challenges

Besides new opportunities, 5G may also open doors for new cyber threats. What are the security challenges you interpret in the 5G era?

With the 5G connectivity standard in play, wireless performances will go to the next level. Apart from improving speeds, efficiency, and latency, 5G will be able to support a massive scale of devices and simultaneous connections.

As 5G adoption accelerates in the coming times, organizations will need higher levels of network security and reliability to protect both their users and their business-critical applications as it will enable cybercrime opportunities. Moreover, the mitigation of applications and network functions to the cloud, along with network slicing, will open up new attack surfaces.

Today's hybrid work environment, an increased number of endpoints, and the adoption of distributed or remote work arrangements have already created network and threat visibility challenges to combat bad actors.

What are the complexities you see in network partitioning with dynamic spectrum sharing in 5G?

The latest 5G networks promise download speeds of 10 to 20 times faster than any of the current networks. Besides, 5G network is likely to aid in the efficient implementation of augmented systems and making the Internet of Things a reality. However, 5G is expected to come with some complications and complexities too.

We feel that Dynamic spectrum sharing (DSS) will bring significant benefits to mobile network operators (MNOs), enabling them to expand 5G coverage. But one key aspect to take into consideration when making measurements for DSS is the synchronization between 4G and 5G systems. They must remain synchronized in the time and frequency domains to prevent resource block misalignment. The other key aspect to pay attention to is the fast coordination rate between the LTE and NR packet schedulers that is essential to handle the dynamic allocation of resources.

Experts also claim inbuilt cyber security measures in 5G. What is the cyber resilience features 5G offer?

5G is the first generation of cellular technology that is designed with virtualization and cloud-based technology in mind. With cloud-based technologies, software execution can now be disconnected from specific physical hardware by utilizing Software Defined Networking (SDN) and Network Function Virtualization (NFV). Also, today mobile security has significantly evolved since the 4G days and the 5G standard offers several strong security capabilities, such as features for user authentication, traffic encryption, secure signaling, and user privacy. Having said that since this technology is new and evolving, the concept of '5G security' still lacks an official definition.

> “5G offers several strong security capabilities, such as features for user authentication, traffic encryption, secure signaling, and user privacy; however, since this technology is new and evolving, the concept of '5G security' still lacks an official definition.”

5G is said to be a major boost for IoT initiatives across industries, however, we still don't have IoT security standards. How will it be a challenge?

As we all know, the internet of things is booming and is expected to bring in a big boost from 5G cellular technology with significantly faster data throughput; support to all machine-type communications enabling large numbers of machines or devices to communicate with each other without any human interaction or control; and ultra-reliable, low-latency communications overall.

One of the biggest issues that cannot be ignored is most of the Indian sectors using digital technologies or integrating emerging technologies do not have a digital risk element defined by a regulatory authority. We still lack a comprehensive national cyber security norm or strategy.

What are the security best practices you suggest for 5G networks? How can AI/ML-driven network management help? We all know by now that 5G is going to bring in many business benefits while having a transformational impact on the global economy and society. In such a scenario, organizations will have to understand the scope of attacks to ensure system and data integrity. They would need to study options and explore the latest security software, tools, and services ideal to fit into an overall network and applications security architecture. Installing malware protection on your devices while ensuring that none of them, particularly IoT devices, are using the factory default passwords, always making sure that devices are patched and running the latest OS version, keeping up with the latest news and developments on cyber security threats and crimes and last but not the least, partnering with well established and reputed cyber security solution providers. Today, AI/ML technologies are so matured that all communications service providers (CSPs) are applying them to their network including sensitive parts of their networks that directly impact user experience.

5G Addresses Many Security Threats Present in Previous Gen Networks

DIPESH KAURA
GM, South Asia, Kaspersky

While noting added avenues of cyber-attacks in the 5G platform, Dipesh Kaura, GM, South Asia Kaspersky, in a brief conversation with Amit Singh, highlights security controls built into 5G to address many of the dangers present in 4G, 3G, and 2G networks. He underlined that 5G offers improved subscriber identity protection, new mutual authentication capabilities, and extra security measures

How do you see 5G changing the security landscape for enterprises in India?

With its increased network capacity, reduced latency, higher dependability, improved availability, and improved user experiences, 5G has completely transformed how people and devices connect. But, 5G implementation introduces more security issues and network security concerns, as with any new technology. Organizations must secure their data and optimize their investments by understanding the cyber security issues related to the implementation of 5G. The dramatic increase in bandwidth that makes 5G possible, also adds avenues of attack. The network has moved from centralized, hardware-based switching to distributed, software-defined digital routing. Physically, low-cost, short-range, small-cell antennas deployed throughout urban areas become new challenging targets. 5G additionally complicates its cyber vulnerability by virtualizing higher-level network functions formerly performed by physical appliances in software. Finally, additional vulnerability is created by attaching tens of billions of hackable smart devices to the network, referred to as IoT.

How do 5G security concerns differ from previous generations? What is the resilience it offers?

There are a few significant security wins in 5G. Many relate to anti-tracking and spoofing features that make it harder for bad actors on a network to track and manipulate individual device connections. To do this, 5G encrypts more data, so less is flying around in the clear for anyone to intercept. 5G is much more software and cloud-based system than previous wireless networks, allowing better monitoring to spot potential threats. It will also enable operators to do 'network slicing'—segmenting the system into numerous virtual networks that can be managed and customized separately. All this means that different 'slices' could have various tailored protection setups for specific types of devices.

> “There are a few significant security wins in 5G. Many relate to anti-tracking and spoofing features that make it harder for bad actors on a network to track and manipulate individual device connections. To do this, 5G encrypts more data, so less is flying around in the clear for anyone to intercept.”

5G is said to be a major boost for IoT initiatives across industries, however, we still don't have IoT security standards. How will it be a challenge?

It is a significant challenge, as they offer more and more services and facilities. It is critical to guarantee security, uphold customers' trust, and provide appropriate protection. The inability to establish secure connections is one of the main issues. Since IoT devices have few resources but additional difficulties, such as poor testing, vulnerable APIs, weak passwords, lack of visibility, open-source code vulnerabilities, limited security integration, and overwhelming data volume, implementing the majority of the currently used security measures can be difficult.

We already understood these things, which is why 5G has security controls built in to address many of the dangers now present in 4G, 3G, and 2G networks. These controls include improved subscriber identity protection, new mutual authentication capabilities, and extra security measures.

How can enterprises relook at their cyber security/ network security strategies in the 5G era? How can AI/ ML-driven network management help?

We intend to use a zero-trust framework for that. All users seeking or accessing data must follow obligatory verification and authorization, and we will check the security settings.

With a zero-trust framework, 5G cybersecurity has the potential to:

- Remove implicit trust and verify each step of digital engagement.
- Reduce threat surface by ensuring that only authorized user access is granted.
- Protects against online interference on multiple devices and offers secure access to services.
- Monitors security for cyber vulnerabilities, implements security standards, and ensures compliance
- Every action on the 5G network is safe thanks to the zero-trust architecture's end-to-end security and monitoring techniques.

Further, AI/ML can be used to plan the 5G network, automate network operations, slice the network, lower operational costs, and improve service quality and customer experience (RPA). The expansion of IoT devices will be crucial in helping wireless carriers develop, run, and manage 5G networks.

4G Network Vulnerabilities will Persist in 5G for Some Time: Ingram Micro

ANURAG SINGH
Director, Head of Advanced Solutions, Ingram Micro India

Anurag Singh, Director, Head of Advanced Solutions, Ingram Micro India, in a quick conversation with Amit Singh, highlights the security challenges in the 5G era and how the next-generation networks change the traditional assumptions and approaches

As India moves towards the 5G era, what are the security challenges you interpret in the 5G networks?

The integration of 5G networks poses significant challenges for the majority of enterprises due to a lack of global best practices or insufficient wireless network experience. Security and privacy are two issues that industries are concerned about while defending data from outside incursions. This worry is caused by the increasing volume of data handled, which makes it an appealing target for hackers. Once 5G devices are compatible with mobile device management systems, this problem might go away.

How does 5G challenge traditional assumptions and approaches in cyber-security?

The emerging fifth-generation networking has a lot of potentials and thus is also more vulnerable to cyber-attacks than the previously used networks. The below points outline how 5G networks are more vulnerable to cyberattacks than their predecessors:

- 5G increases its vulnerability to cyberattacks by virtualizing in software higher-level network operations that were previously carried out by physical appliances.
- The dramatic increase in bandwidth made possible by 5G opens up new attack vectors.
- The network's vulnerability is also increased by the use of numerous hackable smart devices (which are tiny computers) or IoT.

> “5G has challenged conventional ideas about network security as well as the security of the hardware and software that connect to that network. In times of economic pressure on investments that don't provide a profit, ISPs (internet service providers), like 5G networks, function as private players.”

However, the ecosystem surrounding 5G can be better protected than that of previous generations, with security controls from stronger encryption to privacy protections built into networks by design. Compared to past generations, there is a lot more at stake with the shift to 5G. This is because, in contrast to the successions of earlier generations, 5G more dramatically diverges from the current generations.

One of the areas where 5G and earlier generations differ most significantly is network speed. On 5G networks, super-high-speed airwave allows devices to transmit much larger volumes of data at faster rates.

The fact that we are rapidly consuming up the bandwidth of the previous generations is one of the key reasons why the transition to 5G has dragged on despite concerns about the technology.

Along with being fast response and having a larger capacity, 5G also outstrips the previous generations in terms of latency. The time it takes for data to be sent from one device to another is referred to as latency.

How do 5G security concerns differ from previous generations?

5G has challenged conventional ideas about network security as well as the security of the hardware and software that connect to that network.

In times of economic pressure on investments that don't provide a profit, ISPs (internet service providers), like 5G networks, function as private players. Other ISPs' inaction can weaken the protective measures one ISP has put in place. The incentive for all ISPs to invest in such security is diminished as a result. Therefore, in situations where the market is unable or unwilling to do the task effectively, cyber accountability calls for a combination of market-based incentives and proper regulatory monitoring.

How are security brands positioned to address the security challenges coming with 5G networks?

The majority of businesses adjusting to 5G will require a sizable amount of new hardware. The vast amount of equipment needed will make this a logistical difficulty because it will take a while to put everything up. This may lead to careless errors that are difficult to spot after the fact, and these oversights may later result in significant issues.

Additionally, a lot of networks are currently switching from 4G to 5G. As a result, for as long as the upgrade process takes, 4G network vulnerabilities will persist in 5G networks.

MNO's Security Capabilities are Critical for Success in Vertical Use Cases

Vishak Raman, Vice President, Sales, India, SAARC and Southeast Asia, Fortinet, in a detailed interaction with Amit Singh, highlighted that the benefits of 5G far outweigh its potential risks—but only when security is an integrated part of the process and solution. He added that native 5G security features are important, and that operators should offer a shared responsibility model

VISHAK RAMAN
Vice President, Sales, India, SAARC and Southeast Asia, Fortinet

Enterprises are upbeat about the 5G launch in terms of a new wave of opportunities for businesses and unlocking the next level of growth for the country. What are the new opportunities and growth 5G is going to bring for businesses in India?

In addition to exponentially faster speeds, 5G will also introduce greater capacity, reduced latency, and more flexible service delivery. This will enable organizations to provide better content, more real-time transactions, and much richer user experiences across entertainment and commercial activities.

5G will also have an impact far beyond interconnecting endpoint devices. IoT devices will be enlisted to track other devices and users, monitor inventory, gather user and device information, and provide real-time data that can impact everything from agile application development and manufacturing floors to managing and coordinating resources in highly connected environments such as smart cities.

Enhanced communication services within connected cars, for example, will go well beyond the current set of interactions that already occur internally between onboard IoT devices such as braking, environment monitors, GPS, and even entertainment systems. Live connections between drivers and businesses will enable financial transactions, such as paying for fuel, ordering food at a drive-thru restaurant, or paying tolls, without having to pull out a credit card. Communications between vehicles and between cars and infrastructure-based IoT will enable enhanced traffic management and augment things like autonomous driving at highway speeds.

Likewise, there are significant implications for healthcare and medical IoT. 5G speeds will allow the real-time transmission of data to support things like remote surgery, the tracking of monitors and other connected medical devices, including wearable medical IoT, and the analysis of tests and scans by remote professionals. These advances will not only allow patients to have access to the best physicians in the world, but they will also extend 21st-century medical care to remote locations that currently lack reliable medical resources.

■ How do 5G security concerns differ from previous generations?

In previous mobile generations, security was all about protecting the network itself, creating a walled-garden environment for the core of the network by securing all external exposure points, such as the internet/PDN, roaming, RAN to core access, external partners, etc. This is also valid to 5G, with the appropriate integration and compatibility to 5G technologies and architectures. But the unique nature of 5G and its role and criticality in the business segment means that security's role is changing and expanding, and should encompass the following main roles:

□ Protect the 5G mobile infrastructure from attacks to ensure service continuity and availability. This is similar to the traditional security role in previous mobile generations.

□ Protect the larger 5G ecosystem required to deliver 5G-enabled use cases for enterprise verticals to meet security and regulatory requirements.

> “Although 5G has some built-in security, organizations will still need to integrate a larger cybersecurity strategy to confidently move to 5G applications.”

□ Enable monetization via a wide range of 5G security services to organizations through managed security services as part of service/use case offerings.

Security is a condition for true and meaningful 5G adoption as a platform for innovation and transformation.

■ Experts also claim inbuilt cyber security measures in 5G. What are the cyber resilience features 5G offers?

Fortinet conducted a survey around security in enabling 5G adoption in business verticals, and the results are very clear. Almost 90 percent of respondents stated that the MNO's security capabilities are either critical or very important for success in vertical industry use cases. More than 80 percent consider native 5G security features as important, but only a baseline for the security needed to serve the 5G market.

Another interesting data point arising from the survey is that 54 percent of respondents believe operators should offer a shared responsibility model. However, nearly all those who support this approach believe that a shared responsibility model should be offered as an option alongside the alternative of comprehensive, full-stack, end-to-end security. True to the traditional telco business model, fully 86 percent of respondents believe operators should offer full-stack security.

The benefits of 5G far outweigh its potential risks—but only when security is an integrated part of the process and solution. Although 5G has some built-in security, organizations will still need to integrate a larger cybersecurity strategy to confidently move to 5G applications. They need a solution that will provide comprehensive protection at 5G speeds without compromising end-to-end visibility, automation, and enforcement throughout the ecosystem's attack surface. And to do that most efficiently and securely, the solution must also be part of a coherent, integrated, and self-healing security platform. This will enable organizations to confidently distribute 5G services from the core of their network out to its furthest reaches while allowing them to continue developing and deploying critical digital innovation.

■ How can enterprises relook at their cyber security/ network security strategies in the 5G era? How can AI/ ML-driven network management help?

5G is simply a critical enabler for the real objective, which is the deployment and enablement of a great number of use cases that bring value and innovation to the enterprise. These may

include such things as closed-loop process automation, real-time logistic management, augmented reality, predictive maintenance, and more. Delivery of such use cases requires creating, deploying, and managing an interconnected 5G industrial ecosystem, including all related OT/IIoT devices and vendors, industrial applications and tools—on-site and on public/partner clouds, and the 5G

5G will Drive Shift toward Distributed AI to Enable Decision-making at the Edges

JASPREET SINGH
Partner, and Clients and Markets Leader – Advisory Services, Grant Thornton

Jaspreet Singh, Partner and Clients and Markets Leader – Advisory Services, Grant Thornton, in a detailed conversation with Amit Singh, highlighted that a paradigm shift is necessary from the traditional centralized and virtual cloud-based AI to a distributed AI framework where the decision-making intellect is nearer to the edge of 5G networks in order to achieve even lower latencies, enabling event-driven analysis, real-time execution, and decision-making

Enterprises are upbeat about the 5G launch in terms of a new wave of opportunities for businesses and unlocking the next level of growth for the country. However, 5G may also open doors for new cyber threats. What are the security challenges you interpret in the 5G era?

The advantages that 5G offers inevitably come with a few cyber security issues. Businesses may set themselves up to be pioneers in the 5G era by investing time in securing 5G infrastructure. Data exfiltration attempts on 5G networks are more lucrative for cybercriminals since a lot more data is transferred in a given amount of time. An aspect of weakness is also the software's integrity, particularly when it originates from open sources and the entire software distribution network. The significant increase in bandwidth that enables 5G also opens up new attack vectors. Small-cell antennas with a short range and low budget that are widely used in urban areas are now deemed critical threats. Thus, a considerably increased, multifaceted cyber-attack risk is created by 5G networks. The new network 'ecosystem of ecosystems' that emerges from the redefined architecture of networking necessitates a cyber-strategy that is also reinvented. Organizations will need to deal with possible privacy concerns and IoT security risks as they begin to use cutting-edge digital technology and 5G's higher capacity to produce more and better data.

How does 5G challenge traditional assumptions and approaches in cyber-security? What are the complexities in network partitioning with dynamic spectrum sharing in 5G?

5G is more susceptible to cyberattacks than its predecessors were. Chokepoint surveillance and regulation are not available in the 5G software-defined network since they are delegated to a network-wide web of digital routers. The susceptibility of the 5G network is further complicated by the switch from physical devices to virtualization. It will be necessary to upgrade network monitoring tactics for reliability and safety as 5G will empower more IoT devices and replace conventional network design. Dynamic Spectrum Sharing (DSS) makes it possible for a radio channel to support both 4G LTE and 5G while also allowing the 5G signal to share the available spectrum. In order to maximize capacity, service providers will need to take DSS into account in relation to their spectrum holdings and technological advancement strategy which is a complexity posed by the network partitioning. The major obstacle to any cooperation or cohabitation between networks is the extremely varied 'pilot' and 'synchronization signals' needed by devices to coordinate and access the network in the two systems.

> “The susceptibility of the 5G network is further complicated by the switch from physical devices to virtualization. It will be necessary to upgrade network monitoring tactics for reliability and safety as 5G will empower more IoT devices and replace conventional network design.”

How do 5G security concerns differ from previous generations?

The third, fourth, and fifth generations of telecommunication technology are known as 3G, 4G, and 5G, respectively. The main distinction between each generation is based on their capacities. Advancements have been made to Speed, Network power (higher bandwidth), and Ease of access (greater range of service) with each advancement. Researchers have identified shortcomings in 5G NSA installations that enable downgrade attacks (also known as cross-protocol attacks), in which a phone's connection is purposefully altered to downgrade to older networks, providing cybercriminals with access to vulnerabilities in 3G and 4G services. Networks from earlier generations mostly used the SS7 and Diameter protocols. Common internet protocols (IP) like HTTP and TLS are used by 5G. These open web protocols reduce the entry bar for hackers as well as operators.

What is the level of preparedness you see among businesses against the cyber challenges in the 5G era?

As a whole, it is assumed that companies are now mindful of the exposure to future cyber-attacks. However, some disclose themselves and only respond when attacked. Others who seem proactive delegate the responsibility of safeguarding their IT processes and architecture to their security professionals. Businesses are vulnerable to cyber-attacks and their associated effects when they use this ad hoc approach to controlling cyber risk. Authentication and verification will be crucial to 5G safety since more devices, such as Multi-access Edge Computing nodes, will be connecting to the network. Additionally, businesses will need to think about how to strengthen their vulnerability management procedures for edge devices that may have flaws that go undiscovered and unpatched. The major impediments to the preparedness of the businesses and decision-makers against 5G and cyber challenges include the limited accessibility of vital infrastructure beyond

the urban areas, uncertainty about their company’s ability to adopt the required technologies including the costs related to the same, and security concerns in 5G Era.

Experts claim inbuilt cyber security measures in 5G. What is the cyber resilience features 5G offers?

5G has designed many security measures to ensure protection from threats faced by 4G/3G/2G networks these controls include new mutual authentication capabilities, enhanced subscriber identity protection, and additional security mechanisms. 5G offers the mobile industry an unprecedented opportunity to uplift network and service security levels. 5G provides preventative measures to limit the impact of known threats, but the adoption of new network technologies introduces potential new threats for the industry to manage. 5G also ensures a user plane, which transports traffic from users on the network, would have to have mandated authenticity protection. Multi-network slicing, multi-level services, and multi-connectivity network capabilities will all be provided by 5G. These capabilities will be offered via virtualized and containerized infrastructures to enable the necessary flexibility, agility, and economies of scale. 5G also enables Transport-layer security (TLS) and the new “service-based architecture,” which conceals the structure of the mobile core, provides additional security for the mobile core. For the industry, this represents an innovative method of operation.

5G is said to be a major boost for IoT initiatives across industries, however, we still don’t have IoT security standards. How will it be a challenge?

5G is dynamic and intricate by its very essence. The advent of intelligent connectivity, which is now being promoted, is being brought on by advancements in 5G, artificial intelligence, and the Internet of Things. There are many factors that contribute to the vulnerability of modern gadgets and operating systems, but they all stem from the absence of a single set of cyber security standards prior to now. To assure customers that their product offerings have undergone a security certification procedure, IoT product makers must prioritize testing and certifying their goods to these security requirements. IoT is an effort to link technological advancements with bettering business processes but still poses some challenges due to the lack of security standards. As structures grow more interoperable and networked, attackers have become more skilled, leveraging linked devices to access key infrastructure and create disruption.

How can enterprises relook at their cyber security/ network security strategies in the 5G era? How can AI/ ML-driven network management help?

Cybersecurity now must facilitate edge-to-edge composite systems that are elastic and combine tried-and-true conventional methods with novel ideas. To traverse between both local and remote resources that combine segments modern segmentation tactics like micro-segmentation will need to be planned. IT teams will have to oversee numerous co-managed systems as they install 5G networks and public cloud services. Additionally, businesses need to cover all aspects of the technology stack, such as key generation, cryptography, operations, administration, risk mitigation, and automated process, and also address the security architecture.

In 5G systems, ML and AI will provide additional intelligence and enable a transition from controlling networks to managing services. Wireless operators may shift from a human management approach to self-driven automated administration by using ML and AI to meet a variety of use cases, which will alter network operations and maintenance procedures. Significant levels of synergy exist among ML, AI, and 5G. They all deal with low-latency use cases where data detection and processing must be done quickly. In comparison to 4G, 5G delivers ultra-reliable low latency that is 10 times quicker. A paradigm shift is necessary from the traditional centralized and virtual cloud-based AI to a distributed AI framework where the decision-making intellect is nearer to the edge of 5G networks in order to achieve even lower latencies, enabling event-driven analysis, real-time execution, and decision-making.

Seven Trends that will Transform Automation in 2023

Every Indian organization's journey toward digital transformation is increasingly reliant on automation. 84 percent of Indian firms want to ramp up their robotic process automation (RPA) activities or reach an enterprise-wide RPA deployment by 2025, according to the IDC APJ Automation Survey 2022, which was commissioned by UiPath.

The company said that the rise of the digital workforce and the digital skills rollout will be among the seven big trends that will reshape how India works from 2023.

Automation becomes the new way of operating and innovating

The C-suite has come to see and appreciate the real potential of automation in fostering corporate value and transformation. Automation that is implemented across the entire company improves productivity and efficiency by 40 percent more than automation that is implemented piecemeal. Elevating automation increases its impact, which improves the customer and employee experience, adds more value, and generates more income. According to the UiPath-commissioned IDC APJ Automation Survey 2022, 88 percent of Indian enterprises concur that automation would be essential for business excellence, customer experience, and competitive performance during the next three years.

Automation will counteract growing labor and inflation pressures

Automation assists executives in overcoming difficult financial difficulties, such as lowering expenses and attracting and retaining top people. Another UiPath poll found that 85 percent of respondents thought automation may lower attrition and draw in new employees. Numerous areas can benefit from automation: Organizations can increase employee productivity while improving the work environment to attract (and retain) top talent by increasing their automation efforts. In the upcoming years, executives will understand that outworking inflation is the greatest strategy. To close workforce deficits, 78 percent intend to increase their automation investments. Automation can enable teams to accomplish more with the same resources in both scenarios. The report states that 82 percent of employees in India want to see more operational efficiencies and simplified processes.

Digital CIOs step-up automation to meet new goals

Automation is essential to CIOs' goals as they create a new, digitally oriented foundation for organizational success. 90 percent of CIOs said their position has extended into new areas like analytics, ESG, talent acquisition, and sales and marketing, according to the Global Study of CIOs, August 2022. These are the main areas they have been investing in to reveal those advantages: cybersecurity, cloud, data, and AI. Automation is already being recognized by CIOs as the new essential tool in their toolbox, boosting the other tools in addition to providing its own advantages. In fact, 54 percent of CIOs automate business and IT activities to increase revenue, according to a survey by Foundry.

To uncover bottlenecks, inefficiencies, and possibilities for improvement across entire systems, workflows, and departments, emerging automated discovery tools like process mining and task mining now apply cutting-edge AI to system logs and users' work patterns. According to the CIO's 21st Annual State of the CIO poll, 82 percent of executives think process mining improves the results of automation. Then, even before you automate them, you may use this crucial data to develop new or more valuable processes.

Low code becomes a top priority for automation and AI

The good news is that modern automation platforms provide distinctive low- or no-code capabilities, allowing users to work with straightforward drag-and-drop visual interfaces rather than challenging programming. When businesses use citizen development programs, 29 percent more procedures automate, according to a September 2022 IDC analysis. Now, users of all skill levels may create more of the distinctive automation, data models, and apps they require fast and effectively.

New AI-powered innovations push automation's boundaries even further

Emails, calls, chats, and service tickets all include unstructured content that can be extracted by Advanced Communications Mining and converted into useful information for Natural Language Processing (NLP) model training. Natural Language Processing is expected to grow at a 39 percent CAGR through 2030, according to a Precedence Research estimate from 2022. In-depth consumer insights will be acquired when common queries and requests are automatically handled.

Rounding out digital skills becomes a hot issue for HR and IT leadership

According to the IDC APJ Automation Survey 2022.022, just 46 percent of Indian firms now perform reskilling and upskilling across teams and units, therefore organizations will need to build an extensive training and development plan that focuses on doing so. Indian respondents also emphasized that collaboration with IT (54 percent), clearance from senior leadership (20 percent), and clear instruction on best practices (14 percent), are the critical needs for successful deployments as more firms integrate automation in the work of non-IT sector personnel. Each team member will need to have access to new digitally focused abilities. To hire, train, and upskill these new types of workers, HR and IT departments will need to collaborate; this collaboration will place less emphasis on transactional and repetitive tasks and more emphasis on maximizing the benefits of automation initiatives.

Channel Point

Indian Telcos may Double Investments to Strengthen Network Security for 5G

The advent of 5G is pushing many companies' investments in large amounts of interconnected devices to continue their day-to-day business operations and utilize next gen digital systems. The number of IoT/OT devices connecting to the internet has rapidly increased. Thus, the devices require enhanced security and extra attention to keep them secure.

The connection between 5G and IoT, AI will introduce an alarming number of threats and vulnerabilities, which will have an impact on the health of corporate and private networks in near future. Expert says, with 5G, it is the first time the telcos have a chance to put security at the core of the telecom operations. This will of course increase the need for investment to 2-2.5X from what they are doing now. Network security spending is part of a telcos' IT budget. Currently, telcos spend to 4-5% of their IT budgets on network security (including internal networks and consumer facing aspects). Analysts peg the IT budget of Indian telcos at around 5% of revenue.

In times of economic pressure on investments that don't provide a profit, ISPs (internet service providers), like 5G networks, function as private players. Other ISPs' inaction can weaken the protective measures one ISP has put in place. The incentive for all ISPs to invest in such security is diminished as a result. Therefore, in situations where the market is unable or unwilling to do the task effectively, cyber accountability calls for a combination of market-based incentives and proper regulatory monitoring. Security, confidentiality, and privacy must be a part of the lifecycle of core technology of 5G, and edge and IoT devices along with the traditional underlying compute and storage infrastructure. Strong encryption and anonymization, together with layered security approach is certainly crucial.

How are security brands positioned to address the security challenges coming with 5G networks?

The majority of businesses adjusting to 5G will require a sizable amount of new hardware. The vast amount of equipment needed will make this a logistical difficulty because it will take a while to put everything up. This may lead to careless errors that are difficult to spot after the fact, and these oversights may later result in significant issues.

Additionally, a lot of networks are currently switching from 4G to 5G. As a result, for as long as the upgrade process takes, 4G network vulnerabilities will persist in 5G networks.

Some priorities for telcos would be implement network DDoS protection, implement identity and access management systems. One area where a lot of the investments could be focussed is in using and developing artificial intelligence and machine learning for network security. With greater data traffic, more IoT devices, consumer and enterprise, getting connected to their networks, telcos will need sophisticated AI modules for threat detection and addressal. In fact, with software defined networks. Telcos can quickly detect the threats and greater visibility to the various components in the networks.

K.Singhal

KALPANA SINGHAL, Editor
(E-mail: kalpana@techplusmedia.co.in)

TECHPLUS MEDIA™

EDITOR: KALPANA SINGHAL
CONTENT HEAD: Amit Singh
ASSISTANT EDITOR: Rajneesh De
CORRESPONDENT: Aaratrika Talukdar
CORRESPONDENT: Atreyee Chakraborty

INTEGRATED MARKETING COMMUNICATION:
Aakash Vahal
Saugata Mukherjee, Mamta Dhiman,
Nishit Saxena

ASSOCIATE ANALYST
Shaithra S

SALES:
Harpreet Singh | Pratap Jana

PRODUCTION HEAD:
Aji Kumar

WEBSITE:
Sheetal Varshney/Ramesh Kr

PROMOTION:
Vikas Yadav /Amit Pandey

CIRCULATION:
Pratap

FINANCE:
Inder Pal

HEAD OFFICE:
370A, Sant Nagar, East of Kailash, New Delhi
Tel: 41625763, 26237405, 41620042
Email - kalpana@techplusmedia.co.in

MARKETING OFFICE:
10 UF, West Wing, Raheja Tower,
MG Road, Shanthala Nagar, Ashok Nagar,
Bengaluru, Karnataka-560001

Delhi: 9711841991 | **Mumbai:** 9711841992
Kolkata / Guwahati: 9331072026
Bangalore: 9354347953

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL Printed at Modest Graphics Pvt. Ltd., C 52-53, DDA Shed, Okhla Industrial Area, Phase - I, New Delhi-20, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, Editor- Anuj Singhal

Note: While every possible care is taken prior to accepting advertising material, it is not possible to verify its contents. ITPV will not be held responsible for such contents, or for any loss or damages incurred as a result of transactions advertising/advertorial in this publication. We recommend that the readers make necessary inquiries and verification before remitting money or entering into any agreement with advertisers, or otherwise acting on advertisement in any manner whatsoever.

#1 Backup for Service Providers

Exceed Customers Service level agreements (SLAs) while increasing margins & revenue

VEEAM | CSP PARTNER PROGRAM

Postal Registration No. - **DL(S) 01/3377/2019-21 Posting Date - 13-14, 27-28**
Registered with Registrar of Newspapers of India under RNI No. **DELENG/2010/32787**

PANTUM
प्रिंटिंग के लिए नया युग

Pantum India Product Line

Business is Complicated, Printing Should be Simple

Vibrant 18 Series

Elite Series

PT-L280 Series

PT-L380 Series

PT-B680 Series

Simple&Smart Series

Simple&Smart Series

Mighty Series

4S Efficiency Series

Max Series

PANTUM SERVICE TOLL FREE NO.: 18003098240

WWW.PANTUM.IN

SALES REGION	PHONE NOS.	SALES REGION	PHONE NOS.
West Bengal & North East	98302 28532	Bihar & Jharkhand	9334317035

Know more on @PantumIndia

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, EDITOR: Anuj Singhal