C-SUITE

ISSUE 4 VOLOUME 5 DEC 2023

BENEDICT CHENG

Group Chief Risk Officer at PCCW

POWERED BY ASIA CEO COMMUNITY & CSUITE XCHANGE

The Role

HOW DO YOU DEFINE THE ROLE OF A CHIEF RISK OFFICER IN THE TELECOMMUNICATIONS INDUSTRY, AND WHAT ARE THE KEY RESPONSIBILITIES ASSOCIATED WITH THIS POSITION?

As with any Chief Risk Officer in a specific industry sector, the primary role is to oversee an organization's comprehensive risk management activities, ensuring the timely identification and mitigation of principal and top risks. This pivotal position encompasses a range of key responsibilities. It involves crafting and implementing an enterprise risk management framework tailored to the unique challenges and risks within the telecom industry, such as technology-related incidents, network outages, cyber threats, and regulatory compliance. The CRO also leads risk assessments across various domains, including operational, financial, strategic, compliance, and supply chain, ensuring a thorough understanding and prioritization of organizational risks.

Furthermore, they actively monitor emerging risks by scanning the competitive landscape, tracking market trends, staying abreast of proposed regulations, and considering geopolitical issues. The CRO's role includes providing guidance and reporting to senior management, committees, and board members regarding risk profiles, exposure levels, mitigation strategies, risk appetites, and recommendations for improvement. They also manage business continuity and disaster recovery plans, aiming to minimize downtime and bolster operational resilience. Oversight of information security frameworks, data privacy programs, and physical security protocols is another crucial facet of the role. The CRO plays a key role in promoting an enterprise-wide risk-aware culture through consistent communication and training, and collaborates closely with business leaders to seamlessly integrate risk management into the fabric of business objectives and day-to-day decision-making processes.

In summary, the CRO serves as the central advisor on risk issues and works to create an integrated risk-intelligent culture across the organization. The CRO should always lead by example while acting as enabler such that appropriate risk-taking is balanced with protecting assets/IPs and franchise value of the company.

RISK MANAGEMENT FRAMEWORK

“BENEDICT CHENG

CAN YOU DESCRIBE THE RISK MANAGEMENT FRAMEWORK AND PROCESSES THAT YOU HAVE IMPLEMENTED WITHIN YOUR ORGANIZATION?

THREE LINES OF DEFENSE

Our enterprise risk management framework is guided by the “Three Lines of Defense” model in clarifying roles and responsibilities:

In the first line of defense, we have our business operations and front-line units. Their primary responsibility is to own and manage day-to-day risks directly. They are tasked with the implementation and execution of controls to mitigate these risks. Additionally, this line is responsible for identifying issues and risks as they arise and handling incidents in a timely and efficient manner. In essence, the first line takes ownership of risk management at the operational level.

The second line of defense comprises oversight and control functions. Their role is to provide expertise, advisory services, and quality assurance to the organization. They set the standards, establish frameworks, and formulate policies that ensure compliance with regulatory requirements and industry standards. Moreover, the second line oversees compliance activities and actively challenges the practices of the first line to ensure that best practices are consistently applied across the organization.

The third line of defense takes on the role of independent assurance and audit. Its primary function is to provide independent oversight and validation of controls. This line is responsible for ensuring that the controls in place are effective and that the risk management processes are operating as intended. In doing so, the third line offers valuable recommendations for improvement based on its assessments.

The key objectives of the TLOD are to segregate responsibilities, and to clearly define risk ownership at source through implementation of separate control and monitoring business activities in achieving compliance. More importantly, independent validation of controls and risk oversight is the overarching principle in the TLOD ensuring risks are managed properly at multiple levels in our organization.

IDENTIFY RISK

Telecommunications Industry

WHAT METHODOLOGIES OR APPROACHES DO YOU USE TO IDENTIFY AND ASSESS RISKS SPECIFIC TO THE TELECOMMUNICATIONS INDUSTRY?

In the dynamic telecommunications industry, robust risk management is pivotal to maintaining operational stability and safeguarding against potential threats. This sector employs a range of methodologies and approaches for a comprehensive assessment of risks and vulnerabilities. These methods are critical for ensuring the industry's resilience and ability to deliver uninterrupted services to customers.

Two fundamental pillars of risk assessment include risk factor analysis and business impact analysis. Risk factor analysis involves evaluating potential threats based on their likelihood and the potential severity of their impact. This aids in quantifying the levels of residual risk exposure, offering a basis for targeted risk mitigation strategies. In parallel, business impact analysis is instrumental in identifying critical business functions and estimating potential losses resulting from disruptions. It helps to prioritize resource allocation, ensuring that essential operations receive adequate protection.

For safeguarding digital infrastructure, vulnerability assessments are key. These assessments involve scanning networks, penetration testing of applications and systems to detect security weaknesses or gaps that might be exploited. The focus here is on maintaining a robust cybersecurity posture and overall risk readiness. Moreover, physical security assessments identify vulnerabilities in the physical infrastructure and environmental controls. These assessments guard against risks such as equipment failure, fires, and environmental factors that could disrupt telecommunications operations.

Regulatory and financial crime compliance assessments are vital to ensure adherence to industry regulations and standards, e.g. the Anti-Money Laundering Ordinance (AMLO) and Payment Card Industry Data Security Standard (PCI). This confirms that the organization complies with legal and financial requirements. Moreover, third-party risk assessments evaluate risks linked to external partners, including vendors, suppliers, and outsourced entities. This examination scrutinizes factors such as financial stability and cybersecurity practices to mitigate risks stemming from external collaborations.

Operational risk assessments play a critical role in identifying risks associated with processes, human factors, dependencies, and capacity limitations that could disrupt telecommunications operations. Network modeling is a simulation-based approach used to evaluate infrastructure risks by modeling network traffic loads, potential points of failure, and various operational scenarios. Lastly, continuous monitoring of threat intelligence is essential to track cyber threats, threat actors, malware campaigns, and vulnerabilities, offering insights into risk likelihood.

The most effective risk assessment approach in the telecommunications industry involves a comprehensive blend of quantitative and qualitative data. This combination serves as a foundational benchmark for risk-based decision-making. It guides organizations in the implementation of targeted risk mitigation strategies, ensuring the security and reliability of telecommunications services and aligning with the sector's unique demands and evolving requirements.

Optimal allocation of resources

C-SUITE

ASIA CEO COMMUNITY

HOW DO YOU PRIORITIZE RISKS AND ALLOCATE RESOURCES TO EFFECTIVELY MANAGE THEM?

A critical aspect of risk management in the telecommunications industry is the use of a risk matrix. This tool enables the visualization and calibration of risks on a matrix or in the form of a heatmap, assessing the likelihood versus impact of each potential risk. The focus is on allocating resources to address high likelihood, high impact risks as top priorities. By strategically plotting these risks, organizations can identify and tackle those with the potential to cause the most significant disruptions.

Another crucial step in risk assessment is the quantification of potential loss associated with each risk. This involves estimating potential financial, productivity, and reputation losses that might result from risk realization. Risks associated with higher potential losses warrant more extensive resource allocation, as the impact on the organization is more substantial.

Assessing risk appetite is fundamental in determining how much residual risk an organization is willing to accept. Risks that fall within the acceptable threshold can be

managed with lower resource allocation. Prioritizing risks also involves ranking them by urgency, considering the speed at which they could materialize. Risks that have the potential for faster onset may require more immediate and urgent attention.

Evaluating the effectiveness of existing controls is crucial. In cases where current controls are inadequate, additional resources may be required to reduce the residual risk exposure. Each mitigation plan, depending on the assessed risk, will necessitate specific budgets, tools, and staffing to be effective.

Risk management involves considering dependencies between risks. This includes addressing risks that could trigger cascade effects or contagion. A defense-in-depth strategy is developed accordingly to ensure comprehensive protection. Risks are often classified as strategic, operational, or financial. Strategic risks, in particular, may require more immediate attention at the board level due to their potential impact on the organization's long-term goals.

Where feasible, risks are transferred to external parties, such as insurers, suppliers, or partners, in a cost-effective manner. Additionally, organizations leverage technology to enhance their risk management efforts. Automated threat monitoring and risk analysis tools are employed to augment the capabilities of staff and enhance risk assessment.

Balancing priorities, costs versus benefits, and risk interdependencies is key. The ultimate goal is an optimal allocation of resources to efficiently reduce the most serious residual risk exposures.

COMMON TYPE OF RISKS

In the telecommunications industry, common risks include network outages, cyberattacks, data breaches, and more. Mitigation strategies involve redundancy, cybersecurity, and diversifying vendors, along with a balance of technology, policy, processes, and training for long-term sustainability.

IN THE TELECOMMUNICATIONS INDUSTRY, WHAT ARE SOME OF THE MOST COMMON TYPES OF RISKS THAT YOU ENCOUNTER, AND HOW DO YOU MITIGATE THEM?

NETWORK OUTAGES

Mitigation with redundancy, disaster recovery systems, load balancing

SYSTEMS FAILURES

Prevention with regular maintenance, testing, failover infrastructure

CYBERATTACKS

Protection through firewalls, malware prevention, access controls, encryption, segregation of roles and responsibilities

Charmaine Cheung

EDITED BY

DATA BREACHES

Risk reduction by limiting data collection, encryption, access controls and storage

FRAUD

Detection with analytics, trend/usage monitoring and internal controls

REGULATORY NON-COMPLIANCE

Management through audits, policy and procedures reviews, training

SUPPLY CHAIN DISRUPTIONS

Diversification of vendors, require BC plans, manage inventories

INADEQUATE CAPACITY

Forecast demand, monitor usage trends, scale elastically

LEGACY SYSTEMS

Gradual modernization/digitization, isolate and protect critical systems

THESE MEASURES AIM TO REDUCE THE LIKELIHOOD OF RISKS AND MINIMIZE THEIR IMPACT IF THEY OCCUR.

SKILL SHORTAGES

Talent development and retention, offer competitive compensation

PHYSICAL DAMAGE

Site redundancy, backup power, fire/flood prevention

INSIDER THREATS

Background checks, behavioral monitoring, access limitations, disciplinary actions

REPUTATIONAL RISKS

Social media monitoring, engage customers, ethical practices

MITIGATION STRATEGIES SHOULD FOCUS ON REDUCING LIKELIHOOD OF OCCURRENCE THROUGH PREVENTIVE CONTROLS AS WELL AS MINIMIZING IMPACT IF THE RISK EVENT OCCURS THROUGH DETECTIVE CONTROLS AND INCIDENT RESPONSE PLANS. THE RIGHT BALANCE OF TECHNOLOGY, POLICY, PROCESS AND TRAINING IS IMPORTANT IN ACHIEVING LONG-TERM SUSTAINABILITY GOALS.

STAY INFORMED

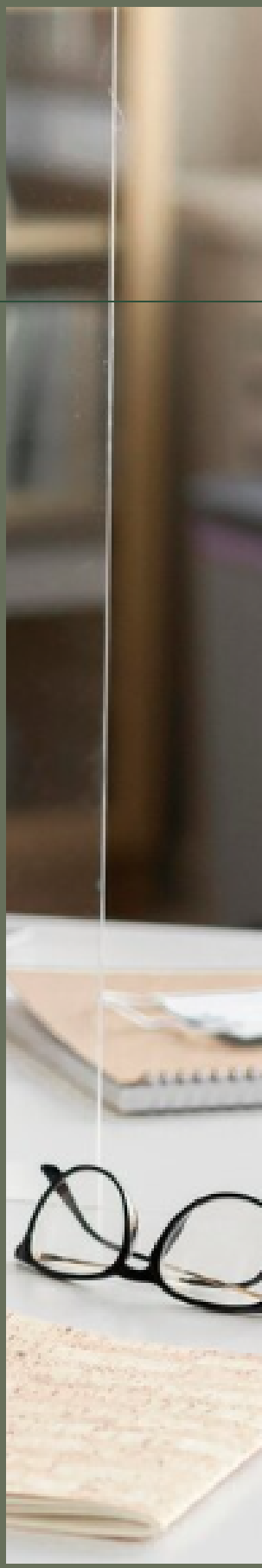
HOW DO YOU STAY INFORMED ABOUT EMERGING RISKS AND REGULATORY CHANGES THAT MAY IMPACT THE TELECOMMUNICATIONS SECTOR?

Staying informed about emerging risks and regulatory changes in the telecommunications sector is crucial for professionals and individuals involved in the telecom sector. Strategies to be considered:

One approach is to subscribe to reputable industry publications and newsletters dedicated to the telecom sector. These publications serve as valuable sources of information, covering emerging risks, regulatory adjustments, and industry trends. Likewise, professionals should actively monitor the websites and publications of regulatory bodies and government agencies overseeing the telecom industry. These organizations often release updates, reports, and announcements concerning the ever-shifting regulatory landscape.

To deepen one's understanding of emerging risks and regulatory changes, joining relevant industry associations and trade organizations is highly beneficial. These groups offer a wealth of resources, including research papers, webinars, and events focused on industry dynamics. This engagement provides a platform for sharing insights and networking with experts who are well-versed in the telecom sector.

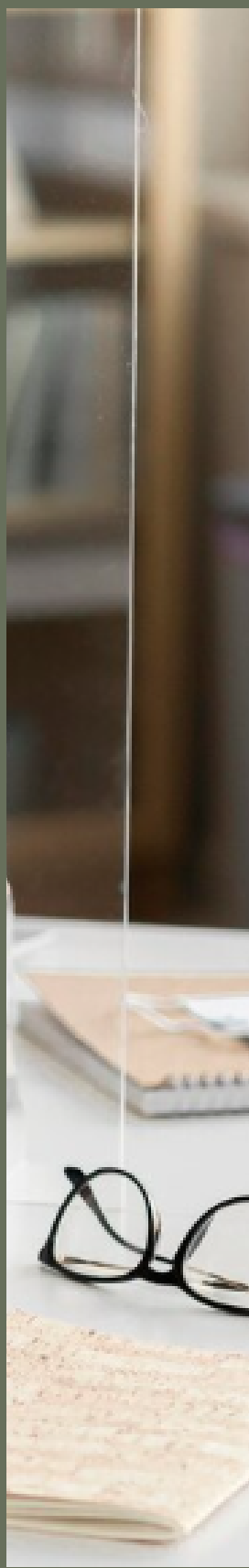
Attending conferences, seminars, and webinars dedicated to the telecommunications sector is another crucial strategy. These events typically feature industry experts and regulatory authorities who provide invaluable insights into emerging risks and regulatory developments. Furthermore, such gatherings offer opportunities for networking, allowing professionals to exchange information and stay updated on the latest industry happenings.



In the digital age, online forums and communities dedicated to telecommunications are also key sources of information. These platforms provide professionals with the opportunity to engage in discussions, share insights, and exchange information about emerging risks and regulatory changes. Moreover, keeping an eye on consultancy reports and market research is vital. Renowned consulting firms and market research companies regularly produce reports that shed light on emerging risks, regulatory trends, market developments, and cutting-edge technologies. These reports offer further valuable insights.

To stay at the forefront of developments, companies in the telecommunications industry might consider adopting advanced technology solutions, such as Generative AI models. These models can be used to plug into social media and industry blogs, recognizing patterns and aggregating data. Following relevant influencers and reputable experts on platforms can also be invaluable, as it ensures real-time access to industry updates, news articles, and analyses related to the telecommunications sector.

By employing these strategies and leveraging technological advancements, professionals and organizations can remain well-informed about the evolving telecom landscape, allowing them to adapt to emerging risks and regulatory changes effectively.



CORPORATE INCIDENT RESPONSE PLAN

CAN YOU PROVIDE AN EXAMPLE OF A SIGNIFICANT RISK EVENT OR CRISIS THAT YOUR ORGANIZATION HAS FACED, AND HOW YOU LED THE RESPONSE AND RECOVERY EFFORTS?

It would be difficult to provide an example of a significant risk event or crisis that my organization has faced due to most of these measures and protocols are proprietary information not to be shared with external parties. What I could describe though is that we have put in place our Corporate Incident Response Plan where there is a process to invoke such plan and assemble the Corporate Incident Response Team for coordination and escalation to authorities if needed. In fact, my role as Group CRO also acts as the CIRT coordinator ensuring the relevant parties have been actively engaged such that remedial actions will be collectively taken to resume/restore business activities safely and timely.

COLLABORATION

HOW DO YOU COLLABORATE WITH OTHER OPERATING UNITS OR TEAMS WITHIN THE ORGANIZATION TO ENSURE A COMPREHENSIVE AND INTEGRATED APPROACH TO RISK MANAGEMENT?

Collaborating with other operating units or teams within an organization is crucial to ensure a comprehensive and integrated approach to risk management. Steps taken to foster collaboration:

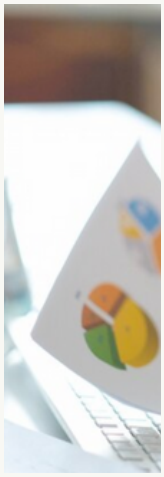
The journey begins with cultivating a shared understanding of the risk management framework and methodologies across all operating units. This involves educating team members on the significance of risk management, its inherent benefits, and how it aligns with the overarching objectives of the organization. It's equally crucial to communicate clearly the segregation of roles and responsibilities within each operating unit, outlining their specific contributions to the enterprise risk management process.

Identifying key stakeholders and operating units that are likely to be involved in or impacted by the outcomes of risk assessments is vital. These may include corporate functions such as legal, finance, operations, IT, human resources, and more. Understanding their specific roles, areas of expertise, and contributions to the enterprise risk management framework helps in effectively aligning efforts.

Creating a risk-aware culture is central to the collaborative effort. This entails promoting open communication, transparency, and a willingness to address and discuss risks openly. The concept of risk management being a shared responsibility is actively encouraged, emphasizing that everyone within the organization has a role to play in identifying, assessing, and mitigating risks.

To facilitate comprehensive risk management, the creation of cross-functional teams or working groups is essential. These teams comprise representatives from various operating units, collaborating on risk identification, assessment, and mitigation efforts. Diverse expertise and perspectives within these teams are key, especially in preparation for the launch of new services or products, ensuring that risks are thoroughly addressed.

Promoting the sharing of risk-related information and knowledge across business and corporate functions is facilitated through various means. This may include regular meetings, workshops, training sessions, and the utilization of collaborative platforms and tools to ensure that vital risk insights and data are readily accessible to relevant parties.



Embedding risk management into the core business processes, planning, budgeting, and decision-making processes is critical. This entails considering risk factors when developing policies, implementing new initiatives, or making operational changes, ensuring that risk management is intrinsically woven into the fabric of the organization's activities.

Finally, to ensure the ongoing effectiveness of the collaborative risk management approach, regular reviews and evaluations are essential. This process involves seeking feedback from corporate and control functions, identifying areas for improvement, and making necessary adjustments. An enduring commitment to a culture of continuous learning and improvement in risk management practices is encouraged.

BY FOLLOWING THE ABOVE STEPS, MY TEAM CAN PROMOTE COLLABORATION AND INTEGRATION OF RISK MANAGEMENT EFFORTS ACROSS BUSINESS AND FUNCTIONAL UNITS, LEADING TO A MORE COMPREHENSIVE AND EFFECTIVE APPROACH TO RISK MANAGEMENT WITHIN OUR ORGANIZATION.

COMMUNICATION PRESENTATION

HOW DO YOU COMMUNICATE RISK-RELATED INFORMATION TO SENIOR MANAGEMENT AND THE BOARD OF DIRECTORS TO FACILITATE INFORMED DECISION-MAKING?

The first step involves gaining a deep understanding of the senior management and board members. This includes considering their backgrounds, existing knowledge, and current priorities. Tailoring the communication to their level of comprehension and focusing on the aspects most relevant to them is fundamental.

The next phase entails identifying the most significant risks pertinent to the organization's objectives and operations. These risks must be prioritized based on their potential impact and likelihood. To provide context, it's essential to offer a concise overview of the organization's goals and strategies. This initial context helps explain how these identified risks could influence the achievement of these objectives, often reinforced through real-world case studies.

To add a quantitative dimension to risk communication, efforts should be made to quantify these risk attributes using relevant metrics, such as financial impact or probability, often presented in the form of Key Risk Indicators (KRIs) and heatmaps. This visual representation aids in enhancing the understanding of risks and facilitates comparison and prioritization. In parallel, it's crucial to articulate the potential impact of each risk attribute on the organization's strategic objectives, financial performance, and reputation. This is achieved through a combination of qualitative and quantitative information that effectively conveys the significance of each risk.

In the subsequent phase, the focus shifts to providing concrete risk mitigation strategies and recommendations for each identified risk. These recommendations present actionable steps that can be taken to promptly and effectively reduce these risks, including alternative options such as risk hedging and their associated costs and benefits. Additionally, it is important to highlight the interdependencies and correlations between different risk attributes, demonstrating how they can amplify or offset each other. This broader perspective allows senior management and the board to understand potential cascading effects.

STRATEGIES FOR EFFECTIVE RISK COMMUNICATION WITH SENIOR MANAGEMENT AND THE BOARD

Finally, in order to foster an environment of open communication, senior management and board members are encouraged to ask questions and seek clarifications. The readiness to provide additional information or thematic analysis as needed ensures that the communication remains adaptable and responsive to the specific needs and preferences of the audience. By following these steps, risk communication becomes a powerful tool to empower decision-makers to take informed and actionable steps in managing risks effectively.

Effective communication of risk requires a balance between providing sufficient information and avoiding overwhelming the audience in terms of technicality. Tailor approach to the specific needs and preferences of senior management and the board and be prepared to adjust the communication style where necessary.

ASIA
CEO
COMMUNITY

KEY PERFORMANCE INDICATORS

WHAT METRICS OR KEY PERFORMANCE INDICATORS (KPIS) DO YOU TRACK TO MONITOR THE EFFECTIVENESS OF YOUR RISK MANAGEMENT STRATEGIES?

Effectively tracking and monitoring the performance of risk management strategies is a critical component of ensuring an organization's resilience and success. To accomplish this, organizations utilize a range of metrics and Key Performance Indicators (KPIs) that provide valuable insights into the effectiveness of their risk management efforts. These metrics help measure, evaluate, and optimize risk management endeavors in a structured manner.

One essential aspect of this process is measuring the overall level of residual risk exposure and its potential impact on an organization's objectives. This involves employing metrics such as quantifying risk exposure value, risk rating qualification, and assessing alignment with risk appetite.

Furthermore, organizations need to assess the effectiveness of risk mitigation measures and controls in reducing the likelihood or impact of potential risks. Metrics like the risk mitigation ratio and control effectiveness index play a pivotal role in gauging the efficiency of these measures.

In addition to these internal metrics, it is crucial to identify and monitor leading indicators, which provide early warnings of potential risks. These indicators are often tailored to reflect the organization's unique risk profile, ensuring that they are relevant and accurate.

To gauge the effectiveness of risk management strategies, organizations must also measure the frequency and impact of risk events. This involves quantifying the number of risk events, evaluating their severity, and calculating the associated costs or losses. Analyzing trends in these metrics helps pinpoint areas where risk management strategies may require refinement.

An equally vital aspect is measuring the time taken to respond to identified risks. This metric evaluates an organization's ability to detect and respond promptly, enhancing its risk management capabilities. Metrics such as the average time to respond or to implement risk mitigation measures offer valuable insights into remediation times.

Assessing
Risk Management Effectiveness

Moreover, understanding an organization's risk culture and the level of awareness among employees regarding risk management practices is key. Workshops and training sessions help assess the overall understanding of risk management principles, adherence to policies, and the perception of risk within the organization.

Lastly, to gain insight into the financial impact of risks on the organization, it is essential to measure the cost of risk events, including expenses such as insurance premiums and risk transfer costs. By comparing these costs over time, organizations can effectively evaluate the impact of their risk management efforts.

In this holistic approach to risk management, organizations tailor the selection of specific risk metrics and KPIs to their unique context, encompassing industry sector, risk profile, and business objectives. Regular reviews and updates of these metrics ensure their continued relevance and effectiveness, particularly in the ever-evolving landscape of risks and business strategies. This ongoing evaluation empowers organizations to adapt their risk management strategies efficiently and proactively, ultimately enhancing their ability to navigate a complex risk environment.

WHAT DO YOU SEE AS THE BIGGEST CHALLENGES AND OPPORTUNITIES IN RISK MANAGEMENT WITHIN THE TELECOMMUNICATIONS INDUSTRY IN THE NEAR FUTURE?

The telecommunication industry continues to face several challenges and opportunities in risk management in the near future.

In this dynamic industry, one significant challenge is the escalating cybersecurity threats. The sector faces an ever-growing menace as it becomes increasingly digitally interconnected. This necessitates a continuous enhancement of security measures to safeguard sensitive data, networks, and customer information from any attempted attacks.

Moreover, the rapid evolution of technologies such as 5G, the Internet of Things (IoT), cloud computing, and the adoption of generative AI presents a dual-edged sword. These advances offer exciting opportunities, but they also usher in new challenges. Risk management must keep pace with these innovations to address potential risks like data breaches, privacy concerns, and operational disruptions.

CHALLENGES

In addition, the telecommunications industry is subject to numerous regulatory requirements, such as data protection, privacy, and network security regulations. Compliance with these regulations can be complex and challenging as their scope and level of sophistication may vary over time. Some older regulations may not be in sync with newer and more updated ones when there are overlaps in certain subject matter such as privacy. Organizations will need to stay updated in recognizing changes in the regulatory landscape while ensuring effective risk management practices are place to meet expanded regulatory obligations

Last, but not least, the global nature of the telecommunications industry involves intricate supply chains, sourcing equipment and components from a web of suppliers and vendors. Managing supply chain risks, such as disruptions, sanctions, quality control, and dependencies on critical suppliers, is essential to maintain seamless operations and service delivery.

However, amidst these challenges, there are opportunities. With vast volumes of data at its disposal, the telecom sector can leverage advanced analytics and artificial intelligence (AI) to extract valuable insights, recognize patterns, and proactively identify and mitigate risks. These technologies offer enhancements in risk assessment, fraud detection, and operational efficiency.

Telecommunication companies also have the opportunity to diversify their business models beyond traditional services, venturing into new domains like IoT, cloud services, product innovations, or digital platforms. Risk management plays a pivotal role in assessing and managing the associated risks, fostering innovation.

Collaborative efforts and partnerships within the industry hold the potential to strengthen risk management practices. Sharing best practices, threat intelligence, and insights about emerging risks can fortify risk mitigation capabilities and bolster the resilience of the entire telecommunications ecosystem.

Moreover, integrating risk management strategies into customer experience initiatives is a powerful way for telecom companies to build trust and loyalty. This involves ensuring data privacy, transparent communication about security measures, and prompt handling and resolution of customer concerns.

The telecommunication industry is dynamic and constantly evolving. Adapting risk management practices to address these challenges and seize opportunities is essential for organizations to thrive in the years to come.

COME AND JOIN US

FEEL FREE TO CONTACT

ceo@asiaceo.club

Lemmi Centre, unit 1703, 17/F, No. 50 Hoi Yuen Rd, Kwun Tong, Hong Kong

www.asiaceo.club

+ 852 3590 3939