Middle East

Point of View

Published by Deloitte & Touche (M.E.) and distributed to thought leaders across the region | Fall 2023

Securing the future

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

Fall 2023
Middle East Point of View
Published by Deloitte & Touche (M.E.)

www.deloitte.com/middleeast

A word from the editorial team

Mahatma Gandhi once said, "The future depends on what you do in the present." This simple yet powerful idea highlights how each small step, whether personal or business-related, shapes the future we aim for. In the ever-changing business world, our decisions today have a ripple effect for years to come.

Securing the future requires strategic thinking and a visionary approach embracing innovation, adaptability, and sustainability. Successful enterprises advance with a forward-looking mindset in a rapidly evolving technological era. It's not just about bytes and algorithms; it's about building a foundation that withstands the test of time. Sustainable practices are not just buzzwords but the basis for resilient nations and businesses.

As we all know by now, climate change is a threat to the health of our planet and our collective future. Seeking to tackle this global challenge, thousands will be gathering in December 2023 for COP28 in the UAE. In the article *COP28: Transparency drives sustainability reporting,* Damian Regan weighs in on how "while the primary focus of the COP will be global climate change and key reporting of GHG emissions at a country level, many conference attendees will recognize the sentiment of transparency as being relevant also at a corporate level and to a wider range of ESG related topics and metrics."

The convergence of initiatives like COP28 and electric vehicles (EVs) underscores the integral role the Middle East plays in securing a sustainable future. This shift not only aligns with global environmental goals but also positions the region as a leader in clean energy adoption. In Dr. Ahmed Hezzah's article, *The Middle East goes electric!*, he states that "the global automotive sector is on the brink of a seismic shift, with electric vehicles (EVs) leading the way as the most promising contender in the pursuit of sustainable transportation." He discusses how as the world aspires for a greener future - the Middle East region continues to make one stride after another.

As businesses expand within their respective markets, their dependence on service organizations for supporting their expanding operations intensifies. In *The power of third-party assurance reporting in today's world*, Bhavna Lakhani, Fadi Ghawi, and Mais Barouqa explain how "Amid global megatrends and a connected financial landscape, organizations increasingly rely on third-party vendors for critical services." This heightened reliance raises critical concerns regarding the topic of security and integrity of the data managed, as is also touched upon in *Consumer privacy: A business imperative in the digital age* by Ikram Moulila.

WhatsApp watch: Are financial institutions under fire? by Collin Keeney, Natalie Forester, and Faiz Ali Khan follows the same wave by putting the spotlight on off-channel communications: the use of unapproved applications on mobile devices to participate in communications concerning a firm's business. Data governance, the use of corporate devices versus bring-your-own-device (BYOD), and compliance with data protection and privacy laws become key pieces to the puzzle, hopefully securing the future of business.

In today's fast-changing digital world, data centers are crucial for organizations, serving as key drivers for operations and innovation. Beyond just operations, understanding the financial side of data center services is increasingly important. This knowledge influences financial reporting, strategic planning, and investment choices, helping businesses align their strategies with long-term goals, explains Zeeshan Abbasi in *Navigating the financial labyrinth of data center colocation and capacity services*.

Striving to secure one's future takes consistent effort. In *AI in cybersecurity: A double-edged sword*, Tamer Charife and Michael Mossad explain how striking the right balance between reaping AI's benefits in cybersecurity and mitigating its risks isn't a one-time effort but rather a continuous journey that requires constant education, heightened awareness, and an unwavering commitment to navigate the ever-evolving landscape of AI in cybersecurity responsibly and effectively.

As we set our sights on securing the future, let us not forget the lessons of the past. Securing the future is not a singular act but an ongoing journey. It's about marrying the wisdom of experience with the audacity of innovation. We hope you enjoy reading this issue of the Middle East Point of View.

The ME PoV editorial team

Contents

The Middle East goes electric!

The global automotive sector is on the brink of a seismic shift, with electric vehicles (EVs) leading the way as the most promising contender in the pursuit of sustainable transportation. As the world races towards a greener future, the Middle East, often associated with its oil-rich heritage, is making one stride after another in adopting EVs.

This article sheds light on the dynamic Middle Eastern EV market, with a particular focus on the role of customer experience in shaping its current trajectory and future potential.

Understanding Middle Eastern consumer preferences

Consumers

The Middle East is a diverse region with a rich tapestry of cultures and social dynamics. This diversity shapes consumer preferences, thus automakers must carefully navigate this intricate landscape to understand what people want in EVs. Market research shows that Middle Eastern consumers are drawn to EVs that are futuristic looking, mechanically advanced, and filled to the brim with digital innovations.

A large portion of consumers in the region have always shown an affinity towards sophistication in their vehicles. As a result, automakers are investing in blending cutting-edge technology with exquisite craftsmanship to create EVs that appeal to this discerning clientele. These vehicles feature luxurious interior comforts, high-quality materials, and state-of-the-art infotainment systems that are all seamlessly integrated to deliver an immersive driving experience.

Preferences

A recent survey conducted by Deloitte found that 220 local participants, who are all potential EV buyers and owners, consider price and product quality to be the most important factors when purchasing an EV. Participants also prefer to make their own decisions and educate themselves about EVs through various channels such as social media. They are more likely to buy from a brand they are familiar with and prefer to own the car outright rather than lease it.

Most of the participants value in-person showroom visits and test drives, and are motivated to buy an EV for reasons such as reduced maintenance, technological innovations, improved performance, and overall cost-saving improved technology. They prefer to pay with cash and want home charging stations as well. Increased range and faster charging are also important factors, as are rental models and priority customer service. Finally, participants are forward thinking and consider resale value when making an EV purchase decision.

Market

The EV market in the Middle East is expected to witness massive growth in the coming years. It is projected to reach US$7.65 billion by 2028, up from US$2.7 billion in 2023.[1] This surge is being driven by a number of factors, including government initiatives to promote the use of electric vehicles, increased awareness of energy storage solutions, the expansion of 5G telecommunications networks, and the implementation of Vision documents in Saudi Arabia, the United Arab Emirates, Qatar, and Kuwait.

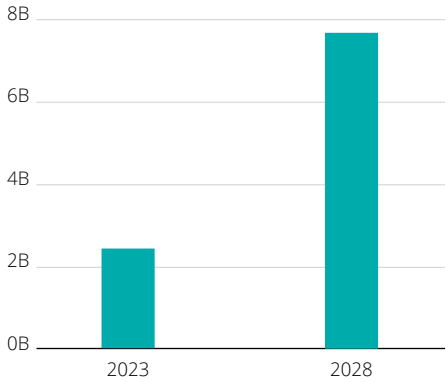


Figure 1: Middle East electric vehicle market (market size is US$ billion)

Joint ventures for the win

Some of the world's most renowned EV manufacturers have already established their presence in the region and are now competing head-to-head for market domination. Brands such as Volkswagen, Nissan, Hyundai, BMW, and Tesla are some of the most popular among local consumers.[2] But new players are progressively venturing into the region and expanding their horizons by forming partnerships with local organizations. Some recent examples include:

- Chinese EV maker NIO has secured a US$1.1 billion investment from Abu Dhabi investment firm CYVN Holdings to "strengthen its balance sheet and support business growth."[3]
- Saudi Arabia's Ministry of Investment has entered into a US$5.6 billion partnership with Chinese EV startup Human Horizons to develop, manufacture, and sell electric vehicles.[4]
- Saudi Transport General Authority (TGA) recently announced that Lucid electric cars are now available for rent to residents and tourists in the country. This move is part of the country's efforts to adopt clean energy and preserve the environment.[5]
- Lucid Group, backed by the Public Investment Fund (PIF), announced in September 2023 it had opened its first international manufacturing plant in Saudi Arabia's Jeddah city under a deal designed to further the Middle Eastern country's electrification push, and an agreement with the Kingdom to buy up to 100,000 vehicles from the company over 10 years.[6]

Overcoming barriers

Range anxiety

Range anxiety stands as a major obstacle to the adoption of EVs around the world. This is especially true in the Middle East where the vast desert landscapes can make it difficult to find charging stations. However, there are a number of ways to mitigate range anxiety, including the ongoing development of advanced battery technologies that offer longer ranges and faster charging times, as well as the implementation of an EV infrastructure strategy.

Charging infrastructure

A robust charging infrastructure is essential for the widespread use of EVs. In the Middle East, governments are actively working to create a network of charging stations that will make EVs more accessible and convenient for drivers. For example, by 2025, both the Saudi Electric Vehicle Charging Infrastructure Development Initiative (SEVCIDI) and the Dubai Electricity and Water Authority (DEWA) are planning to have installed 50,000[7] and 1,000[8] charging stations in Saudi Arabia and Dubai respectively. Not only does this effort promote practicality, but it also demonstrates the region's commitment to sustainability.

Weather conditions

The extreme temperatures in the Middle East pose a challenge for EVs which may struggle to maintain optimal performance in hot weather. According to a 2019 study by the American Automobile Association, EVs could lose up to 17% of their driving range in temperatures above 35°C.[9] EV manufacturers are tailoring vehicle components to not only withstand but thrive in these conditions. Battery cooling systems are being meticulously optimized to combat the searing heat and ensure consistent performance and prolonged lifespan.

Promoting a green community

In the Middle East, governments, businesses, and communities are working together to promote sustainable practices, such as the adoption of EVs. They are offering incentives such as tax breaks, toll waivers, and preferential parking to help make EVs more affordable and convenient, eventually leading to a wider adoption rate among the population. The United Arab Emirates Ministry of Energy and Infrastructure (MoEI) has announced that it plans to have 50% of all cars on UAE roads electric by 2050. This ambitious prospect is supported by Dubai's own goal to have 42,000 EVs on its roads by 2030,[10] which is roughly six times the number of EVs currently in use in the Emirates.[11]

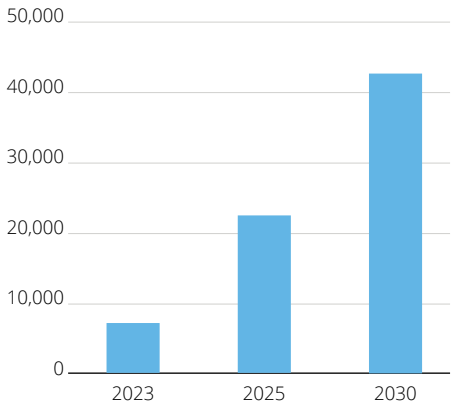


Figure 2: Number of electric vehicles in Dubai

To encourage people to choose EVs over conventional vehicles, manufacturers need to highlight the environmental benefits of EVs. EVs produce zero emissions, which can help to reduce air pollution and improve air quality. They also use less energy than gasoline-powered cars, which can help to reduce greenhouse gas emissions and combat climate change. This is in line with the global shift towards EVs, as people are increasingly aware of the need to "go green" and support the universal goal of net-zero emissions by 2050, as well as limit global warming to no more than 1.5°C, as mentioned in the United Nations' Paris Agreement.[12]

The Middle East is looking to redefine transportation in the 21st century by harmonizing luxury, technology, and environmental consciousness. Automakers are adapting to changing consumer preferences by offering more luxurious, technologically advanced, and environmentally friendly vehicles. Governments, businesses, and consumers are all working in tandem to create a more sustainable tomorrow, powered by electric vehicles. As governments provide incentives, businesses develop new technologies, and consumers embrace change, the Middle East is moving towards a future where sustainable mobility is a reality.

By **Dr. Ahmed Hezzah**, Director, Consumer and Commerce, Consulting, Deloitte Middle East

Endnotes

1. Mordor Intelligence, (2023) Middle East Electric Vehicle Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028). Available at: https://www.mordorintelligence.com/industry-reports/middle-east-and-africa-automotive-electric-vehicle-market.
2. Mordor Intelligence, (2023) Middle East and Africa Automotive Electric Vehicle Market Share. Available at: https://www.mordorintelligence.com/industry-reports/middle-east-and-africa-automotive-electric-vehicle-market/market-share.
3. CnEVPost, (2023) NIO secures $1.1 billion investment from Abu Dhabi fund. Available at:https:// cnevpost.com/2023/06/20/nio-secures-1-1-billion-investment-from-abu-dhabi-fund/.
4. CNBC, (2023) Saudi Arabia signs $5.6 billion deal with Chinese parent of high-end EV brand HiPhi. Available at: https://www.cnbc.com/amp/2023/06/12/saudi-arabia-signs-5point6-billion-deal-with-chinese-parent-of-hiphi.html.
5. Al Arabiya News, (2023) Saudi transport authority brings Lucid EVs to car rental offices. Available at: https://english.alarabiya.net/News/saudi-arabia/2023/07/19/-Saudi-transport-authority-brings-Lucid-EVs-to-car-rental-offices.
6. Reuters, (2023) Lucid opens first international EV factory in Saudi Arabia. Available at: https://www.reuters.com/business/autos-transportation/lucid-opens-first-international-ev-factory-saudi-arabia-2023-09-27/.
7. CNBC, (2023) How the Middle East is Preparing for the Post-Oil, EV Era of Transportation. Available at: https://www.cnbc.com/2023/07/20/how-the-mideast-is-preparing-for-post-oil-ev-era-of-transportation.html.
8. Construction Week, (2023) Dubai to Build 1,000 New Electric Vehicle Charging Stations. Available at: https://www.constructionweekonline.com/projects-tenders/dubai-to-build-1000-new-electric-vehicle-charging-stations.
9. AAA, (2022) AAA Study: What's the Real Range of Electric Vehicles? Available at:https://info.oregon.aaa.com/aaa-study-whats-the-real-range-of-electric-vehicles.
10. Zawya, (2023) Range Anxiety, Accessibility Pose Concerns for EV Adoption in the UAE. Available at: https://www.zawya.com/en/business/energy/range-anxiety-accessibility-pose-concerns-for-ev-adoption-in-the-uae-mxquy5em.
11. International Trade Administration, (2023) United Arab Emirates Electric Vehicle Market. Available at: https://www.trade.gov/market-intelligence/united-arab-emirates-electric-vehicle-market.
12. Middle East Institute, (2022) The Environmental Cost of Electric Vehicles. Available at:https://www.mei.edu/publications/environmental-cost-electric-vehicles.

AI in cybersecurity: A double-edged sword


AI
27 NHT KLPOLK 789n TYd6
UYe6 OQA09 WQhnS61
61 DREb UTr450 Nlk4
QANh 9754K RFdpc ITr7
82AS QMjh 0341H KmsP 62CVT
0 11 0010
0 11 0 1
10 1001 01010110
1 0
10
0 11 0010

In an era where the digital landscape evolves at breakneck speed, the quest for security has taken centre stage. The interconnectedness of our modern world has opened unprecedented opportunities for innovation and communication, but it has also exposed us to a growing array of cyber threats. As businesses and individuals rely more than ever on digital technologies, the vital role of cybersecurity cannot be emphasized enough.

The digital frontier

Imagine a world where our every move, our every thought, lives in the digital realm. Our thoughts are shared openly on social media platforms, capturing our emotions, ideas, and opinions for the world to see. Our physical presence is captured through check-ins, travel updates, and real-time location sharing, creating a digital trail of our journeys. In this interconnected landscape, the line between the logical and physical worlds blurs into our identity, seamlessly merging our digital persona with our real-life experiences. It's a frontier where security battles exploitation, defining our digital era.

AI's role in the battle

Enter artificial intelligence (AI), a technological marvel that has promised to revolutionize cybersecurity. With its ability to process vast amounts of data, recognize patterns, and make split-second decisions, AI offers the potential to bolster our digital defences. But, like any powerful tool, AI can be a double-edged sword. It holds the key both to fortifying our security and to unleashing new forms of cyber threats.

Overview of the journey

In this article, we embark on a journey through the paradoxical realm of AI in cybersecurity. We'll begin by exploring the promises AI holds, from supercharging threat detection to automating security tasks. But stay with us as we venture deeper, for the path of AI in cybersecurity is not without its shadows. We'll uncover the darker side of AI, where it empowers cybercriminals, raises ethical dilemmas, and challenges the regulatory landscape. As we navigate these dualities, one thing will become clear: AI in cybersecurity is a potent force, capable of both safeguarding and endangering our digital world.

The promise of AI in cybersecurity

In an ever-evolving digital landscape where cyber threats are a constant presence, AI stands as a beacon of hope for bolstering our defences. This section explores the potential benefits of AI in the realm of cybersecurity, shedding light on how this powerful technology can transform our approach to digital protection.

Improved threat detection and response times

At the forefront of AI's contribution to cybersecurity lies its unparalleled capacity for threat detection and rapid response. Unlike rule-based systems that struggle to keep pace with the evolving tactics of cybercriminals, AI employs machine learning algorithms to analyze vast datasets in real-time. It excels at identifying anomalies and potential threats, allowing for lightning-fast detection and swift, proactive responses. This capability is critical in preventing data breaches and minimizing the impact of cyberattacks.

69%

of enterprises believe AI is necessary for cybersecurity due to increasing number of threats that cybersecurity analysts can handle.[1]

15%

average decrease in the median dwell time - the time between an attacker accessing their victim's systems and the attack being detected or executed.[2]

Enhanced automation for routine security tasks

AI-powered cybersecurity solutions offer a significant advantage by automating routine security tasks that once demanded substantial human effort. Activities such as continuous monitoring of network traffic, identifying vulnerabilities, and applying security patches can be handled efficiently by AI-driven tools. This not only reduces the workload on cybersecurity teams but also minimizes the risk of human error in these repetitive processes.

Scalability and adaptability

In the face of ever-evolving cyber threats, scalability and adaptability are paramount. AI-driven security systems exhibit the ability to effortlessly scale to handle increasing data volumes and a growing number of connected devices. Moreover, they possess the inherent capability to adapt and learn from new threat patterns, continuously improving their ability to safeguard digital environments. This adaptability is essential in an environment where cyber threats continually mutate and evolve.

A real-life example

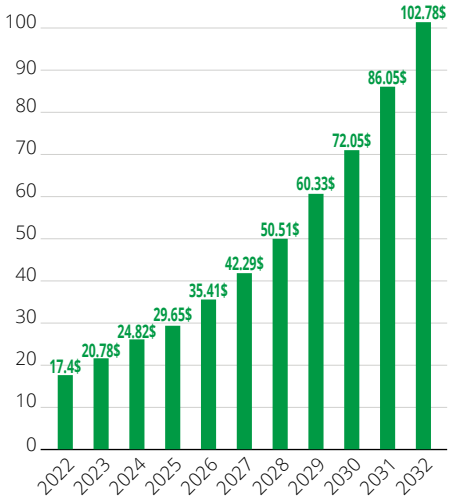
One particular case study exhibited how a leading technology company helped a global industrial supplier deploy an integrated set of managed security services that use AI to provide 100% visibility and the ability to process millions of events per day.[3]

The industrial supplier faced challenges such as increasing complexity and sophistication of cyber threats, lack of visibility and control over its global IT infrastructure, high cost and effort of managing multiple security tools and vendors, and limited availability and expertise of security analysts. The technology company helped the industrial supplier implement a comprehensive security solution that covered security monitoring and analytics, security orchestration and automation, security testing and optimization, and security services for cloud.

The solution used cognitive computing to augment human intelligence and automate the analysis of security incidents, AI to orchestrate and automate incident response actions, continuous testing and optimization of the security posture, and cloud security services. The benefits of the AI-based security solution for the industrial supplier included improved detection and prevention of cyberattacks, reduced time to respond and remediate incidents, enhanced visibility and control over the IT infrastructure, optimized security operations and reduced costs, and increased efficiency and productivity of security analysts.

This case study demonstrates how AI can help improve cybersecurity by enhancing automation for routine security tasks, improving threat detection and response times, and reducing human errors and biases.

The benefits are evident in the forecasts of the global AI in cybersecurity market size,[4] which was evaluated at US$17.4 billion in 2022 and is expected to hit around US$102.78 billion by 2032, growing at a CAGR of 19.43% between 2023 and 2032.



Source: www.precedenceresearch.com

Figure 1: Artificial intelligence (AI) in cybersecurity market size, 2022 to 2032 (US$ billion)

AI-powered threats: The dark side

While AI holds the promise of fortifying our digital defences, it also presents a dark and ominous facet. In this section, we venture into the shadowy realm of AI-powered cyber threats, where technology originally designed to protect can be turned into a potent weapon by malicious actors.

The emergence of AI-driven cyber threats

The rapid advancement of AI technology has given rise to a new breed of cyber threats. Attackers now harness the power of AI to craft more sophisticated and evasive attacks. AI-driven malware, for instance, can adapt to the target environment, making it exceptionally difficult to detect and mitigate. Similarly, AI can be employed in social engineering attacks, where it generates convincing phishing messages tailored to exploit individual vulnerabilities leveraging a new technique referred to as "deepfake."

AI in action

These threats are not theoretical; they have materialized in various forms, highlighting the potency of AI in the hands of malicious actors.

- Earlier this year, hackers used AI to bypass Bitfinex's biometric authentication system, which required users to verify their identity with their face and voice. The hackers injected fake video streams into the verification process, fooling the system into thinking that they were the legitimate users. The hackers also used deepfake technology to create realistic facial images that matched the voice and behavior of the victims. The hackers stole US$150 million worth of various digital assets, including Bitcoin, Ethereum, and Tether.[5]
- In 2021, a cyber espionage campaign dubbed Operation Diànxùn was uncovered by researchers from McAfee.[6] The campaign used AI to create phishing emails that targeted telecommunications companies around the world. The emails used natural language generation to craft convincing messages that appeared to come from legitimate sources, such as job recruiters or industry experts. The emails contained malicious attachments or links that delivered malware to the victims' devices.
- In 2020, a cryptocurrency platform was targeted by a voice-spoofing attack that used AI to impersonate the CEO's voice and tricked an employee into transferring US$243,000 to a fraudulent account.[7]

These examples underscore the alarming reality of AI-driven threats. As we delve into the statistics that illuminate the prevalence of such attacks, it becomes evident that these incidents are not isolated; they represent a growing trend in the world of cybersecurity.

According to a report from Webroot, more than 90% of cybersecurity professionals are concerned that hackers will use AI in cyberattacks against their company that are more sophisticated and harder to detect. Similarly, a survey by CyberArk found that 93% of cybersecurity professionals expect AI-enabled threats to impact their organization. Finally, based on research conducted by Checkpoint,[8] the average weekly cyberattacks per organization by region shows a significant increase across all regions in 2022 compared to 2021 thanks to generative AI models.

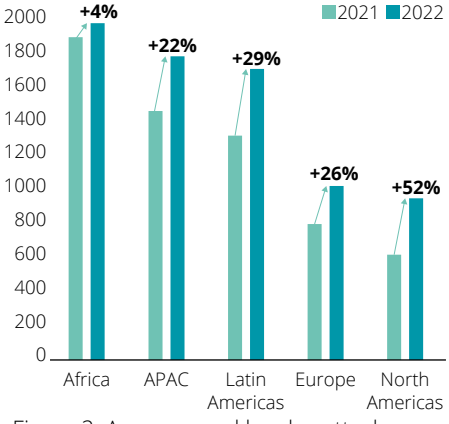


Figure 2: Average weekly cyberattacks per organization per region

These statistics highlight the growing concern within the cybersecurity community about the potential for AI-powered threats.

The regulatory landscape

The regulatory landscape surrounding AI in cybersecurity is a critical aspect of ensuring responsible and secure AI implementation.

Examination of current regulations

Governments and regulatory bodies worldwide are increasingly recognizing the need to establish guidelines and regulations for AI in cybersecurity. These regulations aim to address the ethical, privacy, and security concerns associated with AI technologies. The field of AI regulation is still evolving globally; therefore, businesses should respond proactively to AI regulations by developing a robust AI governance program that informs the AI lifecycle.

In recent years, several countries and regions have issued or proposed AI-related laws and regulations covering various aspects such as data protection, human rights, accountability, transparency, and safety. Some of the notable examples are:

- The EU's Artificial Intelligence Act, which is a comprehensive legislative proposal that aims to create a harmonized legal framework for AI in the EU. The proposal defines four categories of AI systems based on their risk level and sets out different requirements and obligations for each category. The proposal also establishes a European Artificial Intelligence Board to oversee the implementation and enforcement of the rules.
- The US's National Artificial Intelligence Initiative Act, which is a law that establishes a coordinated federal initiative to accelerate AI research and development, promote public-private partnerships, foster education and workforce development, and ensure ethical and trustworthy AI. The law also creates a National Artificial Intelligence Advisory Committee to provide advice and recommendations to the federal government.

From the perspective of the Middle East, Saudi Arabia has specific regulations and policies related to AI. The Saudi Data and Artificial Intelligence Authority (SDAIA) is responsible for the country's AI regulations. The SDAIA has created a data governance framework at the national level that outlines the laws and regulations for national data management and governance, as well as the protection of personal data. This framework includes:

- Data Management and Personal Data Protection Regulations and Standards
- National Data Governance Policies
- Data Classification Policy and Regulations
- Personal Data Protection Law and The Implementing Regulation
- Data Sharing Policy and Regulations

In addition to this, the Saudi Food & Drug Authority has published guidance on AI and 'Big Data' in the context of medical devices. These regulations aim to ensure that AI is used responsibly and ethically, while also promoting innovation and growth in the field.

While in the United Arab Emirates (UAE) regulators and organizations, such as the UAE's Ministry of AI and Smart Dubai, have taken a soft approach to regulation, mostly in the form of non-binding guidelines. These guidelines are intended to foster the development and uptake of AI in an ethical, transparent, and responsible manner while minimizing pitfalls such as discrimination and algorithmic bias.

Industry standards and compliance

Government regulations are not the only factors influencing the role of AI in cybersecurity. Industry-specific standards and compliance frameworks are equally crucial. These guidelines, which organizations follow to ensure their AI systems align with industry best practices, are continually evolving. For instance, the NIST AI Risk Management Framework (AI RMF), launched on 26 January, 2023, is a key standard in this domain. This framework, developed through public-private collaboration, is designed to enhance trustworthiness in the design, development, use, and evaluation of AI products and services.

In the same vein, the ISO/IEC AWI 27090 is another significant standard under development that addresses security threats and failures in AI systems. It aims to equip organizations with a better understanding of the implications of security threats to AI systems throughout their lifecycle and offers strategies for detecting and mitigating such threats.

As the integration of AI in cybersecurity becomes more prevalent, experts across the field emphasize the pressing need for robust, enforceable policies. Many argue for the establishment of stringent laws and regulations to govern the ethical and secure usage of AI. Striking the delicate balance between fostering innovation and implementing necessary regulations stands as a pivotal challenge as we advance into an increasingly digital future.

Striking the right balance: Mitigating risks

Striking the right balance in the use of AI in cybersecurity is a formidable task, akin to walking a tightrope. On one side, we have the transformative potential of AI, which promises to revolutionize cybersecurity with unprecedented levels of protection and resilience. On the other side, we face the risks of misuse and unintended consequences, which could amplify existing threats or create new vulnerabilities.

Navigating this delicate equilibrium demands a proactive and dynamic approach. Organizations need to stay abreast of the latest advancements in AI and continually assess and address the evolving landscape of risks associated with its use. It's about making informed decisions, leveraging AI's strengths to enhance cybersecurity defences while taking calculated measures to minimize its potential pitfalls.

However, adopting AI in cybersecurity is not just about harnessing its power; it's about doing so responsibly and judiciously. This is where continuous education and awareness come into play. As AI continues to evolve at a rapid pace, so too does the complexity of the risks associated with its use in cybersecurity. This dynamic landscape necessitates a commitment to ongoing learning and awareness at all levels of an organization.

Continuous education empowers individuals and organizations to stay ahead of the curve, equipping them with the knowledge and skills to leverage AI effectively and safely. It fosters a culture of vigilance, where potential risks are identified and mitigated proactively rather than reactively. Moreover, awareness plays a crucial role in ensuring that all stakeholders understand the implications of AI in cybersecurity. It promotes informed decision-making and encourages responsible use of AI.

In essence, striking the right balance between reaping AI's benefits in cybersecurity and mitigating its risks isn't a one-time effort. It's a continuous journey that requires constant education, heightened awareness, and an unwavering commitment to navigate the ever-evolving landscape of AI in cybersecurity responsibly and effectively.

Concrete steps to be taken include: Firstly, defining a controls framework is crucial. This involves establishing a comprehensive set of policies, standards, guidelines, and best practices that govern the development, deployment, and use of AI systems within an organization. It sets the foundation for responsible and secure AI usage.

Secondly, developing a defensible security architecture is key. This means designing and implementing a robust and resilient architecture capable of protecting AI systems from both internal and external threats. It's about building fortifications around AI assets.

Thirdly, implementing tailored security solutions for AI can provide an added layer of protection. Specialized tools and platforms specifically crafted for testing, validating, monitoring, and moderating AI solutions can help ensure their integrity and reliability.

Lastly, bolstering defense by harnessing AI threat intelligence is essential. With the emergence of new AI-specific cyber threats, adopting a proactive and holistic approach to secure AI systems and applications becomes paramount. It's about staying one step ahead of potential threats.

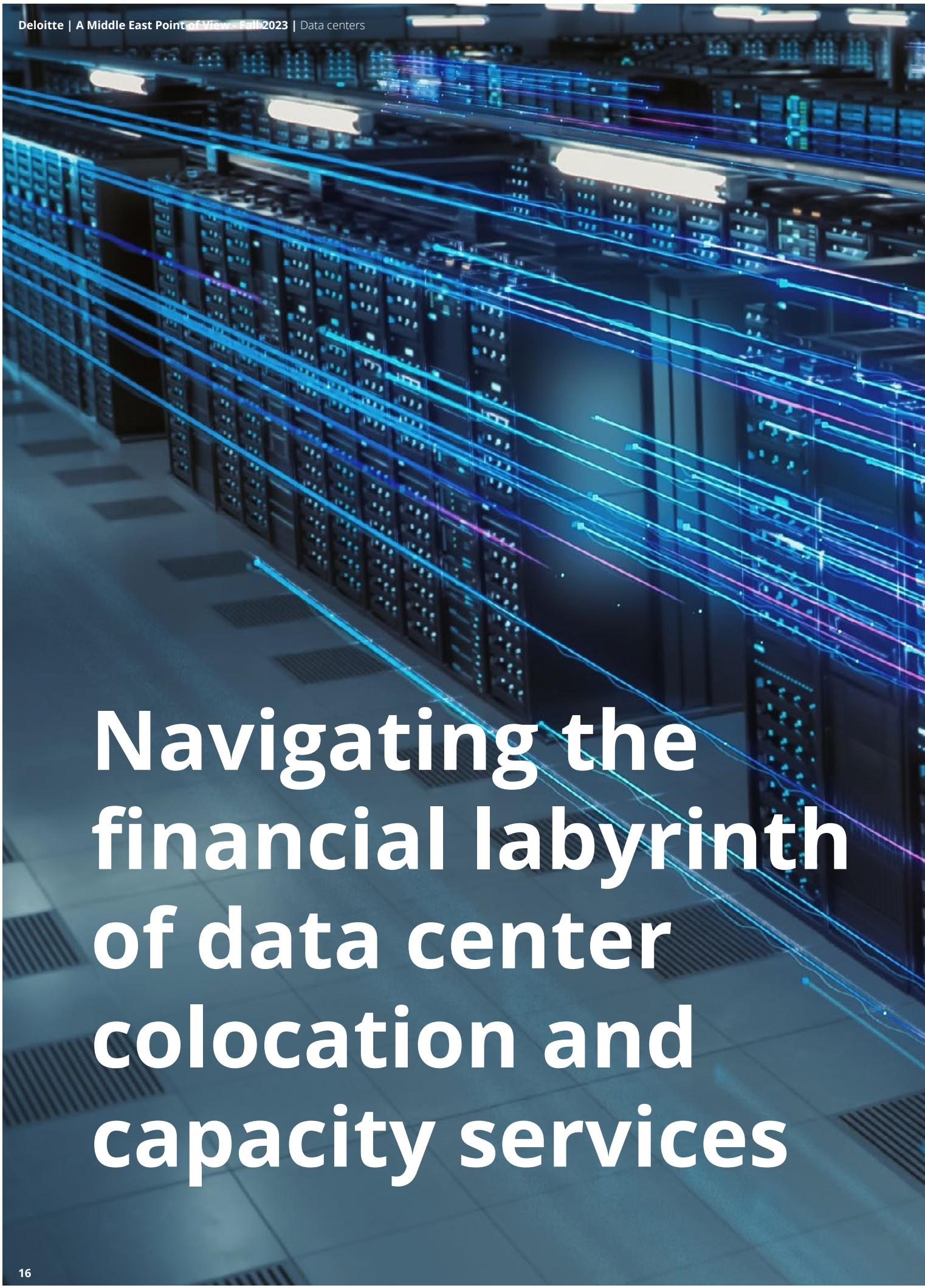
In conclusion, securing AI in cybersecurity is a multifaceted challenge that requires a strategic blend of policy-making, architectural design, specialized solutions, and threat intelligence. It's a journey that demands continuous effort, vigilance, and adaptation.

By **Tamer Charife**, Cyber Emerging Technologies Leader, Cyber Risk Services and **Michael Mossad**, Cyber Emerging Technologies Director, Deloitte Middle East

As AI continues to evolve at a rapid pace, so too does the complexity of the risks associated with its use in cybersecurity. This dynamic landscape necessitates a commitment to ongoing learning and awareness at all levels of an organization.

Endnotes

1. https://zipdo.co/statistics/ai-use-in-cyber-security/.
2. https://securityintelligence.com/news/global-median-dwell-time-drops-to-record-low/.
3. https://www.ibm.com/case-studies/andritz.
4. Artificial Intelligence (AI) Market Size, Growth, Report By 2032 (precedenceresearch.com).
5. Bitfinex Owner Offers $150M Buyback to Bitcoin (BTC) Hack Victims - Bloomberg.
6. https://blog.avast.com/deepfake-voice-fraud-causes-243k-scam.
7. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-dianxun-cyberespionage-campaign-targeting-telecommunication-companies/.
8. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks - Check Point Blog.



Navigating the financial labyrinth of data center colocation and capacity services

In the rapidly evolving digital landscape, data centers have emerged as technological linchpins, with organizations increasingly relying on these powerhouses to drive operations and innovation. Yet, it's not just the operational aspects that demand attention; delving into the financial intricacies associated with data center services is becoming equally crucial. Such insights play a pivotal role in shaping financial reporting, strategic planning, and investment decisions, ensuring that businesses align their strategies with fiscal prudence and long-term objectives. Within this dynamic arena, two distinctive models of data center services have carved niches for themselves: data center colocation services and avant-garde data center capacity services.

Switching lanes: Transitioning from colocation to data center capacity for future-proof infrastructure

Data center colocation services: A tangible asset approach

Data center colocation typically offers clients control over dedicated floor space, where they can house their hardware, servers, and storage. This model emphasizes the provision of physical space, power, cooling, and connectivity, allowing clients to manage their equipment directly while benefiting from the data center's infrastructure. The colocation model represents a tangible asset approach, focusing on the physical attributes of the service and giving clients a significant degree of control over their dedicated space.

Data center capacity services: The integrated paradigm

On the contrary, data center capacity services present a contrasting paradigm, emphasizing integrated services over dedicated physical space. In this model, the focus shifts towards the seamless provision of specialized space, resilient power, cooling, network connectivity, and security. The capacity services approach intertwines these components, forming an interdependent and harmonious service that aligns with the client's operational needs. Here, the emphasis on integrated services offers a holistic solution, with each component significantly influencing and reinforcing the others, to create a cohesive, value-driven offering.

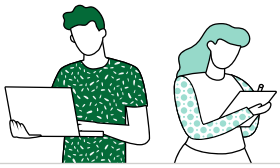
Evolving organizational preferences

Technically, the distinction between these models is increasingly being scrutinized by organizations exploring optimal solutions for their digital infrastructure needs. While colocation services offer tangible control and dedicated space, the integrated nature of capacity services brings forth a synergistic amalgamation of essential components. This shift towards a service-oriented approach represents a new frontier in data center solutions, with its potential impact and practicality yet to be fully explored and understood by many organizations.

IFRS 16
Leases

VS

IFRS 15
Revenue from customer contracts



Data center colocation	VS	Data center capacity
Client recognizes a right-of-use asset and a corresponding lease liability Data center recognizes lease variables	**Asset recognition**	It is a service arrangement rather than involving an asset Data center capitalizes assets utilized in service provision
Lease of data center white space Client will bring, install, and manage its own hardware including servers, racks, and allied infrastructure	**Contract**	Provision of data center capacity Integrated services include specialized space, cooling, and allied environment
Data center recognizes income evenly over lease term	**Revenue**	Recognized as services are rendered to the customer
Fixed periodic lease payments	**Payments**	Variable – based on utilized capacity
Against leasing a data center white space	**Consideration**	Against provision of integrated data center services

IFRS evolution: Redefining balance sheets as capacity services challenge colocation norm

Financial implications: An IFRS perspective

At its core, data center colocation service offers companies the luxury of dedicated space to house their hardware, granting them autonomy over equipment and operations, while providing the benefits of enhanced security, power, and connectivity. This leasing arrangement, viewed through the accounting lens of IFRS 16, casts intriguing shadows on the client's balance sheet, revealing the intricacies of asset and liability management. Conversely, the capacity services model, under the aegis of IFRS 15, refrains from direct balance sheet implications, focusing instead on the recognition of revenue over the contract period. For clients, this translates to a lighter balance sheet, potentially enhancing financial ratios and offering a degree of agility in financial reporting and strategic planning.

A win-win move: Data center capacity services - Boosting agility for providers and clients alike

Strategic choices for data center companies

For data center companies, navigating this strategic crossroads is laden with challenges and opportunities. Their core competency lies in operating extensive, state-of-the-art facilities for clients who prefer to remain unencumbered by the complexities of managing data centers. Yet, the vast majority of their primary assets—data centers—are entangled in lease arrangements, creating a financial tableau that demands careful navigation.

Emergence of a new model

The introduction of data center capacity services offers a paradigm shift, presenting an alternative to the tangible ties and balance sheet implications of asset-specific leasing. With its inherent flexibility and adaptability, this model aligns seamlessly with the dynamic needs of clients, casting a variant financial shadow that may intrigue and sway stakeholders, lenders, and investors.

The future beckons: Colocation to capacity - A strategic leap forward in data center dynamics

Dynamics and choices: A strategic interplay

The nuanced interplay between these models elucidates divergent dynamics and strategic choices for both clients and providers. Colocation services resonate with clients who value autonomy and control, while capacity services cater to those seeking seamless, integrated solutions without the balance sheet encumbrances. The resultant choice can significantly alter the financial narratives and strategic trajectories of both data center companies and their clients. In this intricate dance, lenders and investors scrutinize the evolving financial landscapes, evaluating creditworthiness and risk through the prisms of these models. The choice between asset-centric and service-centric models can shape the financial dialogue, influencing lending terms, investment decisions, and the overall financial health and strategic positioning of the parties involved.

In conclusion, traversing the labyrinth of data center colocation and capacity services unveils a rich tapestry of insights, considerations, and strategic inflection points. The nuanced financial and operational threads woven into these models guide the steps of clients, providers, lenders, and investors. The choice, far from being inscribed in stone, is etched in the evolving narrative of the industry, with the informed and strategic decisions of its participants shaping the contours of the future.

By **Zeeshan Abbasi**, Partner, Risk Advisory, Accounting & Reporting, Deloitte Middle East

The nuanced interplay between these models elucidates divergent dynamics and strategic choices for both clients and providers. Colocation services resonate with clients who value autonomy and control, while capacity services cater to those seeking seamless, integrated solutions without the balance sheet encumbrances.

WhatsApp watch: Are financial institutions under fire?


WhatsApp
Messenger
Simple. Reliable. Secure.
OPEN

From its origins as a personal messaging app, WhatsApp has evolved into an indispensable tool for quick and efficient communication, both personally and professionally. In the UAE alone, approximately 7.99 million people use WhatsApp,[1] which accounts for roughly 80% of the population.

Given its user-friendly interface, many have utilized the application for business communication purposes. Studies indicate that messaging applications, such as WhatsApp, have been used for tasks such as finalizing contracts, circulating business plans, and even sharing sensitive personal information of employees. A study by Veritas in 2021 revealed that 87% of UAE's office workers had admitted to using such messaging applications to share business or sensitive information.[2]

This presents a direct challenge for companies in complying with regulations around the retention of business communications.[3] In recent years, the US securities regulator, the Securities and Exchange Commission (SEC), has turned its attention to brokers and investment advisors for failing to keep records of "off-channel" communications.

Off-channel communications: The use of unapproved applications on mobile devices to engage in communications relating to a firm's business.

In December 2021, the SEC fined J.P. Morgan Securities LLC (JPMS), a broker-dealer subsidiary of JPMorgan Chase & Co., for widespread and longstanding failures by the firm and its employees to maintain and preserve written communications. This was the first of many probes marking the beginning of numerous investigations into such behavior by multiple companies.

As of 29 September 2023, the SEC has issued fines to multiple firms for similar failings totaling over USD two billion[4] (some of which are detailed below).

Date	Company/Event	Fine (US$)
December 2021	JP Morgan[5]	125 million
September 2022	16 firms (including Barclays Capital Inc. and Goldman Sachs & Co. LLC)[6]	1.1 billion (combined)
May 2023	HSBC and Scotia Capital[7]	22.5 million (combined)
August 2023	11 Wall Street firms (including Wells Fargo Securities and BNP Paribas Securities Corp.)[8]	289 million (combined)
September 2023	10 firms (including Interactive Brokers and Robert W. Baird & Co. Inc.)[9]	79 million (combined)

Regulations

Record-keeping regulations exist at local and global levels, particularly within highly regulated industries, such as certain financial services. In the UAE, data retention requirements vary depending on the location of the company's registration, with differences between free zones, such as the Abu Dhabi Global Markets (ADGM), the Dubai International Financial Center (DIFC), and the mainland. In the DIFC where companies are regulated by the Dubai Financial Services Authority (DFSA), organizations are required to adhere to DFSA's Conduct of Business Rulebook (COB), which dictates that electronic communications related to transactions, depending on their nature, must be retained for specified periods of time.[10]

These rules are applicable to all forms of electronic communication, including WhatsApp conversations by employees. For organizations operating in multiple jurisdictions, their data retention and record-keeping requirements may be more extensive or complex. Therefore, it is crucial for organizations to understand the applicable local and international laws and regulations to develop effective strategies and methods to adhere to these requirements.

The solution(s)

If using WhatsApp entails a potential regulatory cost to financial institutions, should these companies prohibit employees from using mobile communication applications for business purposes, or would it be more advisable to implement monitoring solutions that allow for the capturing and retention of business communications on applications like WhatsApp?

In either scenario, several key factors should be taken into consideration, including data governance, the use of corporate devices versus bring-your-own-

device (BYOD), and compliance with data protection and privacy laws.

Organizations should put a focus on data governance, ensuring the implementation of robust policies and procedures that cover various areas, such as the acceptable usage of corporate devices, social media and communication channels, as well as the use of BYOD and data retention. Policies alone are not enough to ensure compliance, as exemplified by JPMS, which had policies in place forbidding the use of non-approved communication channels.[11] Regular employee training and the enforcement of policies with repercussions for non-compliance are critical components of a company's data governance strategy, in addition to ensuring adequate involvement and alignment from multiple departments within an organization.

Effective data governance requires tone-from-the-top, in both compliance and enforcement of policies and procedures. One of the key findings from the SEC's investigations into Wall Street companies was that senior employees were involved in off-channel communications, some of whom were also responsible for overseeing the conduct of junior employees.[12]

To mitigate the risk of fines arising from off-record communications, organizations including J.P. Morgan, Deutsche Bank, and UBS, have started implementing monitoring solutions on employees' mobile devices to monitor and preserve messages.

Privacy considerations

Data privacy and protection regulations must also be considered in a company's efforts to monitor and preserve data. In the UAE, there are multiple laws related to data protection, which may apply depending on the registered location of the company. These laws have an impact on an organization's ability to monitor personal data and an individual's right to privacy. Striking a balance between companies having control over their business data and respecting employees' privacy is necessary.

The SEC explicitly mentioned in their press release that personal devices were frequently used by employees to communicate business matters via various messaging platforms,[13] hindering the ability to maintain and preserve records. Therefore, the common use of BYOD within the UAE may also represent a challenge.

Given the sensitivity of data on BYODs, organizations may not be able to obtain consent to preserve copies of business communication data or to install monitoring and preservation solutions. Gaps in record-keeping may arise if employees leave a company after having used non-monitored BYODs for business communication. Alternatively, there is a risk of data being deleted by employees, for instance, through disappearing messages, wiping, and the manual deletion of messages or chats. Regulators do not appear to be sympathetic to such explanations for having gaps in records.

There is no one-size-fits-all solution. Many organizations may have a complete ban in place for communicating via apps such as WhatsApp for business purposes, however, a weak data governance culture and lack of enforcement may result in gaps that put the organization at risk of regulatory action that could yield fines or reputational impact. Monitoring employees' mobile devices may be the answer for some organizations, but this must be carefully considered in light of data protection and privacy laws, as well as the rights and consent of individuals. In the UAE, the high prevalence of BYOD may deter some companies from implementing such measures.

A key takeaway is the importance of cross-departmental collaboration involving Compliance, HR, IT, Cybersecurity, and other functions to equip the organization and its employees with the knowledge, policies, procedures, and tools to ensure compliance while respecting the delicate balance between data control and privacy.

Another takeaway is that organizations need to have a plan in place for accessing, capturing, and reviewing off-channel communications if and when they occur. Electronic discovery services, including data imaging of mobiles and application data and processing and hosting of data using forensic software, could be used both proactively and reactively, to secure and ensure access to off-channel communications for regulatory compliance monitoring as well as responding to complaints.

By implementing stringent policies, educating employees, ensuring proper data management and governance, and utilizing monitoring and eDiscovery services, companies can reduce their risk and be better prepared to face investigations. The convenience of WhatsApp in corporate communication can coexist with regulatory compliance if managed prudently, ultimately safeguarding a company's reputation and financial stability.

By **Collin Keeney**, Partner, **Natalie Forester**, Manager, and **Faiz Ali Khan**, Assistant Manager, Financial Advisory, Deloitte Middle East

Endnotes

1. https://www.globalmediainsight.com/blog/uae-social-media-statistics/.
2. https://globalcioforum.com/87-uae-employees-share-sensitive-data-via-messaging-and-collaboration-tools-veritas-survey/.
3. https://www.sec.gov/news/press-release/2021-262.
4. https://www.reuters.com/business/finance/us-sec-charges-12-firms-with-record-keeping-failures-2023-09-29/#:~:text=NEW%20YORK%2C%20Sept%20 29%20(Reuters,messaging%20channels%20for%20 discussing%20business.
5. https://www.sec.gov/news/press-release/2021-262.
6. https://www.sec.gov/news/press-release/2022-174.
7. https://www.sec.gov/news/press-release/2023-91.
8. https://www.sec.gov/news/press-release/2023-149.
9. https://www.sec.gov/news/press-release/2023-212.
10. https://dfsaen.thomsonreuters.com/rulebook/cob-67-record-keeping-voice-and-electronic-communications?highlight=record&phrase=false.
11. https://www.complianceweek.com/regulatory-enforcement/big-bank-messaging-app-crackdown-exposes-policy-holes-monitoring-struggles/32002.article.
12. https://www.investmentnews.com/wall-street-girds-for-whats-next-in-whatsapp-probe-240907.
13. SEC.gov | SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures.

Consumer privacy: A business imperative in the digital age

In today's data-driven world, one of the biggest challenges that businesses face is managing data. With increasing volumes of data being collected and processed, ensuring consumer data privacy becomes a constant challenge. Data breaches are not only harmful to businesses and organizations but also affect consumers, who often suffer financial and emotional damages, ultimately leading to a loss of consumer confidence and trust. In response to recent prominent data breaches and growing awareness about personal privacy, regulators have enacted laws and regulations to protect and uphold the rights and privacy of individuals. This article outlines the importance of data privacy, the challenges associated with data compliance, and the necessity of cultivating a culture of privacy awareness.

Consumer data: A powerful tool in the hands of consumer businesses

Consumer data is the information trail left by consumers when navigating the digital world or trading online; this includes personal preferences, demographic data, behavioral patterns, location-tracking, and other forms of personally identifiable information. Consumer data can provide businesses with invaluable insights to better understand consumer preferences, trends, and behaviors. It can help enhance the user experience, develop new products and services, and personalize advertising.

However, as businesses collect, store, process, share, and even sell more and more consumer data, they also face a significant duty—the duty to safeguard the privacy of consumers who become increasingly aware of their personal privacy. Data protection and privacy can be a source of differentiation and customer satisfaction, contributing to business retention and sustainability.

The General Data Protection Regulation (GDPR): Five years later

It has now been five years since the GDPR in the European Union (EU) came into effect as one of the strongest and most comprehensive data protection regulations.[1] The GDPR provides greater protection and rights to individuals while placing limits on what organizations can do with personal data. Personal data is at the heart of the GDPR, which has transformed the way businesses can handle consumers' personal information. There are strict regulations on how businesses can collect and process personal data, and heavy fines can be imposed in case of non-compliance.[2] The GDPR has not only changed the European data privacy scene but has also influenced the world, as it also applies to businesses that are based outside of the EU.[3]

Data privacy: The key to building consumer trust

In a digital world, data privacy stands as one of the key pillars for maintaining consumer trust and fostering increased loyalty. As consumers become more aware and sensitive about their data privacy, implementing robust measures can give businesses an edge over their competitors and help forge strong consumer relationships.

Transparent data practices, explicit consent mechanisms, and stringent security measures form the foundation for establishing trust with consumers.

Organizations that explain their data practices to consumers in easy-to-understand language clearly demonstrate their commitment to transparency, fostering trust. Seeking explicit consent from consumers grants them freedom from intrusion into their private data, boosting their confidence. Building robust data security measures further reinforces consumer faith by assuring their personal information and financial data are protected from potential threats and breaches.

Data privacy compliance: The challenges

Organizations face numerous data privacy challenges, starting with the cost of privacy as a function; becoming privacy-compliant requires a considerable investment in time, resources, and effort. Additionally, there is the cost of maintaining data privacy, as companies may invest in key security technologies. Data classification is another challenge, as organizations must identify and classify personal data within their systems, a process that can be both time-consuming and costly, particularly for consumer businesses with large amounts of data.

Cross-border data transfers present an additional challenge, particularly for global businesses. With diverse data protection regulations in various countries, organizations operating internationally must comprehend and adhere to the data compliance requirements specific to each jurisdiction.

However, the biggest challenge in data privacy remains human error. The World Economic Forum's Global Risks Report 2022 highlighted the critical challenges related to cybersecurity and data breaches, with one alarming statistic: 95% of data breaches were caused by human error.[4] Addressing this issue requires significant investment in training and education, robust policies and procedures, and technology solutions such as data loss prevention.

Data ethics: Embracing ethical data practices

Ensuring the ethical collection, storage, and analysis of consumer data is not only a legal requirement but also a moral obligation. Ethical data measures are critical to prevent bias in data collection and analysis, as well as discrimination and other harmful consequences. Prioritizing ethical data practices allows businesses to cultivate trust, mitigate risks, and bolster their reputation, thereby contributing to their long-term success and sustainability within an ever more data-centric world.

As businesses incorporate technology and data at the core of their business strategy, consumers will remain loyal to the brands they trust. Data ethics is a fundamental part of this process.

Building a culture of data privacy: The importance of education and collaboration

While approaching data privacy compliance as an independent function can significantly help achieve privacy goals, from operational efficiency to legal compliance and consumer trust, all internal stakeholders, including legal teams, IT teams, HR teams, and marketing and sales teams, must work hand in hand as the primary generators and users of consumer data.

Furthermore, every other employee must be trained and equipped with the knowledge of ethical data practices. Building trust requires a joint effort to ensure the responsible use and protection of data. A fundamental component of this effort involves educating users about the best privacy practices by raising awareness about their rights, the types of data collected, how it is utilized, and the measures in place to protect it.

Case studies: The cost of data breaches

Google's privacy controversies

The first significant fine under the GDPR was levied against Google with a EUR50 million (US$52.9 million) fine from the French data protection regulator, the Commission Nationale Informatique & Libertés (CNIL). The fine was issued for two main reasons: Google's failure to provide sufficient information to users regarding how it utilizes data collected from 20 different services, and not obtaining proper consent for processing user data.[5]

Meta's violation of GDPR rules

Meta, the owner of Facebook, was fined by the Irish Data Protection Commission (DPC) for violating the GDPR by transferring personal data of EU users to the US without adequate safeguards.
The fine of EUR1.2 billion was the largest GDPR fine ever and was imposed following a binding decision by the European Data Protection Board (EDPB), which resolved a dispute between the DPC and other EU data protection authorities.
Meta was also ordered to stop transferring user data to the US by October 2023 and to delete any data that was transferred unlawfully since July 2020.[6]

Facebook's data scandal

The Facebook/Cambridge Analytica scandal was a major data privacy breach that took place in 2018. It involved the misuse of personal data from millions of Facebook users by a political consulting firm called Cambridge Analytica. This firm used the data to influence elections and campaigns worldwide, without the users' consent or knowledge. The scandal sparked public outrage, triggered regulatory investigations, and significantly tarnished Facebook's reputation and trust.

In December 2022, Facebook's parent company, Meta (formerly known as Facebook), agreed to pay US$725 million to settle a class-action lawsuit related to the scandal. This settlement represents the largest in a US data privacy class action and encompasses all US Facebook users who had active accounts between May 2007 and December 2022.[7]

Yahoo's data breach

In 2016, Yahoo, one of the largest internet companies in the world, disclosed two massive data breaches that occurred in 2013 and 2014. The breaches affected over three billion user accounts, exposing names, email addresses, passwords, and security questions. The breaches were attributed to state-sponsored hackers and resulted in a US$350 million cut in Yahoo's sale price to Verizon.[8]

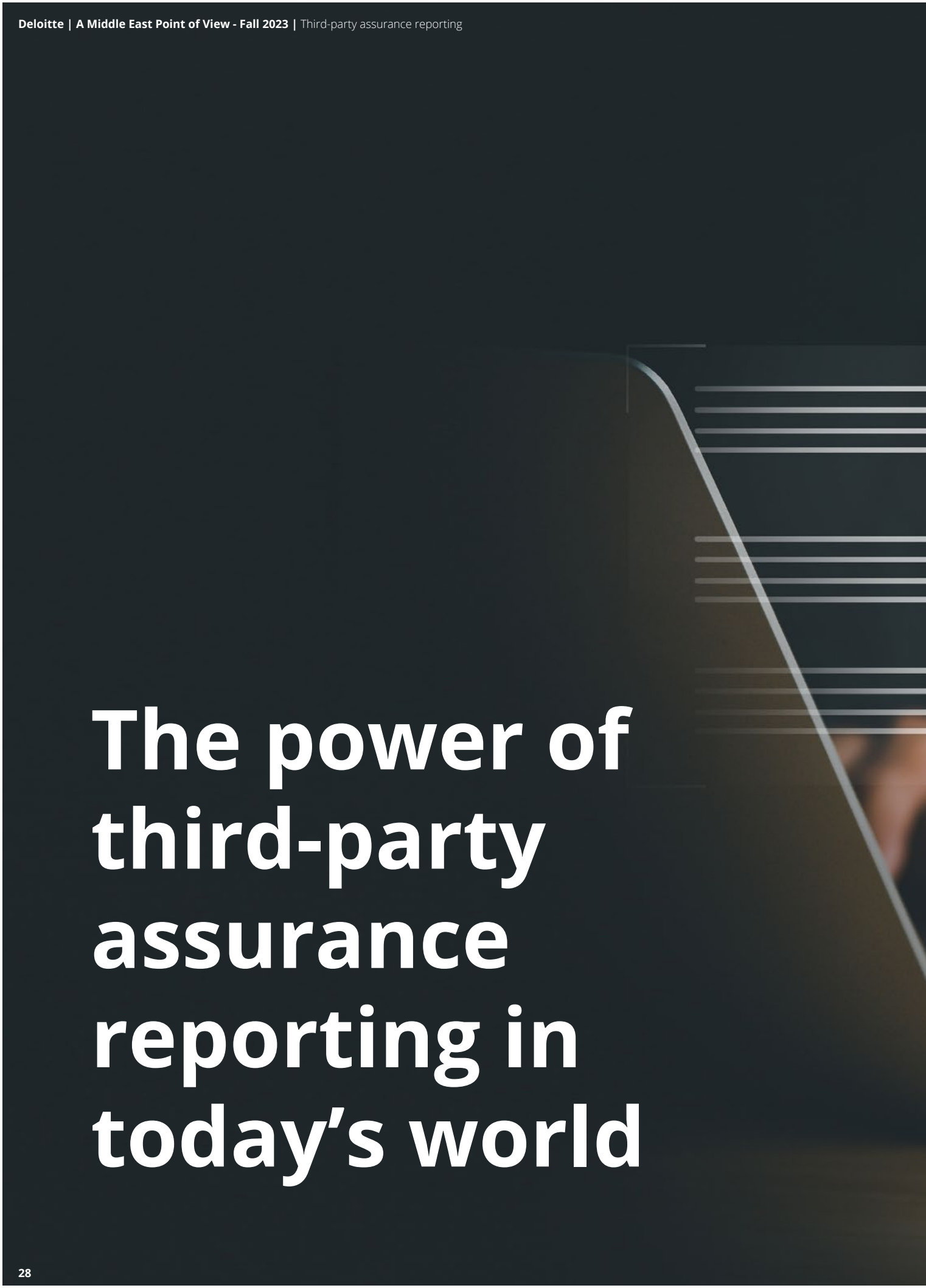
These case studies provide valuable insights into the real-world effects of data breaches in consumer businesses. The impact of data breaches can be substantial, and beyond the financial fines and legal repercussions, the reputation damage can erode customer trust and loyalty, leading to further loss of profits and market share. Prioritizing data protection ensures legal compliance, financial stability, and sustained reputation, while strengthening trust between businesses and consumers.

By **Ikram Moulila**, Director, Financial Advisory, Deloitte Middle East

Endnotes

1. Source: General Data Protection Regulation (GDPR) – Official Legal Text – Key Issues. Link: https://gdpr-info.eu/issues/.
2. Source: General Data Protection Regulation (GDPR) – Official Legal Text – Fines / Penalties. Link: https://gdpr-info.eu/issues/fines-penalties/.
3. Source: General Data Protection Regulation (GDPR) – Official Legal Text – Third Countries. Link: https://gdpr-info.eu/issues/third-countries/.
4. Source: World Economic Forum – Global Risks Report 2022 – Page 52. Link: https://www.weforum.org/publications/global-risks-report-2022/
5. Source: European Data Protection Board, 21 January 2019 - The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | European Data Protection Board (europa.eu).
6. Source: European Data Protection Board, 22 May 2023 - https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.
7. Source: Court filing of the proposed settlement agreement between Meta and the plaintiffs, which was disclosed on 23 December 2022 - https://www.justice.gov/crt/case-document/file/1514126/download.
8. Source: Reuters, 4 October 2017, based on Yahoo official announcement - https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1.

In a digital world, data privacy stands as one of the key pillars for maintaining consumer trust and fostering increased loyalty



The power of third-party assurance reporting in today's world

Amid global megatrends and a connected financial landscape, organizations increasingly rely on third-party vendors for critical services. The Deloitte Global Outsourcing Survey 2022 indicated that 76% of global executives outsourced their IT services via third-party models, while 52% of global executives outsourced various business functions.[1]

Considering the growth of the outsourcing ecosystem, compliance pressures grow and regulations evolve. Customers now demand security and confidentiality assurances through third-party assurance reports, typically Service Organization Control (SOC) reports. These reports assess internal control effectiveness in meeting shared business objectives; they are also commonly used and requested, especially by service organizations serving customers across diverse regions.

SOC reports encompass three primary types: SOC 1, SOC 2, and SOC 3, each tailored to specific objectives and areas of emphasis. The below table provides insight into the differences between each type.[2]

SOC 1	SOC 2	SOC 3
Designed to assess the effectiveness of internal controls pertaining to financial reporting, making them particularly pertinent to financial processes such as payroll, accounting, and financial transaction processing.	Examination of controls related to specific trust categories; availability, processing integrity, confidentiality, and privacy of a service organization's systems and services.	Closely resemble SOC 2 reports but are intended for a broader audience. They provide a condensed overview of a service organization's controls without delving into intricate details.
Applicable to organizations providing services that could impact the financial statements of their clients, including third-party administrators, payment processors, and cloud service providers.	Well-suited for any organization that delivers services involving sensitive data or critical processes, such as data centers, managed IT services, or Software as a Service (SaaS) providers.	Similar to SOC 2 reports, SOC 3 reports apply to organizations offering services with an emphasis on security, availability, processing integrity, confidentiality, and privacy.
They delineate critical controls essential for ensuring financial accuracy and compliance while evaluating their design and operational efficiency.	Aligns with the Trust Services Criteria and evaluates controls related to security, availability, processing integrity, confidentiality, and privacy, depending on the specific criteria.	Evaluate controls based on the Trust Services Criteria, albeit in a less detailed and technical manner compared to SOC 2 reports.
Primarily serve the interests of the service organization's management, the service auditor, and the customers of the service organization.	Customers, business partners, and regulatory authorities commonly request and rely on SOC 2 reports to assess the security and privacy protocols of service providers.	Designed for public consumption and are frequently utilized for marketing purposes. They are openly accessible to anyone and offer a generalized assurance of a service organization's controls and practices.[3]

Disclaimer: SOC 1 and SOC 2 are terms used to distinguish between reports that focus on internal controls over financial reporting (SOC 1) and reports that focus on internal controls over data management (SOC 2). Not all reports across all regions use the SOC framework (e.g. under ISAE 3402, there are frameworks such as AAF 01/20 from the UK, GS 007 from Australia etc.), however for simplicity, we categorized the type of report framework as either SOC 1 or SOC 2.

Why third-party assurance reporting?
Third-party assurance reporting provides benefits to both service organizations and their customers. Some of the key benefits for service organizations who request third-party assurance reporting, explicitly SOC reporting[4], are:

- Positive SOC reports offer a competitive edge, showing dedication to security and reliability, attracting new clients, and increasing conversion rates.
- SOC reporting enhances credibility by providing high assurance on internal controls.
- Simplifies due diligence, reducing customer audit efforts, reassuring existing clients, and increasing customer retention rates.
- Helps meet compliance requirements, avoids legal issues, reduces audit costs, and enhances operational efficiency and risk management.

For businesses engaging with service organizations, some of key benefits of requesting SOC reports are:[5]

- SOC reports instill customer confidence in a service provider's commitment to security, reliability, and transparency.
- SOC reports provide insight into a service organization's controls, helping customers understand data handling and operations.
- Strong SOC reports build trust in data safeguarding, particularly for sensitive information.
- Relying on SOC reports instead of extensive audits leads to cost savings for customers, reducing expenses and administrative overhead.
- In regulated sectors, SOC reports serve as evidence of compliance with specific prerequisites, valuable for sensitive data or specialized industry regulations.

Third-party assurance attestation journey
For service organizations that are preparing to conduct SOC 1 , SOC 2, or SOC 3 attestations, and in order to move from the steady to the ready stage, there are key steps to be taken to accomplish an efficient assessment:

A. Define SOC report scope
B. Understand current state of controls
C. Assess design and implementation of controls
D. Identify gaps in achieving control objectives
E. Report to management with insight and recommendations for remediation

Upon completing the readiness assessment, service organizations will have the opportunity to showcase the level of effectiveness of their internal controls within the environment where customer data and information are hosted. If positive outcomes are confirmed in the report, this can position them as industry leaders, instilling confidence and trust among their customers.

Even if companies today are not yet prepared for third-party attestations, forward-thinking organizations are planning for the future.

Prior to jumping ahead in conducting an attestation assessment, companies can opt towards having a readiness assessment. Service organizations will be able to answer the following questions:

- Is my organization properly prepared for an SOC attestation?
- Are my relevant internal controls effective and policies in place?
- What are the key weaknesses present?
- How can those weaknesses be remediated before the attestation?

With this context in mind, Deloitte surveyed a sample of TPA reports (where permissible) from across the globe and from multiple industries to benchmark them and identify further insights and trends of key interest to the global TPA community. The key highlights from the benchmarking analysis of 98 sampled TPA reports include:

- TPA reports address internal control over financial reporting (ICFR) and operational areas but recently started to adapt more on emerging digital and cloud-related risks, requiring organizations to monitor and assess third-party risks amid the evolving risk landscape.
- Emerging risks and growing third-party reliance create an opportunity for TPA reports to offer assurance in broader areas, enhancing their value in the outsourcing ecosystem.
- Increasing awareness and use of SOC 2+ reports is driven by the growing compliance costs as organizations strive to meet customer, regulatory, and stakeholder demands. This trend is expected to result in continued demand growth.

In brief, as businesses expand within their respective markets, their dependence on service organizations for supporting their expanding operations intensifies. This heightened reliance raises critical concerns regarding the security and integrity of the data managed. Consequently, third-party assurance reporting addresses key inquiries, such as the security of data and the effectiveness of controls within the service organization responsible for businesses' information. As business navigates this landscape, fostering a proactive commitment from service providers to the robustness of internal controls environment fortify the foundation upon which successful business expansion rests.

By **Bhavna Lakhani**, Partner, Technology Assurance & Analytics, **Fadi Ghawi**, Director, Technology Assurance, and **Mais Barouqa**, Senior Manager, Technology Assurance, Deloitte Middle East

Endnotes

1. "Beyond outsourcing: Entering a new sourcing ecosystem,", Deloitte & Touche, 2022.
2. "Third- Party Assurance Engagement – SOC2," Deloitte & Touche.
3. "Third Party Assurance Engagement – SOC2," Deloitte & Touche.
4. "Providing Assurance through SOC Reports," Deloitte & Touche.

COP28: Transparency drives sustainability reporting

In December 2023, over 75,000 individuals are expected to attend the United Nations Climate Change Conference (COP28) in the UAE, an annual gathering of countries seeking to tackle the global challenge of climate change. In addition to governmental representatives from nearly 200 countries and heads of state, they will also be joined by a large number of delegates from environmental NGOs, think tanks, the private sector, and other organizations.

The central theme of the two-week conference is climate change and the imperative for countries to confront the global climate challenge by fulfilling their commitments to reduce Greenhouse Gas (GHG) emissions. The conference aims to delve into strategies and actions that nations must undertake to effectively address climate change and honor their pledges for emissions reduction

A key contributing feature to the discussions will revolve around "transparency," the process of reporting and reviewing relevant climate information and data at a country level, as described by the UN entity tasked with overseeing the conference, the UN Climate Change secretariat. The arrangements that have been put in place seek to ensure the availability of regular data on countries' GHG emissions, policies and measures, progress towards targets, climate change impacts and adaptation, levels of support, and capacity-building needs. As stated, "By providing clear and robust data and information on climate action, transparency also serves to build trust, credibility, and accountability among all those involved."[1]

While the primary focus of the COP will be global climate change and key reporting of GHG emissions at a country level, many conference attendees will recognize the sentiment of transparency as being relevant also at a corporate level and to a wider range of ESG related topics and metrics. Over the past few years, the development of corporate sustainability reporting, covering an increasingly wider range of concerns beyond climate change and responding to an increasingly varied group of users, has been meteoric. Indeed, in certain jurisdictions, sustainability reporting is also moving from a voluntary to a mandatory reporting regime.

In 2023, significant steps forward were made, both internationally and regionally, which will help to "build trust, credibility, and accountability" between companies and their key stakeholders – investors, financers, consumers, suppliers, and the wider society.

On the international front

Internationally, there have been a number of milestones which have clarified the nature of sustainability reporting and its future direction:

- **Global Reporting Initiative (GRI):** In January 2023, the updated GRI Universal Standards became effective. The GRI has developed over 25 years and is the world's most widely used sustainability reporting standard. This year's update strengthens the standards intending to deliver the highest level of transparency for a company's impact on the economy, the environment, and people. As a stand-alone, impact-focused standard issued by a company and usually published on its website, it is readily accessible to a very wide group of stakeholders and explains a company's "outward" impact. GRI typifies the concept of a stand-alone sustainability report.

  GRI remains a key sustainability reporting standard, widely used across the Middle East and increasingly promoted by regional stock exchanges.

- **International Sustainability Standards Board (ISSB):** In June 2023, two new International Financial Reports Standards (IFRS S1 & S2) were launched by the ISSB, focusing on climate related financial disclosures.

  These standards intend to result in a high-quality, comprehensive global baseline of sustainability disclosures focused on the needs of investors and financial markets. With their alignment to a company's financial statements, and being the product of a number of previous climate-related financial disclosure standards amalgamated together, they primarily report the impact on a company of climate-related change, i.e., "inward" impact.[2] This is of particular relevance to investors as being descriptive of the impact of climate change on enterprise value.

  Effective 1 January 2024 for jurisdictions that adopt them, these standards are currently undergoing scrutiny and consultation with regards to their practical application by those adoption bodies. Anecdotally, these standards are currently being considered by regulators across the Middle East and evaluated for their effective adoption and use in their local markets.

- **European Sustainability Reporting Standards (ESRS):** In July 2023, the European Commission adopted the ESRS. One of the central pillars of the Corporate Sustainability Reporting Directive (CSRD) is the requirement for in-scope companies to produce disclosures in accordance with the ESRS, which will involve reporting on a broad range of sustainability topics and applying a "double materiality" approach. This combines the "outward impact" reporting of GRI with the "inward impact" reporting of IFRS S1 & S2. The directive will also make it mandatory for reported sustainability information to be assured.

  According to the European Commission, approximately 50,000 companies are expected to be impacted by the requirements of CSRD, and the first wave of companies to be reporting will have to apply the new rules from as early as 2025, for financial years beginning on or after 1 January 2024.

  While not directly applicable to Middle East companies, ESRS will be relevant to those based outside of the EU but with

operations within. Therefore, such entities will need to consider their footprint and determine whether or not they trigger the necessary criteria and are required to comply.

- **COSO Internal Controls for Sustainability Reporting (ICSR):** In March 2023, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a landmark interpretive report on how the existing COSO Internal Control Framework can apply to sustainable business activities and information.

  Their report "Achieving Effective Internal Control Over Sustainability Reporting (ICSR)," illuminates how the COSO Framework's 5 components and 17 principles can help companies establish an effective and integrated system of internal control over their material or decision-useful sustainable business information.[3]

  Given the increase in expectation by users of the robustness and accuracy of a company's published sustainability information, the processes which create that information should be part of an effective internal controls environment; this is in-line with published financial information. The ICSR framework provides clear guidance on how such environments should be developed and maintained.

  Middle East entities that are more advanced in their sustainability reporting maturity and, in particular, are looking at preparing climate related financial disclosures, should consider developing an ICSR framework to help meet the level of quality and robustness expected for the reported information.

On the regional front

Regionally, there has been a noticeable increase in sustainability reporting activity, with regulators and stock exchanges supporting the development of such reporting practices. There is also a growing effort to synchronize these initiatives with international standards, reflecting a global commitment to fostering sustainable business practices.

- **GCC Exchanges Committee ESG metrics:** In January 2023, the Committee released a unified set of ESG Disclosure Metrics that includes 29 metrics aligned with the World Federation of Exchanges, the Sustainable Stock Exchanges Initiative, and GRI.

  The GCC ESG Disclosure Metrics are an important step towards standardizing ESG disclosure across the GCC region, which currently uses different approaches of reporting. The metrics are voluntary and serve as a guideline for companies, particularly those who have yet to start their ESG disclosure approaches. The metrics do not replace existing ESG disclosure guidelines that GCC stock exchanges have already issued.

- **Amman Stock Exchange (ASE):** In January 2023, the mandatory requirement for ASE listed companies in Jordan to create and publish a GRI sustainability report came into effect. It was previously announced in the ASE Guidance on Sustainability Reporting Guidance 2022.

- **Muscat Stock Exchange (MSX):** In September 2023, the MSX in Oman launched a new report providing guidelines for listed companies to deal with information and data related to basic elements of sustainability.

  The guidance included two key announcements: firstly, effective from January 2024, companies should consider reporting, on a voluntary basis, a set of ESG metrics, based the GCC ESG Disclosure Metrics and also issue a GRI Sustainability Report; but, effective from January 2025, both ESG metrics and the GRI Sustainability Report will be mandatory.

Previously, in 2021, the UAE's Securities and Commodities Authority made GRI reporting mandatory for listed companies on the Dubai Financial Market (DFM) and Abu Dhabi Securities Exchange (ADX); and in 2022 in Egypt, the Financial Regulatory Authority made Task Force on Climate-Related Financial Disclosures (TCFD) reporting mandatory for certain large listed companies. With the inclusion of both Jordan and Oman this year in making GRI Sustainability Reporting mandatory in due course, this demonstrates the commitment to international sustainability reporting standards by Middle East regulators and stock exchanges.

With COP28 being an event at which big announcements are often made, some Middle East countries may take the opportunity to publicly commit to adopting one of the standards mentioned above; and indeed, some organizations are likely to use the occasion to demonstrate how far in their sustainability reporting they have come. These are all positive moves in the drive towards "transparency," which will ultimately help in the objectives of the COP28 event.

By **Damian Regan**, Sustainability Reporting & Assurance Leader, Deloitte Middle East

Endnotes

1. What is transparency? | UNFCCC - https://unfccc.int/process-and-meetings/transparency-and-reporting/about-transparency/what-is-transparency.
2. The ISSB has drawn on existing standards and frameworks that are used widely by companies, including IFRS Accounting Standards, the Task Force on Climate-related Financial Disclosures (TCFD) Recommendations, the SASB Standards, the Integrated Reporting Framework CDSB Framework, and World Economic Forum metrics to streamline sustainability disclosures - IFRS - Ten things to know about the first ISSB Standards.
3. ICSR | COSO.

Thought leadership publications from Deloitte

ME PoV provides you with a selection of Deloitte's most recent publications accessible on Deloitte.com

ME PoV

ME PoV Summer 2023 issue
Swift moves

Energy & Resources

Leading the path towards methane abatement

Islamic Finance

Islamic Finance as a catalyst for financing the Sustainable Development Goals (SDGs)

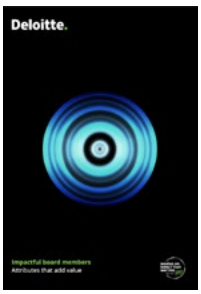
Construction

Deloitte GCC Powers of Construction 2023

Climate

Deloitte 2023 CxO Sustainability Report

Human Capital



Impactful board members
Attributes that add value

Board Impact
Understanding and measuring the value of a board

ME Human Capital Trends 2023

Financial Advisory

Real Estate Predictions 2023
A market overview of Dubai and KSA

Trade and Transit
Evaluating the India-Middle East-Europe economic corridor

Consulting

Unlocking the e-commerce potential in a post-COVID world

Annual global competitiveness overview Who is winning the race?

Social Care for the Elderly in the Middle East

Deloitte Global Marketing Trends 2023 – Middle East Resilient seeds for growth

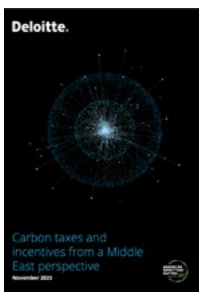
Gaming and e-sports in KSA

TMT

Tech trends 2023

Tax

Key features of the UAE Corporate Tax Law



Carbon taxes and incentives from a Middle East perspective

Risk Advisory

2023 Global Future of Cyber Survey

Deloitte offices

Regional office
Gefinor Center, Block D
Clemenceau Street
P.O. Box 113-5144
Beirut, Lebanon
Phone +961 (0) 1 748 444
Fax +961 (0) 1 748 999

Consulting
Emaar Square, Building 1, level 2
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

Deloitte Digital Center
Al Ra'idah Digital City
Building: RDC IN 01, 1st floor
Riyadh, Saudi Arabia
Phone +966 (0) 11 404 5900

Financial Advisory
Al Fattan Currency House
Building 1, DIFC
P.O. Box 112865
Dubai, United Arab Emirates
Phone +971 (0) 4 506 4700
Fax +971 (0) 4 327 3637

Risk Advisory
Emaar Square, Building 3, level 6
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

Tax & Legal
Al Fattan Currency House
Building 1, DIFC
P.O. Box 282056
Dubai, United Arab Emirates
Phone +971 (0) 4 506 4700
Fax +971 (0) 4 327 3637

Quick links

Website
deloitte.com/middleeast

LinkedIn
Deloitte

Facebook
Deloitte

Twitter
@DeloitteME
@DeloitteMEjobs
@DeloitteKSA

Instagram
deloittemiddleeast

Bahrain
Manama
United Tower
Bahrain Bay
P.O. Box 421
Manama, Kingdom of Bahrain
Phone +973 (0) 1 721 4490
Fax +973 (0) 1 721 4550

Cyprus
Nicosia
24 Spyrou Kyprianou Avenue
CY1075
Nicosia, Cyprus
Phone +357 (0) 22 360300
Fax +357 (0) 22 360400

Limassol
Maximos Plaza, Block 1, 3rd floor
213, Arch. Makariou III Avenue
CY3030
Limassol, Cyprus
Phone +357 (0) 25 868686
Fax +357 (0) 25 868600

Egypt
Cairo
Nile City South Tower, 6th floor
2005 A Cornish El Nile
Ramlet Boulaq
Cairo, Egypt
Phone +20 (0) 2 246 199 09
Fax +20 (0) 2 246 199 04

Alexandria
Madinet El Sayadla
Building No 10, Smouha
Alexandria, Egypt
Phone +20 (0) 3 426 4975
Fax +20 (0) 3 426 4975

Iraq
Erbil
Empire Business Complex
Building C1, 5th Floor
Erbil, Iraq
Phone +964 (0) 66 219 3323

Baghdad
Al Mansour, Al Amirat Street
District 601, Street 15, Villa no. 41
Baghdad, Iraq
Phone +964 (0) 770 694 6554

Jordan
Amman
Jabal Amman
190 Zahran Street
P.O. Box 248
Amman, Jordan
Phone +962 (0) 6 550 2200
Fax +962 (0) 6 550 2210

Kuwait
Kuwait City
Dar Al-Awadi Complex
Ahmed Al-Jaber Street, Sharq
P.O. Box 20174
Safat, Kuwait
Phone +965 2240 8844
Fax +965 2240 8855

Lebanon
Beirut
Arabia House
131 Phoenicia Street
Ain Mreisseh
P.O. Box 11-961
Beirut, Lebanon
Phone +961 (0) 1 364 700
Fax +961 (0) 1 369 820

Libya
Tripoli
Tripoli Tower
P.O. Box 93645
Tripoli, Libya
Phone +218 (0) 92 370 1049

Oman
Muscat
Minaret Al Qurum Building, 6th floor
Qurum Area, Muscat
P.O. Box 258
Ruwi, Postal Code 112
Muscat, Oman
Phone +968 (0) 2481 7775
Fax +968 (0) 2481 5581

Palestinian Territories
Ramallah
Al Mashreq Insurance Building
P.O. Box 447
Ramallah, Palestinian Territories
Phone +970 (0) 2 295 4714
Fax +970 (0) 2 298 4703

Qatar
Doha
Al Ahli Bank Building
Sheikh Suhaim Bin Hamad Street
P.O. Box 431
Doha, Qatar
Phone +974 (0) 4434 1112
Fax +974 (0) 4442 2131

Saudi Arabia
Riyadh
Prince Turki Bin Abdullah
Al-Saud Street
Sulaimana Area
P.O. Box 213
Riyadh 11411, Saudi Arabia
Phone +966 (0) 1 282 8400
Fax +966 (0) 1 282 8428

Al Khobar
ABT Building, Al Khobar
P.O. Box 182
Dammam, Saudi Arabia
Phone +966 (0) 13 668 5700
Fax +966 (0) 3 887 3931

Jeddah
The Headquarters Business
Park Tower
40th floor, Corniche Road
P.O. Box 442
Jeddah, Saudi Arabia
Phone +966 (0) 12 578 1000

Sudan
Emaar Square, Building 3, level 6
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

United Arab Emirates
Abu Dhabi
Al Sila Tower, 11th floor
Abu Dhabi Global Market Square
P.O. Box 990
Abu Dhabi, United Arab Emirates
Phone +971 (0) 2 408 2424
Fax +971 (0) 2 408 2525

Dubai
Emaar Square, Building 3, level 6
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

Fujairah
Al-Fujairah National Insurance Co.
Building, 6th floor
P.O. Box 462
Fujairah, United Arab Emirates
Phone +971 (0) 9 222 2320
Fax +971 (0) 9 222 5202

Ras Al-Khaimah
Julphar Commercial Towers, 19th
floor
P.O. Box 435
Ras Al-Khaimah, United Arab
Emirates
Phone +971 (0) 7 227 8892
Fax +971 (0) 7 227 7465

Sharjah
United Arab Bank Building, 13th
floor
Al Buhairah Corniche
P.O. Box 5470
Sharjah, United Arab Emirates
Phone +971 (0) 6 517 9500
Fax +971 (0) 6 517 9501

Yemen
Sana'a
Sana'a Trade Center
Algeria Street, Sanaa
P.O. Box 15655
Alsafyah, Yemen
Phone +967 (0) 1 448 374
Fax +967 (0) 1 448 378

Deloitte.

Deloitte at COP28

We are committed to bringing together global leaders and policymakers across the public, private, and nonprofit sectors to further climate action. Join us at COP28, where we are helping drive the green transition and fostering resilience across these sectors to create a more sustainable, prosperous world.

Scan the QR code to find out more

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche (M.E.) LLP ("DME") is the affiliate for the territories of the Middle East and Cyprus of Deloitte NSE LLP ("NSE"), a UK limited liability partnership and member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL").

Deloitte refers to one or more of DTTL, its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL, NSE and DME do not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 300,000 people make an impact that matters at www.deloitte.com.

DME would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. DME accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

DME is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926. DME's presence in the Middle East region is established through its affiliated independent legal entities, which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME's affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.

DME provides audit and assurance, consulting, financial advisory, risk advisory, and tax services through 27 offices in 15 countries with more than 5,000 partners, directors and staff.

© 2023 Deloitte & Touche (M.E.). All rights reserved.