Aligning cybersecurity to enable the Telco metamorphosis in a post-COVID-19 era

August 2020

EY
Building a better working world

Foreword

Over recent years, telecom operators (Telcos) across the globe have witnessed revenue stagnation in their core services, despite the enormous growth in bandwidth demand and usage. Furthermore, they are also facing competition from digital service providers resulting in shrinking of revenues from core services.

The ongoing digitalization wave has brought a lot of disruptive changes in terms of customer expectations and the way telecommunication services are consumed. Also, digital service providers have an upper hand to Telcos because they can quickly leverage multiple disruptive digital technologies.

Telcos are facing an existential crisis due to these fierce competitions from digital service providers and the rapidly changing environment. Telcos have no other option, but to transform if they are to remain relevant.

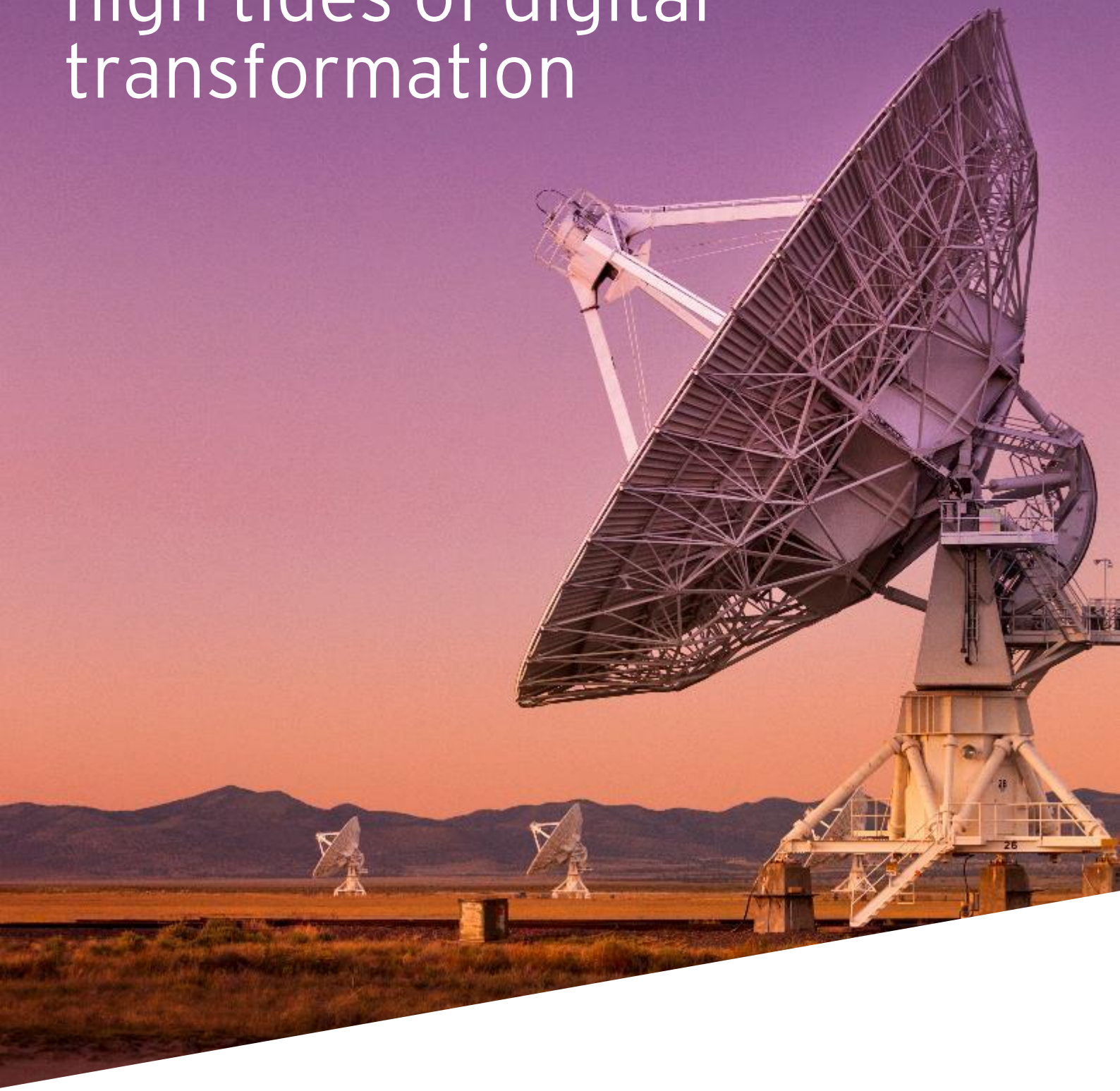
Telcos across the globe are trying to embark on a transformative journey by investing in their digital infrastructure and adopting a business model which focuses on customer experience and technology dominance. Cloud, 5G and Internet of Things (IoT) top the list of technology catalysts that can aid Telcos in the transformation.

There is no doubt that this metamorphosis will provide bountiful rewards to Telcos. However, Telcos will be skating on thin ice, if they are not careful about the cybersecurity implications of this transformation journey.

This white paper focuses on exploring the cyber aspects of the Telco metamorphosis. It also explains some of the best practices that Telcos can adopt to align their cybersecurity strategy to enable the transformation.

Contents

Telcos sailing through high tides of digital transformation



In the wake of years of sluggish growth in traditional services, telecommunication operators are trying to reinvent themselves as digital services providers. Telcos are investing in new breed of technologies such as 5G, cloud and IoT to enable them to undergo this transformation which represents immense opportunities to move up the value chain and find new streams of revenues

> As we continue to experience rapid change across our global communities through digital disruption, it is our role as an ICT leader to leverage and harness this great opportunity for progress.

CEO of a large telecom operator in MENA

> Entire digital strategy should be consumer-first. To understand future needs of consumers and resolving issues, we have to proactively fix consumer issues.

CIO of a large telecom operator in India

Potential revenue opportunities that can be tapped through digitalization

Over-the-top (OTT) services

14.3% CAGR

US$179.9b by 2025[1]

US$1b In Africa by 2025[2]

US$2.97b In MENA by 2025[3]

US$4b In India by 2025[4]

Data monetization

16.75% CAGR

US$4.75b by 2026[6]

4.65% Growth in MEA[7]

7.02% Growth in India[8]

IoT telecom services

36.9% CAGR

US$23.1b by 2023[5]

Mobile payment

28.7% CAGR

US$5.4b by 2023[5]

US$434b In MEA by 2025[10]

US$1.2b In India by 2025[11]

1. Globe newswire
2. PR newswire
3. Research and Markets
4. Research and Markets
5. Livemint
6. Market research future
7. Research and Markets
8. Knowledge Sourcing
9. Globe newswire
10. Globe newswire
11. Globe newswire

To seize the opportunities in the market, Telcos need to adopt a business model which has four focus areas at its heart.

Develop and deliver radically new digital offerings with agility

To escape the profit margin erosion in traditional services, Telcos are developing value-added services by leveraging digital technologies and penetrating adjacent industries such as payments, cloud services, gaming, utilities, and even IT services. In order to do this, Telcos have to invest capabilities that are beyond their core ICT capabilities. Also, these new services would require a completely new group of skill sets.

Omnichannel customer experience

Smartphone-related services are at the heart of today's connected experience. The ongoing digital wave has brought multiple touch points such as smartwatches, Smart TVs, wearable gadgets, smart kiosks, etc. Consumers are demanding seamless customer experience and clear cross-channel pathways across various digital channels. This is opening up avenues where telecom operators are facing competition from digital service providers, OTT players, and device manufacturers. To survive against these competitions, Telcos are pressurized to embrace a customer-centric mindset and reposition themselves to provide a 360-degree omnichannel experience to their customers.

Outcome-oriented service management

The cost pressure on Telcos has intensified manifold over the recent years. Telcos are looking forward to enhance their network agility and streamline their processes to cope with these cost pressures. This also implies that Telcos need to invest in the new generation technical infrastructure which will help them to reduce costs and align their service management processes toward business outcomes.

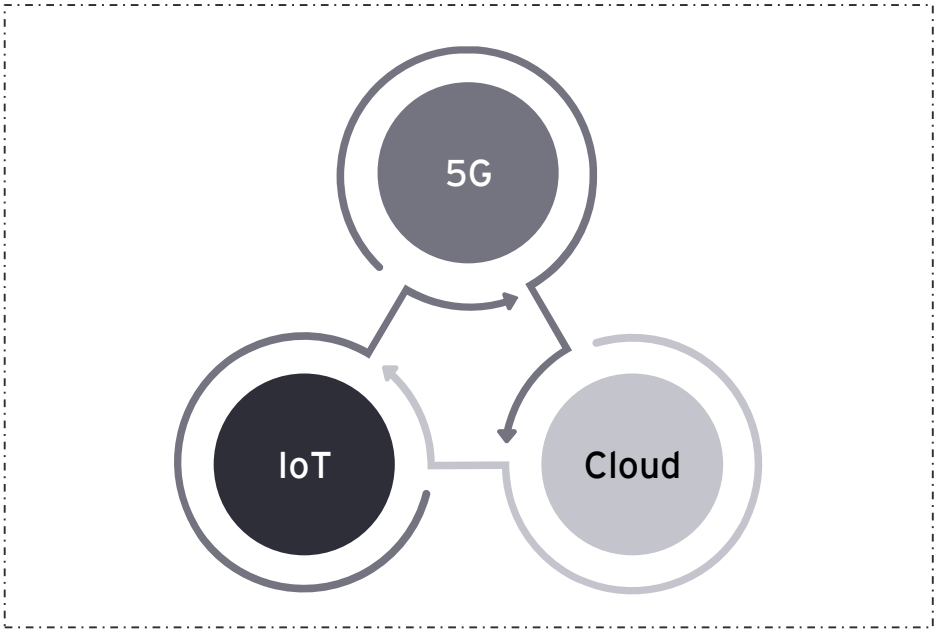
100% consumer trust in data privacy

In the backdrop of the exponentially increasing threats to data privacy of the telecom consumers and the telecom regulatory authorities tightening the regulations, data privacy had risen as a huge challenge to Telcos. This is because of the complexity they add to existing business and operational processes. Despite their huge investments to protect consumer data, Telcos are often finding themselves inadequately protected against cyber attacks targeted at compromising consumer data.

Cyber dimensions of the transformation

To emerge successful, Telcos should prepare themselves for a paradigm shift. They should harness the power of new technologies such as 5G, cloud and IoT to aid them in their digital aspirations. While planning such digital investments which will enable them to cruise through the disruptive market forces, Telcos should also understand that cybersecurity is a linchpin in this transformative journey. Aligning their cybersecurity strategy to their transformation strategy is crucial for Telcos to reap the fruits of their investments.

Key Technology Catalysts of Telco Digital Transformation



5G security: a top priority for Telco leaders

2020 was considered as the year of 5G in the telecom industry. Many telecom operators had plans for large-scale 5G rollouts during this year. 5G technology is often considered as a game changer in the telecom industry due to the paradigm shift it is likely to bring to the industry. It is estimated that 5G will account to around 1.2 billion connections by 2025.[13]

In MENA, Etisalat becomes the first operator in the region to provide 5G services to its customers. Now, the operator has also launched a brand new OTT service called SwitchTV, where the operator is offering a bundled data-free streaming service to its existing subscribers.

Despite the hype around 5G, it raises considerable cybersecurity concerns among the leaders of telecom companies. In a global survey conducted in 2019 among cybersecurity and risk leaders, 83% of the leaders firmly believed that rolling out 5G networks will lead to increased cybersecurity challenges for their organization.[14] The survey report also stated that the vulnerabilities in 5G could also introduce risks around virtualized and cloud native infrastructure.

The key cybersecurity challenges that are introduced due to 5G rollouts are:

- Broadened attack surfaces due to possible vulnerabilities in software used in 5G networks
- Interoperability and sensitivity issues in network hardware caused due to the unique architecture and new functionalities of 5G networks
- Increased exposure to attacks due to the risk profile of a supplier or vendor, as well as the reliance of mobile networks and enterprises on a third-party vendor or supplier
- Network-based threats that can compromise the availability and integrity of 5G networks, which serve as the backbone of mission-critical application

The ongoing COVID-19 pandemic has underlined the importance of 5G network security. Telecom companies are rethinking about the scale and pace of their 5G investments due to the security concerns in 5G and the pessimistic market outlook.

13. GSMA
14. Continuity Central

Cloud: the new hotspot of cyber attacks

Cloud technologies have become a key enabler for Telcos because of the wide array of benefits it offers. Telcos are commercializing "cloud as a user" by realizing cost flexibility for their own organization, and as a provider by offering new solutions for their customers.

Telcos rely on a large computing infrastructure to deliver a diverse set of applications, manage data, and bill services. Migrating to the cloud reduces internal computing resource needs as well as internal costs.

Telcos are also leveraging cloud platforms to develop radically new value propositions that will create new business models and offer a whole new customer experience. Also, the proponents of 5G consider cloud as an essential enabler for 5G networks.

As per the report from INAP, roughly 9 out 10 (88%) of enterprises will migrate some of their workload to cloud by 2022.[15] Despite the significant advantages, cloud platforms have a serious downside. They suffer from four major types of vulnerabilities such as:

- Shared tenancy vulnerabilities
- Poor access controls
- Vulnerabilities due to misconfiguration
- Supply chain vulnerabilities

Due to these vulnerabilities, cloud platforms are less resistant to cyber attacks. Cyber adversaries are increasingly becoming aware of these vulnerabilities. Needless to say, the volume of attacks on cloud platforms are growing exponentially, and cloud environments have become the third most targeted environment for cyber attacks.

South Africa's MTN Group and Etisalat have already monetized cloud service offerings, by providing suite of cloud services at economical pay-as-you-go model to enable small businesses and enterprises to scale-up operations.

The volume of attacks on cloud technology platforms have doubled in 2019 and are accounted for 20% of the reported incidents. After the onset of the COVID-19 pandemic, the number of external attacks on enterprise clouds have increased by 630% within a span of first two months.[16]

15. Forbes
16. Mimecast

IoT: the new weakest link

Telcos can leverage IoT as a consumer to control their own costs and also as a service provider to offer new value propositions to their customers.

Network infrastructure management accounts for the lion's share of the operational costs of Telcos. IoT can always help to control this cost by remote monitoring for management of network assets, physical security and environmental protection.

Telcos can leverage IoT to deliver radically different solutions such as connected cars, IoT platform for Industry 4.0, etc. Also, the IoT platforms can provide a lot of data, which can be leveraged to cement the data monetization strategy of Telcos. In a recent study by IBM, 57% of the Telcos had aspirations to become an IoT platform provider.[17]

In India, Jio has developed an innovative service on its pan-India 4G network called Narrowband Internet of Things (NBIoT). Using NBIoT, data from billions of smart sensors (whether residential, industrial or public) can be collected from across India with the highest reliability and lowest cost. Vodafone Idea and Bharathi Airtel are also preparing to launch commercial NB-IoT services in India.

In South Africa, MTN collaborated with Cisco to deploy the region's first IoT solutions service, which is designed to help enterprises launch, manage and monetize new IoT products and services. Cisco said that MTN will deliver connected services to enterprises more securely and cost-effectively, enabling them to scale globally, as needed.

IoT is a remedy that can address many of today's industrial problems. As a consequence of this, the demand for IoT solutions is soaring up. This increasing demand for IoT is driving device vendors into a race to achieve market dominance in a relatively new and untapped market. Most of the vendors ignore the cybersecurity aspects of the devices due to competitive pressures. It is reported that 98% of all the IoT data traffic is not encrypted.[18] This makes the IoT devices an easy target for cyber adversaries.

The key vulnerabilities of IoT deployments are:

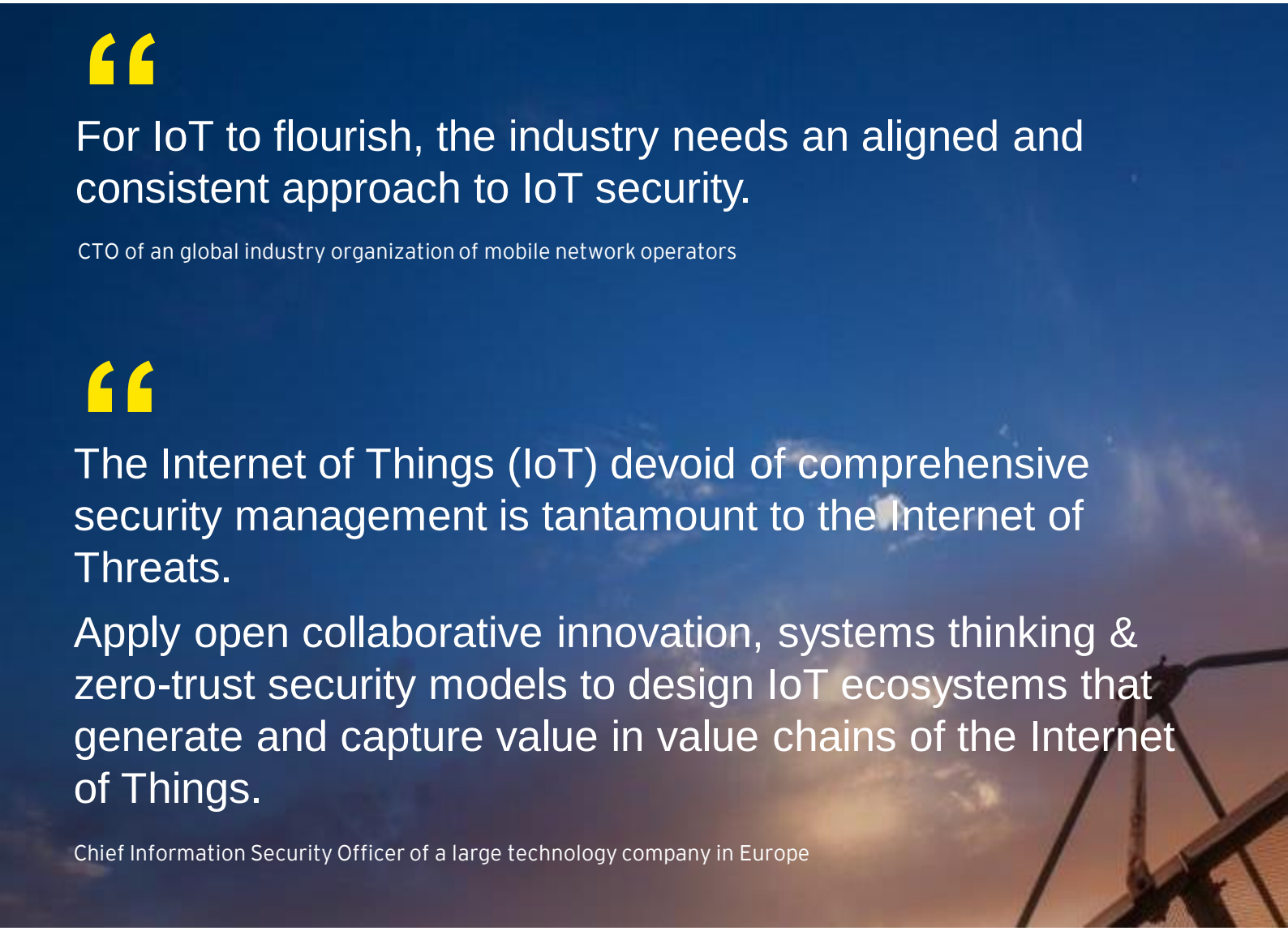
- Weak, guessable and hardcoded passwords
- Insecure network services
- Insecure ecosystem interfaces
- Lack of secure update mechanisms
- Use of insecure or outdated components
- Insufficient privacy protection
- Insecure data transfer and storage
- Lack of device management
- Insecure default settings
- Lack of physical hardening

17. IBM
18. Wire19

In 2019, 61% of the organizations have experienced an IoT security incident. It is reported that, on an average, IoT devices experience 5200 attacks per month.[19]

Since the onset of the COVID-19 pandemic, there has been a significant rise in the number of IoT attacks. It was recorded that the number of attacks against Symantec IoT honeypots increased by 2.2 million compared with previous data, which is a 13% of increase to that of Q4 2019.[20]

For Telcos, IoT deployments are proving to be quite a conundrum figuring out the deployment roadmap and protecting them. It is evident that Telecom companies need a paradigm shift from their "deploy first, protect later" mindset to a "shift-left" practice to consider cybersecurity aspects as early as possible in the implementation of the IoT technologies.



"

For IoT to flourish, the industry needs an aligned and consistent approach to IoT security.

CTO of an global industry organization of mobile network operators

"

The Internet of Things (IoT) devoid of comprehensive security management is tantamount to the Internet of Threats.

Apply open collaborative innovation, systems thinking & zero-trust security models to design IoT ecosystems that generate and capture value in value chains of the Internet of Things.

Chief Information Security Officer of a large technology company in Europe

19. Varonis
20. Symantec blogs

Sprouting cybersecurity opportunities in changing landscape

The changes in consumer landscape, driven by waves of digitalization, are opening up new opportunities in cybersecurity services. Telcos being quick to recognize these opportunities are extending their offerings to penetrate into the cybersecurity market owing to its lucrativeness.

Telcos possess many inherent strengths, which make them a natural choice as a competent security vendor. Telcos can capitalize their strengths and venture into the cybersecurity solutions market as a service provider to generate more revenue streams.

The inherent strengths of Telcos are:

- Access to huge volumes of network data
- Ability to leverage existing large customer base
- Strong footing in cloud-related services market
- Easy extensibility in offering mobile security services

Telcos are joining hands with cybersecurity service providers to address the demand for cybersecurity needs of their customers.

In **April 2019**,

MTN Business Kenya announced the launch of MTN Managed Security as a service – a solution that adds to its array of XaaS offerings to protect their enterprise customers. With this launch, MTN became the first fully certified Managed Security Service Provider (MSSP) in the market.

In **October 2019**,

Du announced its partnership with Wipro to launch IoT security platform in UAE. The platform aims to address the potential threats to securing devices and information within IoT environments.

In **September 2019**,

Emirates Telecommunications Group (Etisalat) has acquired Help AG, a leading provider of tailored cybersecurity solutions and services. After the completion of the acquisition, Help AG will continue to operate as a separate legal entity under Etisalat Digital focusing on the joint cybersecurity portfolio.

In **May 2020**,

Bharti Airtel has launched Airtel Work@Home. This is an enterprise-grade solution designed to enable employees to operate securely from their homes. It bundles a range of connectivity options, collaboration tools, and security solutions that adhere to Indian regulatory norms.

COVID-19 pandemic aggravating cybersecurity pain points

Telcos are grappling to adapt themselves to the changes in the threat landscape due to the digitalization wave. To make things worse, the ongoing COVID-19 pandemic has given rise to new twists in terms of complexity and scale to the cybersecurity needs of Telcos.

After the onset of the pandemic, cyber attacks have evolved into highly sophisticated, dynamic and targeted type of attacks. The increasing variety and volume of attacks are making previously existing network defense mechanisms unreliable. With employees working from home, connecting to their business networks remotely and the consequential increase in potential threat vectors, cybersecurity has become the major pain point for every Telco.

The pandemic has also created further opportunities for threat actors. Almost all the known types of cyber attacks have been reinvigorated with the COVID-19 pandemic themes, including business email compromise, credential phishing, malware and spam email campaigns. Threat detection organizations have found that the monthly volume of all threat activities increased significantly by 33% within the first two months of the pandemic. These include spam, impersonation, malwares and URL blockings. The volume of detections increased from 103.7 million in January 2020 to more than 118.7 million by March 2020.[21]

21. Mimecast

COVID-19 pandemic repercussions on cyber threat landscape

Distributed denial-of-service (DDoS) attacks

- Average bandwidth of attacks have increased by 14%[22]
- Maximum bandwidth has doubled
- Biggest identified attack – 406 Gbps
- 19 attacks used 10 or more different DDoS vectors (no reported attacks of this scale in 2019)

Malware

- Malware detections risen by 35%[24]

Ransomware

- 6 out of 10 malware campaign identified to have ransomware[25]
- Have become highly sophisticated

Signaling threats

- Call tapping on 3G networks have 53% of success
- 9 out of 10 SMSes sent can be intercepted[26]

Attack on employees and consumers

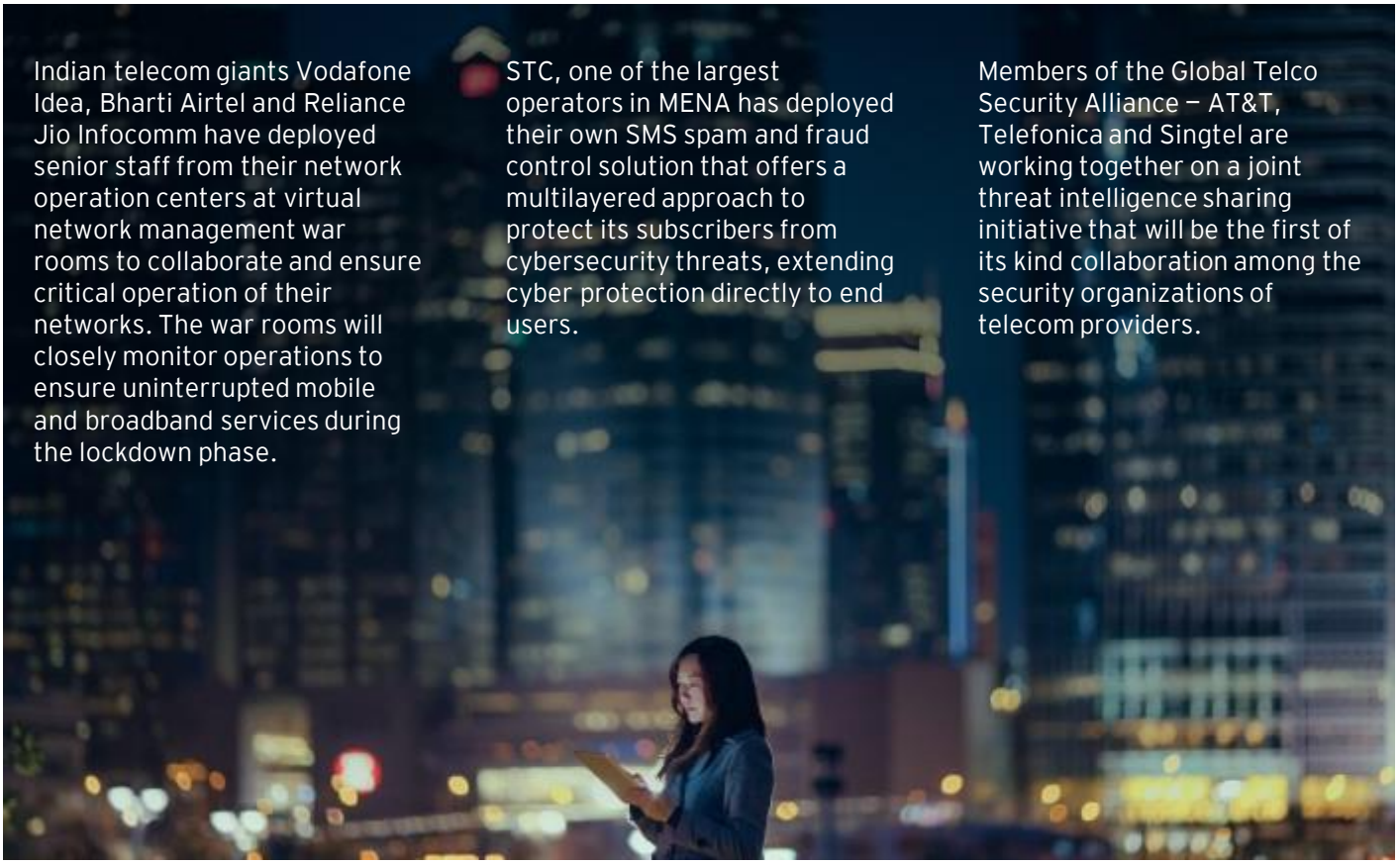
- Employees working from home fall under the highest targeted category for people-based attacks
- Spam attacks of 20.8 million within the first three months of COVID-19 pandemic; which is twice the normal figures[27]
- Increase in impersonation attacks (30%)
- Volume of phishing attacks grown by 300%
- Number of suspicious registrations grown by 450%[28]

> "We have come across media reports on the potential surge in cyber attacks, such as DDoS, malware attacks, and defacement of websites. We have also witnessed an increase in such cyber activity during our security operations."
>
> **Cybersecurity team of a large Indian telecom company on increasing cyber attacks due to COVID-19**

22. Continuity Central
23. Continuity Central
24. Mimecast
25. Mimecast
26. GSMA
27. Mimecast
28. Continuity Central

Telcos inherently provide abundant opportunities for cyber adversaries to launch an attack due to their large customer base. The impact of the ongoing COVID-19 pandemic on cyber threat landscape is alarming. After the onset of the pandemic, the volume of attacks have leaped five to six times of their normal figures. Telcos should prudently revisit their cybersecurity posture to ensure that their business and customers are adequately protected against these spiraling out of control wave of cyber threats.

Telcos response to the COVID-19 pandemic



Indian telecom giants Vodafone Idea, Bharti Airtel and Reliance Jio Infocomm have deployed senior staff from their network operation centers at virtual network management war rooms to collaborate and ensure critical operation of their networks. The war rooms will closely monitor operations to ensure uninterrupted mobile and broadband services during the lockdown phase.

STC, one of the largest operators in MENA has deployed their own SMS spam and fraud control solution that offers a multilayered approach to protect its subscribers from cybersecurity threats, extending cyber protection directly to end users.

Members of the Global Telco Security Alliance — AT&T, Telefonica and Singtel are working together on a joint threat intelligence sharing initiative that will be the first of its kind collaboration among the security organizations of telecom providers.

Outplaying security challenges

Actions that Telcos should take to tackle security challenges

1 Now

General

- External vulnerability assessments and penetration testing
- Continuous patch management
- Deployment of signaling firewall technologies to support the monitoring and blocking of signaling traffic
- Security in cloud architecture
- Third-party risk management
- Compliance to standard industry certifications
- Cybersecurity budget management and management of projects
- Control management review
- Cybersecurity implications of the ongoing 5G and IoT rollouts
- Continuous monitoring on security configuration settings for each layer
- Revisit all BCM and DR security programs and review the list of business continuity scenarios and all related tasks

Consumer security

- Establish channels for quickly informing consumers of suspicious activity or vulnerabilities identified on their systems and support them in addressing any issues, when required
- Protect consumers by default from known cyber attacks, ensure that consumers are informed about the efforts and if desired, provide an option to opt out
- Provide customers with guidance on security best practices and about the channels available to them for reporting suspicious activities
- Provide options for consumers to choose restricting protocols that can prevent damages caused by vulnerable devices
- Block Consumer Premises Equipment (CPE) management protocols from being routed from outside the network unless there are valid reasons for not doing this and ensure that the management plane is not accessible from the internet
- Implement Domain-Based Message Authentication, Reporting and Conformance (DMARC) on network-owned domains and help customers to implement DMARC on their domains

2 Next

Network security (routing and signaling)

- Understand current Border Gateway Protocol (BGP) peering relationships and seek to collaborate with peers to better identify BGP hijacks and be able to effectively respond
- Join the Mutually Agreed Norms for Routing Security (MANRS) project and implement MANRS requirements
- Implement ingress filtering (such as BCP 38 or similar) effective access management for DNS (wherever required) to enhance defense against DDoS attacks
- Raise awareness of the security vulnerabilities of SS7, implement relevant solutions such as the GSMA SS7 filtering standard to better protect customers and ensure that the next generation of signaling is better secured
- Enable Domain Name System Security Extensions (DNSSEC) validation in resolvers and encourage customers to DNSSEC-sign the zones for which they are authoritative

Remote working

- Develop a remote access policy and communicate it to the employees and other stakeholders
- Provide training for employees to be updated about the leading cybersecurity practices
- Conduct phishing exercises for user groups
- Conduct a comprehensive assessment of the VPNs
- Revisit cybersecurity resourcing model

5G security

- Include security components such as edge security, SDN controller security, proactive security analytics for threat detection, hypervisor and container study, and orchestration security to protect 5G networks
- Leverage Management and Network Orchestration (MANO) framework for network slicing, network function virtualization and container management
- Build secure templates for sever deployments and management
- Conduct a comprehensive supply chain assessment and product testing to ensure that the vendor offers security protection for the security lapses for which they are accountable
- Use Security Orchestration Automation and Response (SOAR) for protective monitoring of 5G data
- Do a comprehensive vulnerability assessment of 5G network rollouts through its entire life cycle and implement appropriate security in each stage
- Include mechanisms in 5G rollouts to potentially isolate or close down less secure 2G or 3G networks
- Consider joining in industry initiatives for developing secure implementation models for 5G core and 5G non-standalone (NSA) deployments

Cloud security

- Develop a local policy which covers all cloud delivery models and deployment models including specific controls for provisioning, vendor choice, service implementation, threat detection, data management and destruction
- Use microsegments for the isolation of high-security or legacy areas and use virtualization-aware security tooling to enforce policy and monitor these segments

- Isolate services, tenants, memory and processes effectively
- Use hardware that have appropriate security controls enabled within the virtualization layer
- Purchase virtualization-aware security controls for protecting microsegments and virtual services, and adopt the same approach for cloud services
- Treat virtual systems as physical systems and follow all the applicable IT hygiene practices such as patch management, access controls, vulnerability management, authentication, and hardening practices

IoT security

- Ensure that all IoT devices are compliant with cybersecurity policies, including authentication, encryption, patching and password requirements
- Place compensating controls in place, if password of the IoT devices cannot be changed
- Segment IoT devices from the less secure legacy devices (recommended)
- Include segment blocking mechanisms in place to isolate the segment in the event of an attack
- Monitor IoT traffic to check unauthorized access of the devices
- Restrict access to IoT devices by placing them behind the network defenses
- Restrict outbound activities of IoT devices that does not require external access
- Conduct regular audit of the devices to check the received or transferred data, ensuring that it is sending the expected data to the right location
- Prepare an incident response plan for botnet attacks

Automation and analytics in cybersecurity

- Leverage automation technologies to handle tasks that are repetitive and have high probability for human errors, and to optimize the people utilization of the internal cybersecurity team members
- Use AI network monitoring techniques to identify the root causes of cyber incidents
- Use analytics tools to monitor cybersecurity KPIs
- Use statistical modelling tools for optimizing the cyber spend across the various security components

Collaboration with ecosystem partners

- Collaborate with ecosystem partners to understand the risks of smishing (SMS phishing) on networks and seek inputs to implement measures to reduce and report unusual behavior
- Collaborate with ecosystem partners to spread awareness among retail customers through awareness campaigns

Establish Zero Trust Architecture

- Access based on trust score derived from user identity, device status & context
- Least Privilege
- Adaptive authorization-level based on Trust Score & Risk profile
- Continuous assessment of Trust

Cybersecurity governance

- Create a cybersecurity roadmap to make sure that future security controls are tracked and can be timely implemented
- Increase cybersecurity resource skills and make sure that the security staff is capable to support the newly implemented platforms
- Make sure that data privacy principles and controls are applied for all the data subjects
- Engage a full set of stakeholders to ensure appropriate support and decision-making
- Check effectiveness of implemented cybersecurity controls
- Conduct regular cybersecurity maturity assessments against best practices
- Move away from a "deploy first, protect later" mindset toward a "shift-left" practice, where cybersecurity issues are considered as early as possible in the new deployments and rollouts
- Build a holistic cybersecurity program, which goes beyond technical controls to have a well-balanced protection against cyber threats
- Integrate cybersecurity with business strategy to build trust and create value
- Include risk sharing clauses in contracts with cloud, 5G and IoT technology vendors and service providers
- Clarify the accountabilities of internal cybersecurity teams, service providers, equipment and software vendors of cloud, 5G and IoT technologies
- Set aside a budget for cyber liability insurance

3 Beyond

Collaborate with peers and government agencies

- Collaborate with peers and national as well as international regulatory bodies to determine the most suitable ways to collaborate and protect consumers by default, working together to define new oversight mechanisms and regulatory frameworks, where needed.

Collaborate with manufacturers and vendors to raise security levels

- Collaborate with device manufacturers and vendors to adopt initiatives and frameworks to provide clarity on acceptable minimum standards for 5G equipment and IoT devices across the supply chain. It is recommended to incentivize manufacturers and vendors to do so.

Collaborate with partners (in other industries) to develop security framework for interoperability between sectors

- Collaborate with partners in other industry verticals to develop security frameworks that will enable the interoperability between sectors while penetrating into other industry sectors.

How EY teams can help

How EY teams can support Telcos to stay protected in their digital transformation journey?

Telcos must increasingly rely on new and disruptive digital technologies to help them grow and differentiate themselves in the evolving marketplace. Telcos that lack effective security measures to manage these changes are vulnerable to breaking the trust of their customers, stakeholders, and the marketplace, consequently exposing themselves to an ever-increasing risk.

It's time for a new take on protecting Telcos. This can be achieved by ensuring day-to-day resilience as well as a proactive, pragmatic, and strategic approach that consider risk and security from the onset. This is Security by Design (SbD).

EY Cybersecurity help enables trust in systems, designs and data, so that the organizations can take more risk, make transformational change and support innovation with confidence.

EY Cybersecurity service offerings

The EY organization has a wide portfolio of service offerings for Telcos, which covers aspects such as strategy, consumer security and data privacy, cyber governance and cyber resilience.

Strategy, Risk, Compliance Resilience

Helps clients to evaluate the effectiveness and efficiencies of their cybersecurity and resiliency program in context of the business growth and operations strategies

Data Protection and Privacy

Helps companies to protect their information over the full data life cycle – from acquisition to disposal

Identity and Access Management

Helps companies with their definition of access management strategy, governance, access transformation, and ongoing operations

Architecture, Engineering & Emerging Technology

Helps companies to protect their organizations from adversaries that would seek to exploit weaknesses in the design, implementation, and operation of their technical security controls, including disruptive technologies in the marketplace

Next Generation Security Operations & Response

Helps clients to proactively identify and manage risks, monitor threats, and investigate the effects of real-world attacks which will in turn rapidly integrate cybersecurity functions and technologies to adapt to demands

EY Cognitive Cybersecurity Centre (CCC)

- Next Generation Cognitive Cyber platform to detect threats across Data Centre, Office Network and Public Cloud
- Actionable and Automated response for faster response
- Integrated Fully AI & ML driven Network Flow/Packet, User behaviour analytics, SIEM, Threat Hunting and Big Data Platform

EY DSOC short-term offering to address the COVID-19 cyber risk

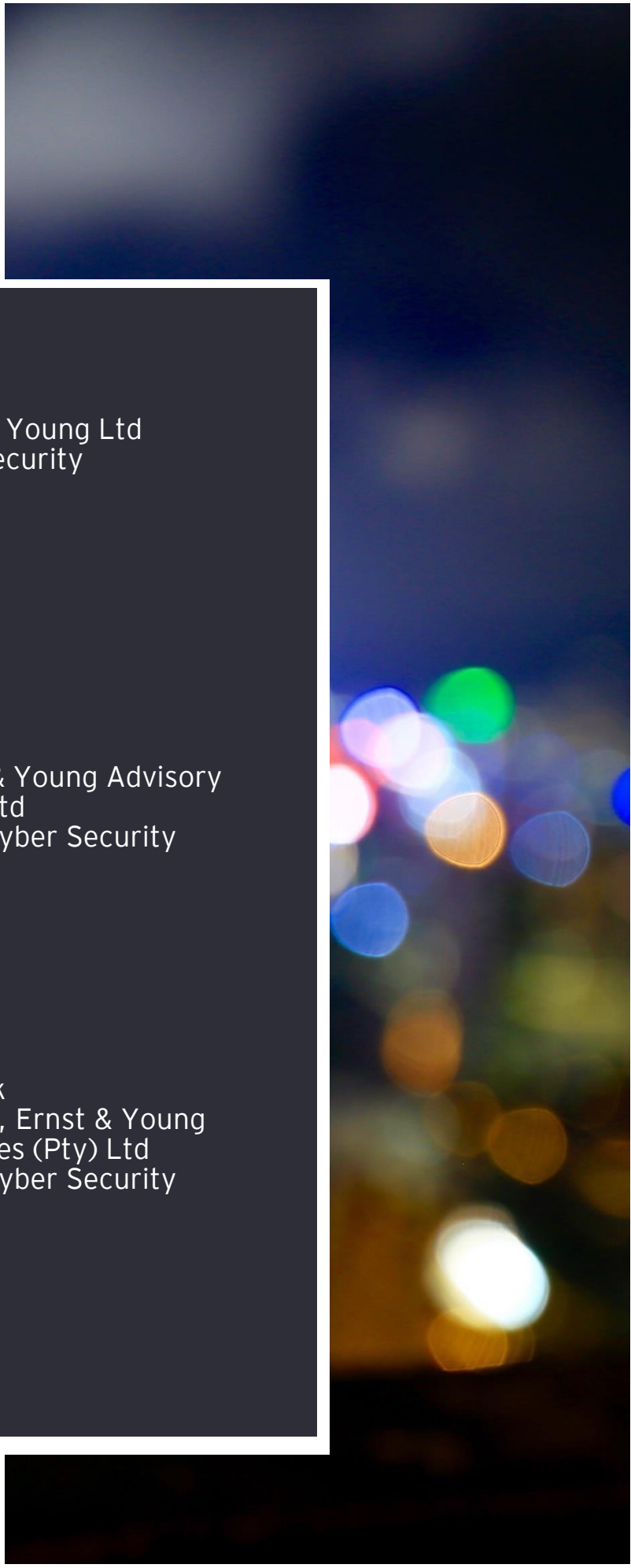
24x7 remote security monitoring services

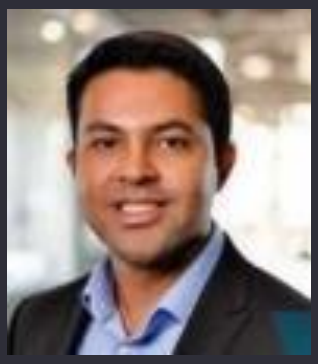
To address the soaring volume of cyber attacks, EY teams offers a rapid deployment of security monitoring solutions by deploying "specialized cyber monitoring technology" or leveraging existing Security information and event management (SIEM) technology to provide 24x7 security threat detection during this COVID-19 pandemic.

EY remote security assessments

To address enhanced telecommuting-related risks amid COVID-19 pandemic, EY teams offers the two-week rapid remote security assessment services which include DMZ or external vulnerability assessment, penetration testing, VPN security assessment, phishing exercise for 50 users and remote access policy development or update.

About authors





Ritesh Guttoo
Partner, Ernst & Young Ltd
Africa - Cyber Security

Cathy Gibson
Partner, Ernst & Young Advisory Services (Pty) Ltd
South Africa - Cyber Security

Pinar Karabacak
Senior Manager, Ernst & Young Advisory Services (Pty) Ltd
South Africa - Cyber Security

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organization or its member firms.

© 2020 EYGM Limited.
All Rights Reserved.

EYG no. 005718-20Gbl

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com