KPMG

Global Perspectives on Cyber Security in Telco:

A roundtable discussion on the state of cyber security management in the telco sector

Contributors

Atul Gupta
Partner,
KPMG in India

Atul is a Partner, Global Cyber Lead for Telco and Head of IT Advisory with KPMG in India. In his global role, Atul is responsible for defining the strategic direction for cyber security in Telco. Atul specializes in leading large-scale transformation and Telco cyber security programs for clients, which enable effective management of emerging cyber threats. Atul holds an MBA in Operations and Systems. He is a Certified Information Security Auditor and trained BS7799 Lead Auditor.

Fred Rica
Principal,
KPMG in the US

Fred is a Principal in KPMG Cyber and the National Cyber Defense Leader in the US. Fred is a skilled technology professional with significant experience in IT security, governance and risk management. Fred is a nationally recognized authority on the subject of information security and has performed or managed numerous security assessments, design and implementation projects of large and complex processing environments over the last twenty five years.

Martijn Verbree
Partner,
KPMG in the UK

Martijn is a Partner in the London office, specializing in cyber security and digital. Martijn has been with KPMG since 1999 and has worked for the Dutch, Australian and UK member firms. During 2015 and 2016, Martijn took a two-year career break from KPMG to run a European technology start-up that provides location management services to enterprise clients and improves last mile delivery, collections and customer engagement.

Dani Michaux
Partner,
KPMG in Malaysia

Dani is a Partner in KPMG Management Consulting IT Advisory based in Malaysia. She is currently the ASEAN and ASPAC Cyber Security Lead and a part of the Cloud Computing Group in KPMG in Malaysia and leading the cloud security initiatives. She has extensive experience consulting multiple clients on cyber transformation projects especially to the financial, telecommunications, energy, and government sectors. She has completed various engagements where she was seconded as the acting Chief Information Security Officer (CISO) for energy and telecommunications clients.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Without a doubt, the telco sector is an industry undergoing significant change. We have seen how these organizations have shifted from traditional business models, as carriers of voice and data connectivity, to enablers of sophisticated technology. This shift is altering consumer and business behaviors, and becoming a critical backbone which industry, government and society depend on.

Everyday, we see innovations that have the potential to transform communication — and therefore the ability of telcos to create new value. There are numerous recent examples of such innovations: APIs which ease information exchange between consumers and business, IoT connectivity that enables supply chains and 5G networks that make smart phones the single-device access point for any need.

This transformation is an exciting opportunity for telcos, both to deliver differentiated services that engage customers, and to unearth new revenue sources that monetize the data they wield. However, it also requires telcos to change their ways of doing business and to pioneer emerging technologies, often by extending their network of ecosystem partners and potentially blurring the definition of a telco. All of this creates new risks and responsibilities relating to cyber security, which telcos must manage, if they are to retain customer trust, navigate increasing regulatory demands and satisfy shareholders.

To illuminate the cyber challenges that telco providers face, we recently brought together several of KPMG member firms regional Global Cyber Security practice leaders for a roundtable discussion of the latest trends. As you'll see, these specialists highlight key themes, regarding the need for telcos to strengthen their governance and resiliency, embed cyber security thinking within the business, and embrace new thinking about the cyber security function itself.

I hope this dialogue provides you with some fresh insights into relevant trends and issues and stirs further discussions about the best practice responses and strategies that are today within reach.

Atul Gupta
Global Cyber Lead, Telecommunications
KPMG International

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

What are the largest cyber security trends among telcos in your region?

Perspective from the USA

Fred Rica
Telecommunications Lead, Cyber Security Services
KPMG in the US

USA (Fred Rica): "I see a new or renewed focus on creating a more robust governance model. This comes after the telcos have spent considerable time and energy on technology solutions, based on the traditional security model of 'Deploy technology first and ask questions later.' The result is that they are really good at scanning the network, but they could be better at interpreting and understanding the results. With so much reporting data and compliance testing, senior leaders are saying, 'Help me understand clearly what and why we are doing this, and how it helps me enable or run my business better?'"

Perspective from Europe

Martijn Verbree
Telecommunications Lead, Cyber Security Services
KPMG in the UK

Europe (Martijn Verbree): "The regulatory drivers are having a big impact, particularly with the GDPR roll-out, European legislation to protect critical national infrastructure, and the introduction of mandatory testing for telcos in the UK — all of which influence regulation in other jurisdictions. Interestingly, this is prompting telcos to look at overall operational resilience and cyber resilience, since new external threats are cutting across physical, network and cyber assets. It's becoming important for these previously-vertical silos to come together and look at the whole, including the horizontal and downstream impacts. The siloed security approach is no longer enough to satisfy a regulator, and you need to rethink this and take a more end-to-end view of organizational security."

Perspective from Asia

Dani Michaux
ASPAC Cyber Security Services
KPMG in Malaysia

Asia (Dani Michaux): "There's much excitement about all the tools and gadgets the telcos are developing and deploying. This is raising big questions about how to introduce innovation without adding vulnerabilities to their networks or our customers, particularly since many telcos are embracing open software, agile development and a growing ecosystem of development and service partners. For example, as telco clients demand more public, private and hybrid cloud services, telcos must manage a number of third parties and sort out dispersed responsibilities, to ensure the right governance and response mechanisms are in place."

Other observed global cyber security trends

- CISOs are being provided broader responsibility and accountability to build cyber resilience across enterprise technology and active telecom network (along with value added services).
- Telcos are enabling new age digital business model and to ensure that the security risks are managed well, cyber risk agenda is being broadened to include digital security risk (covering identity, API security, connected devices amongst many others).
- Regulators are focused on cyber agenda, which is leading to specific compliance requirements on cyber security for Telco. Regulators are ensuring that these requirements are forward looking, factoring in the potential growth on new technologies.
- Cyber Incidents have resulted in far reaching impacts (including interruption of business, loss of intellectual property and reputational damage), leading to global telcos building robust cyber incident response capabilities.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

What leading practices do you see telcos deploying to address these issues?

Perspective from the USA

USA (Fred Rica): "Many telcos are carefully assessing their current governance models, whether they have the right policies and the right roles, responsibilities and reporting relationships. They are seeing the need to consolidate all of their data for better reporting and analysis in an automated fashion, ideally on a single system that can generate 'a single version of the truth,' and create a true governance, risk and compliance platform."

Perspective from Europe

Europe (Martijn Verbree): "Awareness of cyber issues is strong among senior management and boards, however there is still much that could be done to strengthen end-to-end organizational resiliency. There is still too much 'Cyber is the territory of the Chief Information Security Officer (CISO), while someone else is responsible for the rest.' This needs to shift to a more end-to-end risk-based view in which everyone considers systemic risks across the value chain, and not just within their function. This requires a significant business change and it must cascade down from the top through middle management."

Perspective from Asia

Asia (Dani Michaux): "To manage the complex network of service partners, I think the telcos require a different way of thinking, in collaboration with your eco-system partners, and not just within their own organization. For instance, before you decide to adopt a cloud platform, you need to have more strategic discussions with your partners about how to embed security and assign very clear understanding, accountability and contractual provisions for each party."

Other observed global cyber practices

- Board and senior management is being provided common understanding on the cyber risk through Management Reporting and Cyber Dashboarding.
- There is significant focus on securing identities across the multiple channels. This is getting extended to customers to secure digital identities.
- Supply Chain has emerged as a critical area for Telcos from cyber perspective and globally large organizations are ensuring that there is adequate focus on cyber being embedded in Supply Chain and business partners/ third parties.
- Cyber is being proactively focused during transactions (Merger & Acquisition activities) to ensure that risk profile is comprehended and addressed by design.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

How do you see the telcos managing their regulatory obligations?

Perspective from the USA

USA (Fred Rica): "As Martijn mentioned, there is much focus on GDPR, as well as uncertainty, since the guidance is not particularly prescriptive nor are the sanctions for non-compliance clear yet. Whatever the specifics, I don't foresee a scenario where there is less regulation on the horizon, so it becomes a case of telcos identifying if new rules are applicable, determining how to comply and then monitoring their activities to address any gaps. This exercise can be like the 'whack-a-mole' game since you are trying to satisfy many rules and repeatedly testing the same areas. That's why KPMG professionals are helping clients adopt a unified compliance framework by which they use an automated platform to 'test once and comply with many,' when different rules have common elements. That can greatly reduce the burden on business and systems owners."

Perspective from Europe

Europe (Martijn Verbree): "With the new threats crossing previous operational boundaries, regulators will demand evidence of a more integrated approach on the part of the telcos to protect themselves. This will drive telcos to bring together physical security, cyber and the backend networks by which phone calls connect. These areas were traditionally out of the realm of the CISO, but now it is necessary for them to form a coordinated defense. It has become important for these previously-vertical silos to come together and look at the whole, including the horizontal and downstream impacts. The siloed security approach is no longer enough to satisfy a regulator, and you need to take a more end-to-end view of organizational security. This means reorganizing internally, since many telco functions, from voice to data and privacy to fraud, are still managed as silos. This new regulatory pressure is a significant challenge, but it's a good direction for the industry to move to create better operational resiliency to safeguard organizations, their critical networks and customers."

Perspective from Asia

Asia (Dani Michaux): "KPMG professionals see how GDPR can have far-reaching impacts here in Asia. Some organizations don't fully understand this regulation, and they might assume it doesn't apply to them. In reality, even non-EU companies that offer services to EU residents, or process EU resident data, need to comply. Also, the thought of stricter data privacy and security rules can raise concerns among clients as they consider new ways to monetize customer data. This could slow down their innovation initiatives. On a positive note, there may be opportunities for telcos to build more constructive relationships with regulators as national and regional governments intensify their efforts to combat cybercrime. As key participants in the cyber ecosystem, telco operators could play a proactive, collaborative role with government. KPMG professionals have seen examples of industry/regulatory collaboration in the UK, and it can't hurt for telcos to build mature, working relationships with the authorities, so both parties understand each other's positions better."

Other observed global cyber practices to manage regulatory obligations

- Telcos have significant focus on regulatory compliance, specifically with the ongoing convergence with media and banking sector. Telcos are required to adhere to cyber security regulations applicable in the banking and media sectors.
- Telco (and/ or industry representative bodies) are proactively participating with regulator during formalization of cyber compliance and regulatory requirements. This is leading to more effective adoption of regulatory requirements across industry.
- Telcos are preparing to meet the regulatory requirements for services that shall be offered in future. In emerging areas, specifically around IoT and connected devices, Telcos are working with the equipment providers to have robust security controls by design.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

With adoption of new technologies, and potential consolidation and convergence of services, how can telcos prepare for the emerging cyber risks?

Perspective from the USA

USA (Fred Rica): "In addition to risk prevention, the telcos must focus on risk management and mitigation. For example, the coming roll-out of 5G represents the next big evolution of their networks, and the potential to revolutionize the user experience in terms of content and service delivery over your smart phone. Since different customer segments will feel differently about the emerging security and privacy issues, the key could be to empower customers to customize the controls they want, and let them decide when and how they want to be connected. Then, in light of the industry-wide recognition that an incident of some sort is likely inevitable with most new technologies, the telcos must really focus on how to minimize the magnitude of an event, so they can recover as quickly as possible and reduce the impact on their customers."

Perspective from Europe

Europe (Martijn Verbree): "There is certainly consolidation going on, but not in the old way by which 'Company A' buys 'Company B.' Now telcos are partnering with other firms, large and small, through APIs and bringing these ecosystems together, through smart phones and the IoT. This is bringing good ideas to the market, in a bottom-driven way, however, security and risks are often an after-thought because the cyber people are not in the room when these ideas come up. When they are at the table, there can be friction between the security people and the business. The key is to raise awareness in the business among the people who invent and execute ideas without stopping innovation, plus putting in place suitable checks to identify risks quickly before they become big issues."

Perspective from Asia

Asia (Dani Michaux): "Yes, it's crucial for the cyber team to be better involved in the business. I think the CISO of the future won't be the same technical leader as in the past but rather they should be embedded in the business functions, having direct conversations about strategy. That way, security becomes a part of the product, and these controls can be incorporated early on with the ecosystem partners. You can create a strong security culture within the business, empower them, and even decentralize and automate some of the security requirements with digital tools for testing or analytics. Even for complex concepts like digital identities and the challenge of human versus device identities, my view is that KPMG professionals can take the discussion back to the basics and ask, 'What are you trying to do?' and 'What are the exposures you need to consider?' in the early stages of the project. That's a very different ball game, by which you are conducting a proper risk assessment while allowing innovation to continue at the speed that the business needs."

Other leading global practices to prepare for emerging cyber risks

- Adopt holistic approach with appropriate security across data channels/interfaces.
- Establish security as "in-line" process activity rather than a separate activity disjointed from the main process of development and deployment of emerging technology.
- Proactive security risk assessment of new products, channels or any new emerging technology like 5G, IoT, NFV, SDN.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Can telcos turn cyber security into an opportunity to differentiate themselves in their markets?

Perspective from the USA

USA (Fred Rica): "I believe that cyber security is an essential ingredient to telco growth plans and their ability to roll out many cool ideas and more customized products and services. The telcos realize that if they want to have more intimate relationships with their clients, they need to have better security and privacy protections to earn that trust. I often say, 'You don't have brakes in your car so you can go slow, but rather you have brakes so your car can go fast.' If you buy a sports car, you just assume the brakes will work, and that's the same with cyber security.

In terms of leading with cyber security as a market distinguisher, I think that telcos are in a really unique position to fix one of the single biggest security challenges, namely passwords. They are a very inefficient way to verify someone's identity and telcos could resolve the problem by introducing the next generation of user authentication through devices. Today, everyone has a phone on which they likely perform an authentication step already. And, since we use our phones for almost everything, the telco operator knows so much about a customer's behaviour, and the telco could become *the* authoritative source for authentication, for consumers and the companies they deal with. It's an interesting challenge for telcos to think about."

Perspective from Europe

Europe (Martijn Verbree): "I agree there is quite an opportunity for telcos in that area. And, it's likely essential for them to find new ways to add value, in light of the competition in basic carrier services and the fact that it will become a race to the bottom as someone will always offer a cheaper service. The next level of value could be for telcos to be a trusted custodian for my personal data and with my consent, they share information with other development parties for easier, frictionless sign-on, registration and validation processes for the consumer.

Ultimately, a telco could become *the* preferred cyber security provider of connected IoT and also turn all of the consumer data they have to their advantage for their customers and merchants. To do so, the telcos need to sort out who they want to be in the information ecosystem — whether they are bit carriers who move data from 'A' to 'B,' or whether they will develop higher value propositions, likely in partnership with others. To resolve the cyber security hurdles, they need to deal with the traditional business silos, consider how they can take a more front-to-back value chain approach, to resolve the key regulations and the systemic risks, and bake cybersecurity into the design of all those new initiatives."

Perspective from Asia

Asia (Dani Michaux): "Certainly they can turn these investments into opportunity, whether its mobile wallet for consumers or security services for enterprise and industrial customers, some operators being quite aggressive in this area. As people shift to the new digital world, cyber security is paramount to earning customer trust. The challenge is how can you make these new innovations available to consumers as quickly as possible. One of the keys, as we've discussed above, is realizing that you must begin to change your security function in line with what the business is doing. If the rest of your organization is moving to digitization and automation, you need to apply the same thinking to your security function and find ways to shift to the agile world, rethink how you work with the business for the future."

Other leading global perspectives on turning cyber security into opportunity

— Telcos are in unique position to offer cyber security services to enterprises, specifically on back of other enterprise services (including Cloud services). Many operators have already adopted this path and have become trusted enterprise security partners for multiple organizations.

— Cyber is being positioned by large telcos as their commitment to customer on providing trusted services, which is pertinent in era of providing enhanced digital services.

— Cyber criminals have focused attack on the subscriber smart devices, specifically devices having enhanced value added services (such as wallet/content/quad-play services/ authentication channel). Global Telcos are using this as an opportunity to establish trust by providing services on securing end subscriber devices.

— Telcos capture significant information of individuals and there is huge opportunity to provide services based on this data. Effective usage of this data in the era of emerging technology along with adequate cyber security controls shall be a significant differentiator.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Closing notes

Telecom is an industry which has undergone significant transformation and also simultaneously enabled all of us to leverage the power of technology. The emerging technologies continue to demonstrate that this industry will continue to evolve and provide more value added services.

As the industry transforms, there will be newer elements of cyber security risks and it is prudent for Telcos to have a comprehensive risk framework to address them holistically.

This document covered various aspects across the three global regions related to cyber security, specifically factoring in next generation technologies. The areas covered in the document include:

— cyber security trends across Telcos

— best practices being adopted

— practices adopted to manage regulatory obligations

— preparing to deal with emerging cyber risks

— turning cyber security into an opportunity to differentiate in market.

While there are limitations in predicting the future (specifically considering the potential of newer technologies, such as Machine Learning, Blockchain, etc), this document is intended to be helpful in providing insights to build a trusted, resilient, safe and secure environment.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Notes

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Notes

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Contacts

Fred Rica
Telecommunications Lead, Cyber Security Services
KPMG in the US

Martijn Verbree
Telecommunications Lead, Cyber Security Services
KPMG in the UK

Dani Michaux
ASPAC Cyber Security Services
KPMG in Malaysia

Atul Gupta
Global Cyber Lead, Telecommunications
KPMG International

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by Evalueserve.
Publication name: Telco POV article
Publication number: 135815-G
Publication date: January 2019

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.