Annual Security Report 2024

GBM

AI HORIZONS

AI Impact on Cybersecurity and Privacy in the Middle East 2024

Embracing Opportunities and Mitigating Risks in the Age of AI


GBM

CONTENTS

FOREWARD

As we progress through 2024, the landscape of Artificial Intelligence (AI) in the Middle East continues to evolve with groundbreaking innovation and growth. The region has embraced AI and its transformative social and economic growth potential. Initiatives like The National Strategy for Artificial Intelligence 2031 - UAE and Saudi Vision - 2030 highlight the Middle East's ambition to become an AI superpower and its commitment to harnessing the power of AI for national development.

The economic contribution of AI is expected to be around $320 billion, of which $135.2 billion is expected to accrue in Saudi Arabia. In relative terms, the UAE is expected to see the largest impact by 2030, with a 14% boost to the GDP.

The region is fast becoming a blueprint for countries across the globe when it comes to integrating AI and technology to improve daily life. Sectors like healthcare, energy, aviation, construction, etc., are all seeing improvements as AI is used to optimize operations and boost efficiency. Customer experience is also being enhanced with intelligent chatbots providing more personalized experiences and recommendations.

Bassam Rached
General Manager - Technology, GBM

A BRAVE NEW WORLD

However, this mass adoption of AI also brings cybersecurity and privacy concerns to the forefront. New vulnerabilities and attacks are being discovered that can halt the ambitious visions outlined for the region unless preventative measures are implemented. Along with AI's massive potential, cybercriminals can also misuse it, enabling mass automation of cyber attacks. Additionally, the landscape of AI regulatory frameworks and challenges is becoming increasingly difficult due to its fragmented nature.

The region has taken steps to promote the responsible and ethical usage of AI, with initiatives like Digital Dubai's Ethical AI Toolkit guiding businesses, academic institutions, and individuals in navigating the complexities of AI deployment. Global frameworks like the NIST AI Risk Management Framework (RMF) and ISO/IEC 42001 have been released to serve as benchmarks and best practices for responsible AI.

The challenge is not just technical but requires a nuanced understanding of AI's dual nature as both a competitive advantage and a risk.

The following are some key stakeholders that must adopt a collaborative approach to understanding and mitigating AI's unique challenges.

Chief Information Security Officers (CISOs) oversee an organization's overall information security strategy, ensure data protection from cyber threats, and comply with cybersecurity regulations.

Chief Technology Officers (CTOs) lead the development and implementation of technology strategies, ensuring that technological resources align with the organization's goals and innovation needs.

Chief Risk Officers (CROs) focus on identifying and mitigating overall business risks, ensuring regulatory compliance, and safeguarding the organization's overall cybersecurity posture.

Chief Privacy Officers (CPOs) oversee an organization's data privacy policies and practices, ensuring compliance with privacy laws and regulations while safeguarding personal information.

Other industry leaders include executives and decision-makers across various sectors who play a crucial role in shaping industry standards and practices, particularly in adopting and ethically using AI technologies.

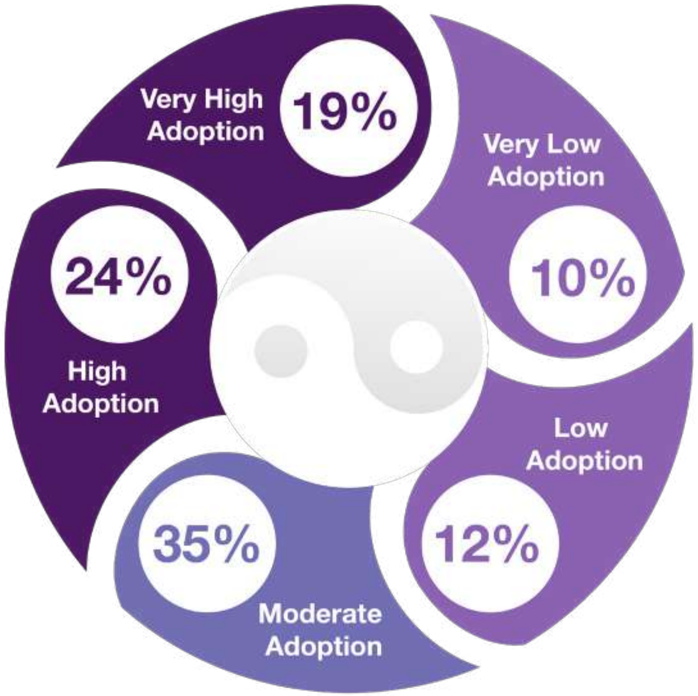
AI - THE DOUBLE-EDGED SWORD

This image has been generated using AI

The rise of Artificial Intelligence (AI) marks a significant milestone in the history of technology, bringing unprecedented opportunities and significant challenges. Generative AI (GenAI), stands at the forefront of this revolution as a key example of AI's dual nature.

> **A majority of organizations (59%) report moderate to high AI adoption in 2024, with significant progress in leveraging AI technologies for core business functions.**

AI Adoption Trends 2024



GenAI has the potential to revolutionize industries and supercharge economic growth, but its capability for content creation raises concerns about ethical and secure data usage and security. As frameworks evolve in the Middle East, there is a critical need to address these challenges to harness the potential of GenAI securely and responsibly. The Global Cybersecurity Outlook 2024 report by the World Economic Forum emphasizes a striking concern among senior leaders: over half view the evolution of cyberattacks facilitated by Generative AI technologies—including deepfakes, phishing, and malware—as their most significant challenge.

The challenge is wider than just GenAI, given the usage of AI in other critical industries. AI models in healthcare can provide personalized patient care. At the same time, the energy sector can benefit from AI's ability to optimize renewable energy production in line with the region's long-term goals on sustainability. An attack or compromise of these AI models in healthcare and energy can have a catastrophic impact if successful and undermine the public's trust in these initiatives.

The Middle East stands at a crossroads with its visionary leadership and strategic initiatives towards AI. Its forward-thinking approach means that AI will be integrated into every aspect of our lives and introduce security and privacy challenges that did not exist before.

The GBM Annual Security Report 2024 aims to help in these efforts and provide insights to technology leaders on navigating this new landscape safely. Leaders across government, business, technology and academia, can use this report to guide their efforts to foster an environment where AI can flourish safely and securely.

THE NATURE OF AI RISKS

The dual nature of AI is particularly pronounced in the Middle East, given the key role that AI plays in economic development within the region. AI offers a transformative opportunity for the Middle East to emerge as a global technology leader, fostering economic diversification and advancing innovation across various sectors. At the same time, however, adopting AI into various industry sectors poses significant security and privacy risks.

This image has been generated using AI

A few of the key risks that are being introduced are:

AI-Specific Vulnerabilities

Weaknesses in AI algorithms and models can lead to cyberattacks, exploiting them to influence decisions and outcomes. Additionally, the vast amounts of information that AI models have access to could create potential avenues for data leakage.

AI-Powered Cyberattacks

AI can power attacks such as phishing, malware, DDOS, and others, effectively automating these activities and leading to a massive boost in their volume and sophistication.

Misinformation

GenAI can be used to spread Deepfakes and AI-generated images for spreading misinformation on social media to influence public opinion. This can lead to nation-state actors manipulating online narratives casting and posing significant challenges to the integrity of information.

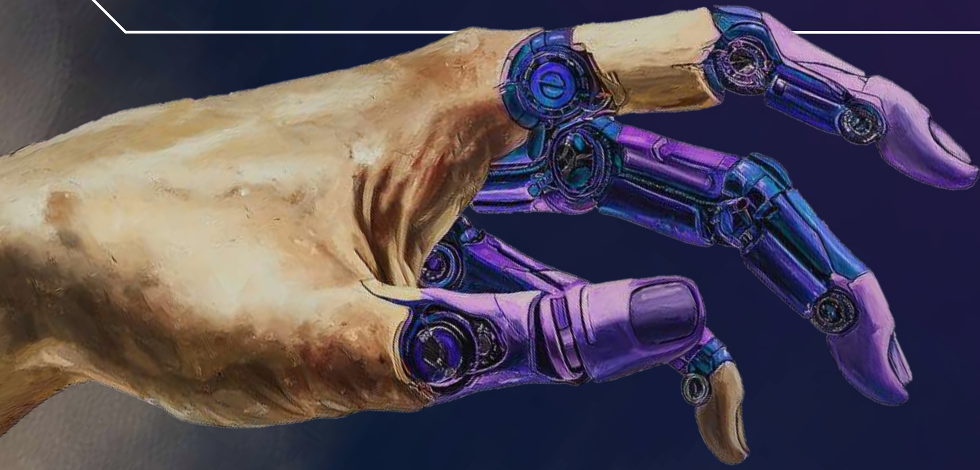
Lack of AI related regulations and standards

The absence of robust and established standards presents a critical challenge. Security and privacy frameworks lack the comprehensive maturity required to effectively counteract and mitigate the unique risks associated with advanced technologies like Generative AI.

* This image has been generated using AI

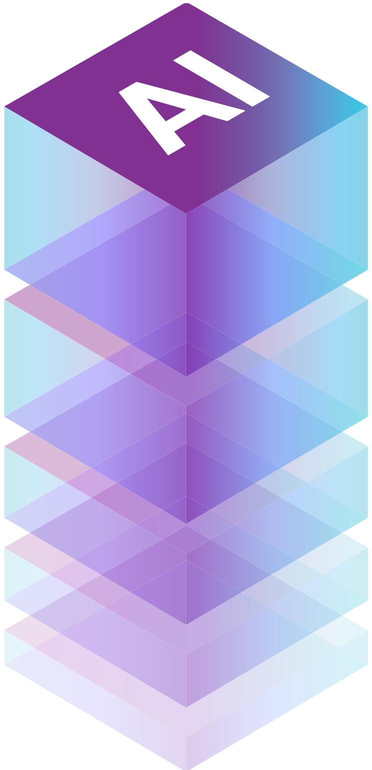
AI AS A CATALYST FOR INNOVATION AND GROWTH

> Generative AI is revolutionizing organizational operations, with 37% citing increased efficiency and 22% highlighting enhanced innovation as its most significant impacts.



This image has been generated using AI

Key Benefits of Generative AI



- **37%** **Improved efficiency and productivity**
- **22%** **Enhanced creativity and innovation**
- **18%** **Data analysis and insights**
- **15%** **Cost reduction**
- **8%** **Improved customer experience**

Along with the highlighted risks, AI's meteoric rise brings many opportunities across various sectors. Generative AI (GenAI), with its unparalleled ability to create text, images, video, and more, stands at the cusp of this transformation, embodying the promise of AI to drive innovation, economic growth, and societal progress.

Revolutionizing Creative Industries

GenAI is poised to redefine the landscape of creative industries in the Middle East. Automating and enhancing creative processes opens up new avenues for content creation, from digital art to personalized marketing campaigns. This democratization of creativity could spur a renaissance in design, entertainment, and advertising, enabling creators to push the boundaries of imagination and reach audiences in novel and engaging ways.

Enhancing Efficiency and Innovation

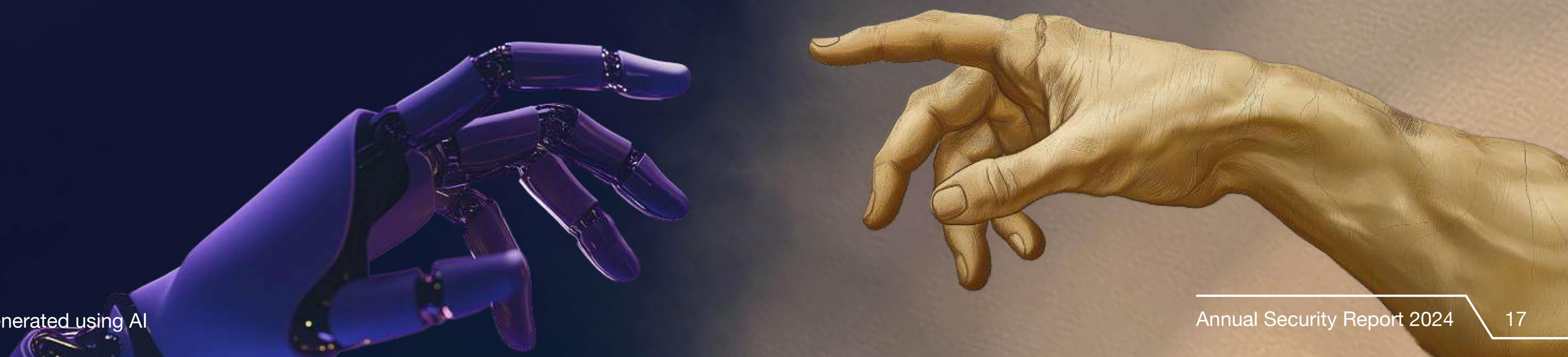
Across sectors, AI's potential to analyze vast datasets can significantly boost efficiency and foster innovation. In manufacturing, AI can predict maintenance needs, minimizing downtime and extending the lifespan of equipment. In agriculture, AI-driven insights can lead to more sustainable farming practices, optimizing water use and crop yields. These applications drive economic growth and address the world's most pressing challenges, such as food security and environmental sustainability.

Driving Economic Diversification

AI offers a strategic pathway to economic diversification for regions like the Middle East. Beyond its role in traditional sectors, AI enables new industries and innovation ecosystems to emerge. Investing in AI-driven technologies can help the Middle East diversify its economy, attract top talent from around the world, and position itself as a global hub for innovation.

Fostering Sustainable Development

Lastly, AI can contribute significantly to the Middle East's sustainability goals. Through optimization and predictive analysis, AI can help manage natural resources more efficiently, reduce waste, and enhance energy efficiency. By aligning AI applications with sustainability principles, economic growth can be driven and ensured to be environmentally responsible and sustainable over the long term.



This image has been generated using AI

THE IMPACT OF AI ON CYBERSECURITY

Integrating Artificial Intelligence (AI) into cybersecurity defenses and solutions has represented a paradigm shift in how the industry has operated for the past few decades. While automation has existed for many years, AI has the potential to take over decision-making and improve the operational efficiency of cybersecurity in a way that was impossible before. As this impact continues, the role of the **Chief Information Security Officers (CISOs)** as a guiding force in steering the adoption of AI becomes even more crucial.

This image has been generated using AI

This image has been generated using AI

Pros and Cons of AI within the Cybersecurity World

As per IBM Cost of a Data Breach Report 2024, the Middle East has remained one of the most targeted regions in the world regarding cyber-attacks. Unsurprisingly, CISOs in the region plan to increase their cybersecurity budgets in 2025 despite an overall tightening of the global economy. AI-powered cybersecurity solutions provide CISOs with a tactical edge with their ability to analyze massive datasets and proactively identify anomalies. It allows CISOs to move beyond simple playbooks and alert-based mechanisms and towards a more strategic approach to cybersecurity. As AI takes over incident response and routine cybersecurity activities with unprecedented speed, cybersecurity teams can be allocated to more complex tasks and challenges.

Similarly, AI's integration into cybersecurity extends to **DevSecOps**, where it can enhance the security posture from the earliest stages of development by automating code reviews and vulnerability scanning, seamlessly embedding security into the development lifecycle. In the domain of **risk & compliance**, AI tools can streamline the monitoring and enforcement of compliance standards, predicting risk scenarios and optimizing compliance processes with evolving regulations. This holistic integration of AI across these domains amplifies an organization's ability to defend against cyber threats. It ensures a more cohesive and agile security strategy tailored to the dynamic nature of cyber risks.

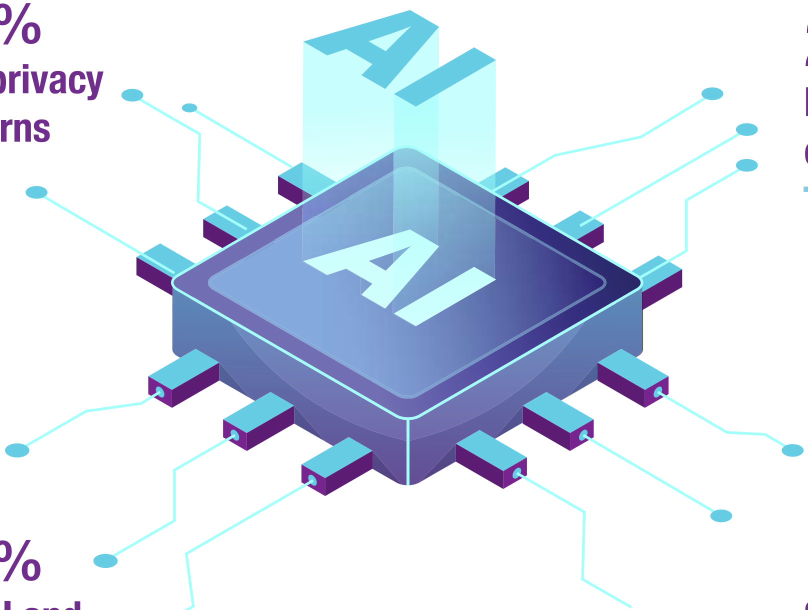
However, the landscape is full of challenges as AI increasingly integrates into cybersecurity. AI introduces new vulnerabilities that cybercriminals can exploit to influence AI algorithms and their outcomes. In the absence of a global security standard for AI systems, ensuring that AI does not become the target of sophisticated cyberattacks is becoming increasingly challenging. AI can also become a "**black box**" with no transparency to its decision-making processes, thus leading to a lack of trust, especially in regions like the Middle East, where frameworks are still being evolved.

> Organizations are grappling with multiple AI risks, with data privacy and regulatory issues taking precedence over ethical and security concerns.

Top AI Risks in 2024

31%
Data privacy concerns

27%
Regulatory and compliance risks



25%
Ethical and bias issues

17%
Security vulnerabilities

THE ROLE OF THE CISO IN INFLUENCING THE FUTURE OF AI

Due to their roles as senior decision-makers, CISOs stand at the intersection of AI and Cybersecurity. While it is typically the business side that drives the adoption of AI technologies to achieve competitive advantage and operational efficiency, the role of the CISO is crucial in ensuring that robust cybersecurity measures underpin this adoption. As digital transformation accelerates across the Middle East, the role of CISOs is evolving; they are no longer solely focused on technology but have become key partners in the strategic implementation of AI.

Some of the key strategic activities that CISOs can undertake are:

1

Establish robust governance frameworks

for the ethical and secure use of AI within their organizations. Typically, CISOs are looked to for advice regarding governance and compliance initiatives, and they have a unique opportunity to influence safe and secure AI adoption within organizations. Setting frameworks that mandate trust, security, and transparency will empower organizations to embrace AI without decreasing their security postures.

2

Improve collaboration

between government entities, private sector organizations, and academia to advance and improve research in AI Security. CISOs can leverage their unique position to bridge gaps between these entities and create initiatives for advancing AI-based cybersecurity. This will cement the Middle East as a benchmark for AI adoption and innovation.

3

Liaise with the Chief Artificial Intelligence Officer (CAIO)

to ensure alignment between AI strategies and cybersecurity policies. This collaboration enables a harmonious approach to adopting AI technologies, where the CAIO's insights into AI potential and applications are balanced with the CISO's expertise in risk management and cybersecurity. By working together, CISOs and CAIOs can drive forward AI initiatives that are not only innovative but also secure and compliant with existing and emerging cybersecurity standards.

This image has been generated using AI

This image has been generated using AI

GBM

As the Middle East navigates the complexities of this new AI-driven world, the role of the CISO is pivotal in harnessing AI as a positive force while mitigating its unique challenges. The leadership and foresight that CISOs bring will power the region toward a secure and resilient future driven by AI.

How does your Chief Artificial Intelligence Officer (CAIO) influence the strategic integration of AI within your organization?

28% Ensuring alignment of AI with business goals

40% No CAIO appointed

Despite AI’s growing importance, 45% of organizations lack a Chief AI Officer, signaling a critical gap in leadership and governance for aligning AI with business goals.

12% Setting and guiding the overall AI vision and strategy

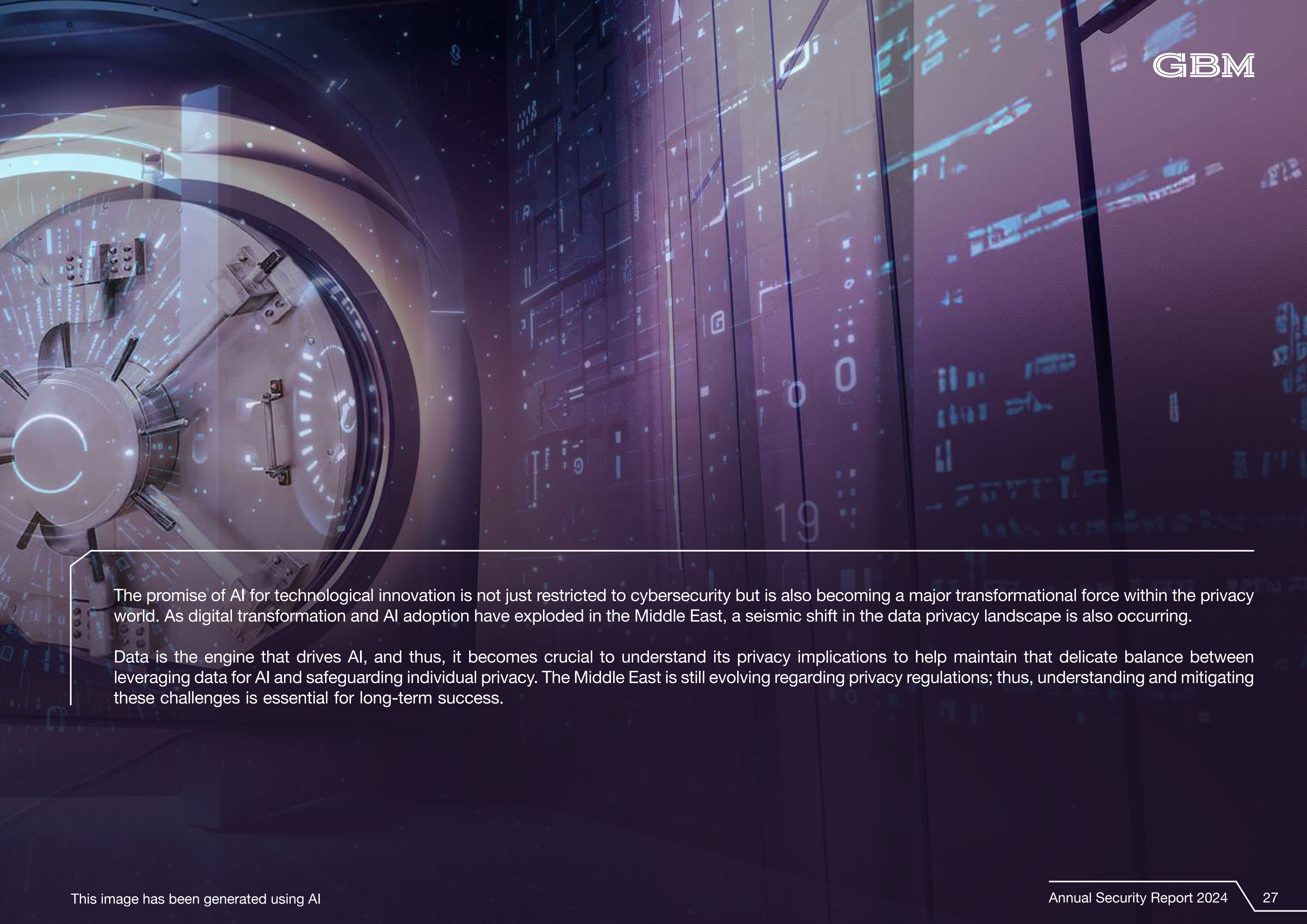
15% Leading AI governance, ethics, and compliance efforts

5% Fostering cross-departmental collaboration for AI projects

GBM

BALANCING AI INNOVATION WITH PRIVACY CONCERNS

This image has been generated using AI



The promise of AI for technological innovation is not just restricted to cybersecurity but is also becoming a major transformational force within the privacy world. As digital transformation and AI adoption have exploded in the Middle East, a seismic shift in the data privacy landscape is also occurring.

Data is the engine that drives AI, and thus, it becomes crucial to understand its privacy implications to help maintain that delicate balance between leveraging data for AI and safeguarding individual privacy. The Middle East is still evolving regarding privacy regulations; thus, understanding and mitigating these challenges is essential for long-term success.

This image has been generated using AI

Challenges in Data Privacy Influenced by AI and Digital Transformation

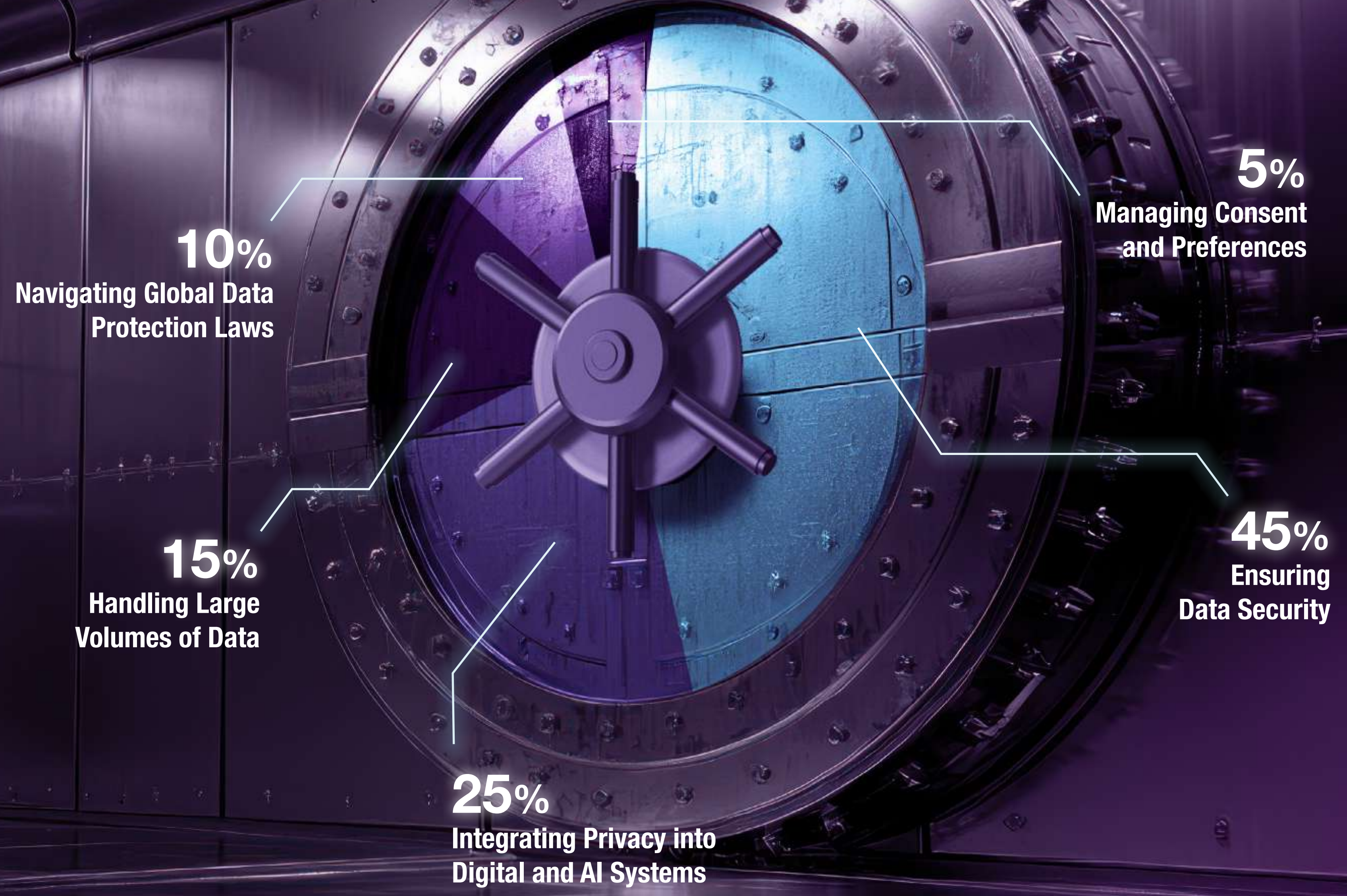
A key privacy challenge that emerges with AI adoption is the massive amount of data needed for AI models and platforms to function effectively. This inevitably involves storing personal information and introducing new privacy challenges, such as breaches and compliance violations. Additionally, AI-powered decision-making fueled by the collection of personal data has the potential to profile and discriminate against individuals, leading to ethical concerns. Concerns around profiling and automated decision-making raise questions about AI systems' fairness, transparency, and accountability.

The cross-border flow of data is another complex challenge due to the fragmented nature of privacy regulations within the Middle East. Organizations planning to utilize AI for cross-border purposes must comply with a patchwork of legal and privacy obligations to remain compliant and protect user privacy.

> **The top concern for organizations is securing data amidst digital transformation, with nearly half struggling to embed privacy protections into their AI systems and manage the vast volumes of data generated.**

This image has been generated using AI

Biggest Data Privacy Challenges with AI and Digital Transformation



This image has been generated using AI

GBM

ETHICAL AI USAGE AND PRIVACY PROTECTIONS

The ethical usage of AI within privacy is based on the three foundational pillars of consent, transparency, and minimization. It is essential to consider these pillars around all AI initiatives in the Middle East:

Consent

The core of privacy revolves around informed consent, i.e., the individual agreeing to collect and use their data. AI systems must ensure that the individuals whose data is being used are fully aware of and can control the consent around their data usage. Organizations must set down clear communication around how AI systems will use data, the scope of its usage, and how individuals can opt out of this process. As AI adoption grows along with privacy awareness, organizations must work to create more awareness around consent mechanisms, especially within the context of AI.

Transparency

Privacy does not end with consent; transparency is another core tenet of responsible AI. Organizations collecting data for AI usage must ensure the algorithms, decision-making processes, and data sources are disclosed to their customers. Trust will directly influence the level of AI adoption by the public; hence, it is crucial to use transparency to demystify AI and assure users about how their data will be ethically used.

Minimization

Ensuring that the level of data being collected is restricted only to the minimum needed is a crucial challenge, especially within the context of AI. The efficiency of AI directly depends on the quantity and quality of the data collected, and organizations may exceed the boundaries of what is needed when gathering this information. Enforcing data minimization practices will prevent privacy violations and help organizations navigate the delicate balance between empowered AI and fostering public trust.

THE RESPONSIBILITY OF DATA PROTECTION OFFICERS IN THE NEW LANDSCAPE

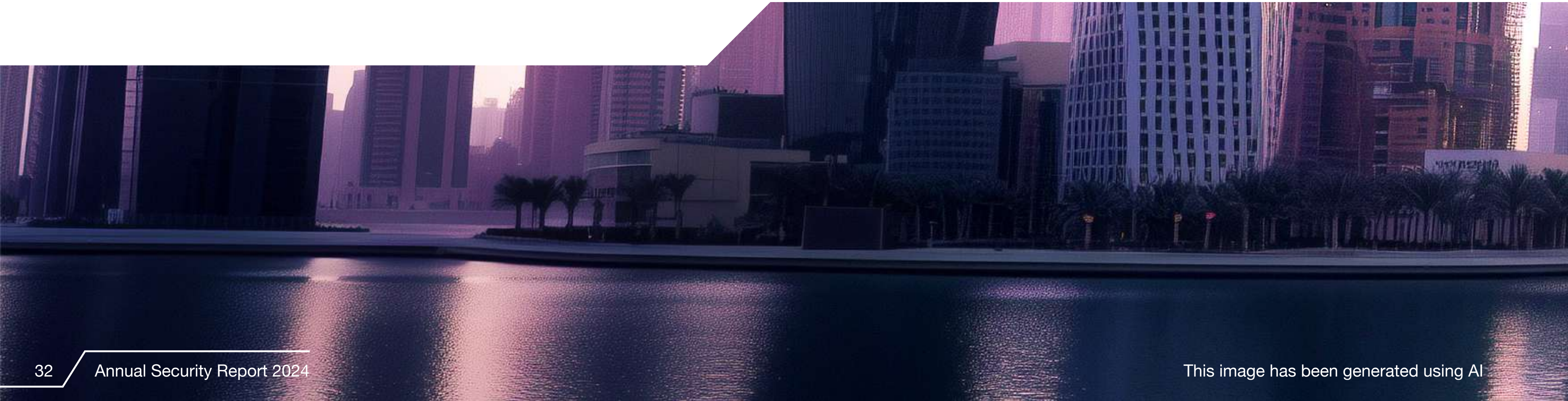
The appointment of a **Data Protection Officer (DPO)** is often the first step in establishing a data privacy program in any organization. DPOs are the single point of contact for all privacy-related issues and are thus at the forefront of addressing these new AI-related challenges.

The role of the DPO in the new AI age will evolve to become more strategic and extend beyond the borders of mere compliance. DPOs like CISOs will have to shape AI policies actively to standardize the new landscape.

The privacy landscape in the Middle East is evolving rapidly, with new regulations being introduced to align with global standards. The EU AI Act, the world's first comprehensive AI law, has already taken effect on August 1, 2024. It will no doubt have a similar impact to how GDPR transformed data privacy practices. DPOs must ensure these regulations and global frameworks are translated into organizational policies that help create a culture of data privacy for all AI initiatives.

Additionally, DPOs must play a key role in embedding privacy by design principles in all AI initiatives. By ensuring privacy is integrated into the fabric of AI systems, they can mitigate the risks of data leakage and non-compliant data collection. Guidelines on how data is collected, used, stored, and protected within AI must be set down and communicated to foster a culture of transparency and trust among customers and regulatory bodies.

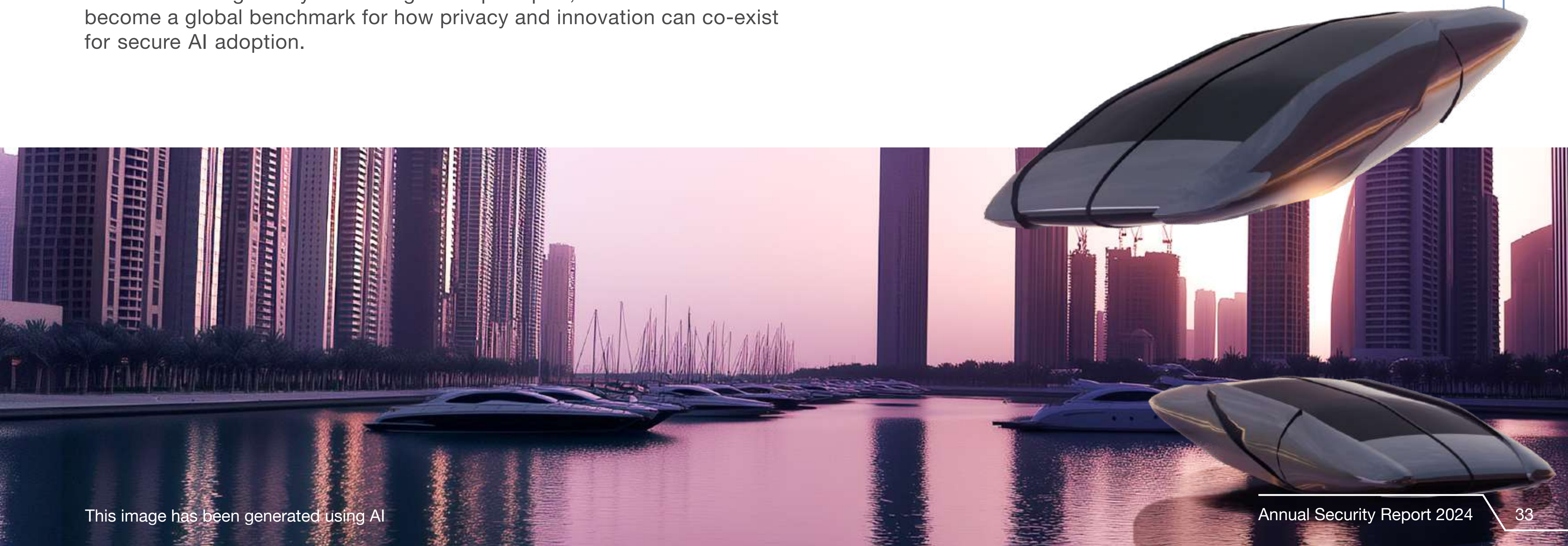
These are just some of the many privacy challenges that DPOs must prepare themselves for in the age of AI. These challenges are difficult but manageable



This image has been generated using AI

as long as the right governance frameworks are implemented. DPOs are crucial in guiding organizations and regulatory bodies in the Middle East through this new landscape by championing a culture of data privacy and ethical data collection practices.

AI presents unprecedented privacy and ethical challenges as the Middle East progresses in its digital transformation journey. DPOs must prioritize principles such as **consent, transparency**, and **data minimization** to empower the region to embrace the full potential of AI while upholding privacy values and individual rights. By embracing these principles, the Middle East can become a global benchmark for how privacy and innovation can co-exist for secure AI adoption.



This image has been generated using AI

A FRAGMENTED REGULATORY LANDSCAPE

The intersection of Artificial Intelligence (AI) and Cybersecurity / Privacy is characterized by a complex mesh of regulations that can become quite challenging to navigate. Countries in the Middle East have adopted differing approaches to regulating and controlling AI, which requires a nuanced approach to understanding the regulatory frameworks in place.

Another challenge is the rapid rate of innovation in the region that often outpaces the development of mature regulatory frameworks. This report section aims to demystify some major AI and Cybersecurity regulations and how CISOs and DPOs should approach them. We will focus on regional programs like the DESC CSP Standard and the Dubai Cyber Force Program, along with international releases like the NIST AI Framework, EU AI Act, and ISO 42001.

Regional Standards, Regulations and Related Developments

The Dubai Electronic Security Center (DESC) CSP Standard and the Dubai Cyber Force Program highlight the Middle East's proactive cybersecurity and data protection approach. These initiatives aim to bolster the emirate's digital infrastructure, ensuring robust protection against cyber threats and enhancement of data privacy. The DESC CSP Standard sets stringent cybersecurity protocols, while the Dubai Cyber Force Program fosters a resilient cyber defense ecosystem, both crucial for the trustworthy deployment of AI technologies.

Additionally, the Dubai International Financial Centre (DIFC) has amended its data protection regulations to ensure that DIFC companies' AI systems follow the principles of transparency, ethical use, fairness, and security that we discussed earlier. This is a great stride forward in bringing the UAE in line with upcoming international regulations like the EU AI Act.

Along with the UAE, the Saudi Data and Artificial Intelligence Authority (SDAIA) issued the final version of its AI Ethics Principles, representing the first AI legal framework in the Kingdom. These developments showcase the rapid pace at which regulations are being launched to ensure the Middle East remains a forward-thinking region for AI adoption.

Following this trend, the Oman Personal Data Protection Law introduced detailed regulations for processing personal data in Oman, ensuring transparency, fairness, and accountability amidst the AI boom. This is a crucial step in ensuring that Oman's digital landscape remains secure and respectful of privacy rights amidst rapid technological advancement. Similarly, the United Arab Emirates has enacted the Protection of Personal Data Protection Law (PDPL), a comprehensive legal framework designed to safeguard individuals' privacy and enhance data security nationwide.

The Kuwait Data Privacy Protection Regulation (DPPR) imposes obligations on data controllers and processors to protect individuals' privacy rights and maintain data security within Kuwait's digital landscape, adapting to the increased integration of AI systems. In Bahrain, the Personal Data Protection Law regulates the processing of personal data to safeguard privacy rights and enhance data security. It addresses the implications of AI integration and data-driven decision-making. Compliance with these laws will be essential for organizations to navigate the complexities of AI adoption while upholding privacy standards and mitigating potential risks associated with AI technologies.

Lastly, Qatar's Personal Data Protection Law highlights Qatar's dedication to protecting privacy rights and securing data within the evolving digital domain. As AI technologies continue to reshape industries and societies across the Middle East, these laws must evolve to ensure that individuals' privacy rights are protected, ethical considerations are addressed, and AI systems operate within the bounds of legal and ethical frameworks.

1

EU AI Act and the NIST AI Risk Management Framework (RMF)

The EU AI Act, with its risk-based classification system for AI applications, sets a historic precedent for regulatory approaches worldwide, including implications for Middle Eastern entities engaging with EU markets. It is expected to have the same global impact on AI as the GDPR had on data privacy. The AI act will provide AI deployers, providers, and developers with a clear risk-based approach towards AI systems, depending on their use. By adopting local regulations derived from the provisions of the standard, the Middle East can take a proactive approach to ensuring alignment with the act once it is released.

Similarly, the National Institute of Standards and Technology (NIST) released the NIST AI Risk Management Framework to define a framework for the governance, management, and mitigation of AI-related risks. Like the EU AI Act, we expect the NIST AI RMF to become an industry standard similar to their earlier publications, such as the NIST Cybersecurity Framework (CSF). The Framework provides a flexible approach to managing AI risks, encouraging innovation while ensuring ethical considerations.

2

ISO 42001 AI Management System

Another significant milestone in the AI governance landscape was the release of the ISO/IEC 42001 Standard by the International Standard Organization (ISO). Heralded as the world's first AI Management System (AIMS), it aims to help organizations mitigate the risks and challenges of AI by implementing a management system framework similar in fashion to existing standards like ISO/IEC 9001 for quality and ISO/IEC 27001 for Information Security. The ISO standards are well regarded within the Middle East region. We can expect ISO/IEC 42001 to become an increasingly popular way for companies to demonstrate compliance with AI best practices.

3

Google SAIF and MITRE ATLAS

While helpful, the previously mentioned frameworks and regulations can sometimes be too high-level and do not provide the technical granularity that CISOs require. This is where Google's Secure AI Framework (SAIF) and MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATLAS) can prove extremely useful.

In Google's words, SAIF provides *"a framework for creating a standardized and holistic approach to integrating security and privacy measures into ML-powered applications."* It aligns with the 'Security' and 'Privacy' dimensions of building AI responsibly. This framework can be used on top of MITRE ATLAS, which provides a knowledge base for understanding and defending against AI-specific threats. These initiatives are particularly relevant for Middle Eastern organizations seeking to align with international AI security and privacy best practices.

4

Gartner AI TRISM

In the context of evolving AI governance, Gartner's AI TRISM (Trust, Risk, and Security Management) stands out as a crucial framework for 2025, emphasizing the importance of trust, risk management, and security in AI applications. This framework ensures AI technologies are developed and implemented responsibly, focusing on transparency, fairness, and privacy. AI TRISM highlights the need for organizations to establish trust in AI systems through interpretability and accountability, identify and mitigate AI-specific risks, and enforce robust security measures to protect against cyber threats and data breaches. By advocating for the analysis of AI models for biases and ensuring their effectiveness and efficiency, AI TRISM complements existing standards like the EU AI Act and NIST AI RMF, offering a comprehensive approach to navigating the complex landscape of AI governance.

In conclusion, the intricate landscape of Artificial Intelligence (AI), cybersecurity, and privacy within the Middle East presents a dynamic and challenging environment that demands a sophisticated understanding of regional and international regulatory frameworks. Adopting these frameworks and standards will foster a secure, trustworthy, and ethically aligned digital future as the Middle East continues to forge ahead in AI innovation.

FACING THE NEW CYBERSECURITY AND PRIVACY LANDSCAPE:

A COLLABORATIVE APPROACH

As we conclude our report, it is clear that the cybersecurity and privacy landscape is undergoing a profound transformation driven by AI. Along with advanced cyber-threat powered and data privacy challenges, the AI regulatory environment is also becoming a challenging maze to navigate.

Navigating this new world requires a collaborative approach to cybersecurity and privacy where CISOs and DPOs can play a crucial leadership role. A siloed approach will no longer work, and instead, a collaborative approach between enterprises, government, academia, and technology providers is needed to create a secure AI-driven future. This section delves deep into how this collaboration may look, focusing on strategies relevant to the Middle East.

Strategic Partnerships between Governments and Enterprises

Governments and enterprises in the Middle East must forge strategic partnerships to develop and implement robust cybersecurity frameworks that address the unique challenges posed by AI. These partnerships can facilitate the sharing of threat intelligence, enhance regulatory compliance, and drive the adoption of best practices. For instance, government-led initiatives can provide enterprises with the necessary guidance and support to navigate the complex regulatory environment. In contrast, enterprises can contribute to shaping policies that foster innovation and security in equal measure. CISOs and DPOs can facilitate these partnerships and drive the conversation forward between the two entities.

Engaging Technology Providers and Academia

Technology providers are typically at the forefront of developing AI-driven cybersecurity solutions. Their collaboration with both governments and enterprises is crucial for the deployment of advanced security technologies that are tailored to the specific needs of the region. Furthermore, academia plays a pivotal role in advancing cybersecurity research and innovation. Collaborative research projects, public-private partnerships, and academic-industry consortia can accelerate the development of cutting-edge cybersecurity technologies and effective strategies against AI-powered threats.

Strategies for Fostering Collaboration

To evolve cybersecurity measures effectively, the Middle East can look to the following key strategies:

1 Establishing Cyber Security Alliances

Regional cybersecurity alliances can facilitate cooperation among Middle Eastern countries, enabling the sharing of threat intelligence, resources, and best practices. These alliances can also serve as platforms for coordinating responses to cross-border cyber threats.

2 Promoting Public-Private Partnerships (PPPs)

PPPs can bridge the gap between government objectives and private sector capabilities, fostering the development of resilient cybersecurity infrastructures. These partnerships can also drive the co-creation of cybersecurity solutions that address the region's unique challenges.

3 Creating Innovation Hubs

Establishing cybersecurity innovation hubs in collaboration with academia and industry can spur the development of AI-driven cybersecurity technologies. These hubs can also serve as cybersecurity training and education centers, building the region's talent pool.

4 Enhancing Legal and Regulatory Frameworks:

Collaborative efforts to enhance legal and regulatory frameworks can ensure that cybersecurity measures keep pace with technological advancements. This involves updating data protection laws, cybersecurity regulations, and compliance standards to address the risks associated with AI. Frameworks like the NIST AI RMF, EU AI Act, and ISO 42001 can be pivotal in establishing trustworthy AI and ensuring privacy, guiding the region towards a future where technology and regulation harmoniously coexist.

Shared intelligence and cross-sector cooperation are leading strategies for organizations looking to fortify cybersecurity. The growing focus on international standards and joint R&D also underscores the need for global alignment and innovation in addressing cybersecurity challenges.

Top Strategies for Fostering Collaboration in Cybersecurity

Strategy	Share
Shared Threat Intelligence Platforms	32%
Cross-sector Cybersecurity Frameworks	23%
Public-Private Partnerships	24%
International Cybersecurity Standards	13%
Joint Research and Development Projects	8%

Call To Action For CISOs

As enterprises continue integrating AI into their operational fabric, the role of CISOs becomes increasingly crucial. They are not only guardians of cybersecurity but also visionaries who must harness AI's potential to fortify their organizations against emerging cyber threats. Drawing from the insights and strategies discussed, here are actionable steps that CISOs can undertake within their enterprises to leverage AI effectively:

Educate and Train on AI Security Ethics and Compliance

As AI becomes a central pillar in cybersecurity strategies, ensuring that AI systems are used ethically and in compliance with regulatory standards is paramount. CISOs should lead educational initiatives within their organizations to highlight the importance of ethical AI use, focusing on data privacy, bias avoidance, and compliance with regional and international frameworks like the NIST AI RMF and EU AI Act.

This image has been generated using AI

Integrating AI with Security Operations

CISOs can leverage AI for boosting the productivity of their security operations via the following

Integrate AI for Proactive Threat Intelligence

CISOs should incorporate AI-driven analytics to sift through the vast landscapes of data their organizations generate. By applying AI to detect patterns and anomalies, they can preemptively identify potential threats before they escalate. Actionable steps include selecting AI tools that offer real-time data analysis and threat intelligence and integrating these solutions into the existing cybersecurity framework.

Foster AI-driven Security Automation

Automating routine security tasks with AI boosts efficiency and frees the cybersecurity team to focus on strategic issues. CISOs should identify processes that can be automated, such as patch management or user behavior analysis, and deploy AI tools to manage these tasks. This approach ensures a dynamic and adaptive security posture.

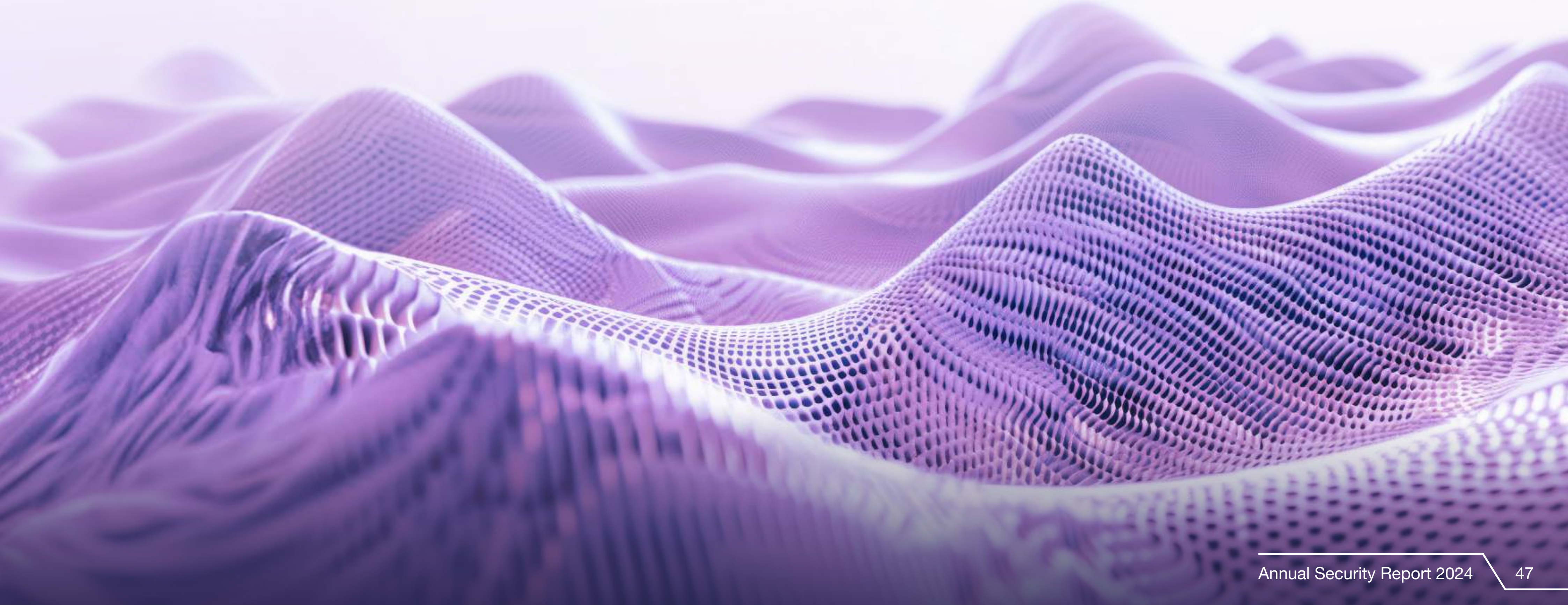
Leverage AI for Enhanced Incident Response

In a security breach, AI can provide rapid response capabilities by analyzing the attack vectors and suggesting containment strategies. CISOs can implement AI-driven incident response systems to reduce downtime and mitigate the impact of breaches. Establishing protocols for AI-assisted decision-making in crises is a critical step in this process.

Setting up AI Governance

Establishing a robust AI governance framework is crucial for ensuring that AI systems are transparent, accountable, and aligned with the enterprise's broader goals and ethical standards. CISOs should work to define clear governance policies that include oversight mechanisms, regular audits, and updates to AI strategies as technology and regulatory landscapes evolve. This governance will help manage risks associated with AI deployment and ensure sustained alignment with organizational values and compliance requirements.

By adopting these strategies, CISOs elevate their organization's security infrastructure and contribute to establishing a secure, AI-driven future.



KEY TAKE AWAYS

In conclusion, the GBM Security Report 2024 has traversed the multifaceted landscape of artificial intelligence (AI), cybersecurity, and privacy, particularly within the dynamic context of the Middle East. The report underscores AI's transformative potential in driving innovation and economic growth while highlighting the cybersecurity and privacy challenges accompanying its widespread adoption. As we've explored, integrating AI into various sectors offers tremendous opportunities, introduces new vulnerabilities, and necessitates a nuanced approach to regulation and ethical use.

The report emphasizes the critical need for a collaborative approach to cybersecurity and privacy involving key stakeholders such as Chief Information Security Officers (CISOs), Chief Privacy Officers (CPOs), government entities, academia, and technology providers. By forging strategic partnerships and engaging in public-private collaborations, the region can develop robust frameworks to address the unique challenges posed by AI and ensure a secure digital future.

As CISOs navigate this evolving landscape, the pivotal role of AI in enhancing threat detection, automating security processes, and driving efficient incident response has been highlighted. However, with great power comes great responsibility, and the ethical deployment of AI technologies, adherence to regulatory standards, and privacy protection remain paramount.

This image has been generated using AI

In light of these discussions, one pragmatic step for CISOs seeking to harness AI's potential within their cybersecurity and privacy strategies is to engage with trusted advisors and industry experts. These partnerships can be invaluable in developing tailored use cases for AI that align with the organization's specific needs, challenges, and strategic goals. Working with companies that serve as trusted advisors can provide CISOs with the expertise and insights needed to effectively navigate the complexities of integrating AI into their cybersecurity and privacy frameworks.

By leveraging such collaborations, CISOs can ensure their AI initiatives are innovative and grounded in best practices for security and privacy. This approach allows for the responsible and ethical use of AI, fostering trust among stakeholders and paving the way for a future where technology enhances security, privacy, and efficiency in equal measure.

The journey toward a secure, AI-driven future is ongoing, and the insights provided in this report serve as a guide for technology leaders looking to navigate this terrain. AI's potential to transform cybersecurity and privacy practices is immense, but realizing this potential requires careful planning, collaboration, and a commitment to ethical principles. By embracing these strategies, CISOs and their organizations can create a secure and prosperous digital era.

This image has been generated using AI

GBM

Authors

Hasanian Alkassab

Director, Security Business Unit
GBM

Akhtar Rasool

Chief Security Architect
GBM

For more information, please reach out to:

Swathi Ravindran
Alliance Marketing Manager

marhaba@gbmme.com

To find out more, visit:
www.gbmme.com

Research Methodology and Disclaimer

The findings and insights presented in the GBM Shield Annual Security Report 2024 are based on research conducted by GBM through an online survey administered to our database of respondents. 500 enterprise businesses were surveyed across 4 markets.

United Arab Emirates (UAE) **Kuwait** **Oman** **Bahrain**

Fieldwork Period: August 2024

The data reflects the perspectives and experiences of organizations within these regions concerning their adoption and management of AI technologies, as well as the associated benefits and challenges. While the report provides valuable insights, the findings should not be interpreted as definitive or exhaustive, as they represent a snapshot in time based on the responses of participants within GBM's network.

All survey responses were collected and analyzed anonymously, ensuring that no personal or sensitive data from individual respondents was disclosed or shared. The information contained in this report is for informational purposes only, and GBM assumes no responsibility for the actions taken based on the results of this research.

About GBM

With more than 30 years of experience, 7 offices, and over 1500 employees across the region, Gulf Business Machines (GBM) is a leading end-to-end digital solutions provider, offering the region's broadest portfolio, including industry-leading digital infrastructure, digital business solutions, security, and services. We have nurtured partnerships since 1990 with the world's leading technology companies and invested in a talented, skilled workforce to implement solutions that cater to customer's specific, complex, and diverse business needs.

Some of our strategic partners in the Gulf include IBM as their sole distributor throughout the GCC (excluding Saudi Arabia and selected IBM products and services) and Cisco as a Gold and Master Partner (the highest level of certification at Cisco).

GBM
Emarat Atrium Building, Block B, 3rd floor,
Sheikh Zayed Road, P.O. Box 9226, Dubai, UAE
www.gbmme.com


GBM