MENA Cyber Summit
2025 Annual Report_

#MENA
CYBER SUMMIT

Issued December 2024

Executive **Summary_**

Welcome to the State of Cyber Security in the MENA Region 2024 Annual Report. For each edition of our regional Cyber Security summits, a report like this one is produced, exploring the themes and topics of each region covered by its respective annual in-person event. This report looks in-depth at several key topics and trends relevant to both IT cyber security professionals from across industries in the Middle East and Northern Africa, including exclusive interviews with the region's leading CISOs and security leaders.

The theme of our 2025 edition of the event is "Getting the Cyber Security Basics Right Whilst Accelerating Future Innovation." This is essential to discuss when overcoming issues in cyber security, as we need to ensure we have the correct people, processes, and technology strategies in place through our organisations, hence getting the basics right. Consequently, this theme ensures that we can overcome challenges in each of these areas in the short, medium, and long term while overcoming common cyber security issues faced in the region and new challenges brought by an expanding threat landscape, new regulations, and challenges that are unique to the Middle East and Northern Africa itself. Subsequently, this report will explore how CISOs and other practitioners can address them through a security lens and look towards the future to see how we can best ensure our organisations stay secure moving into 2025 and beyond.

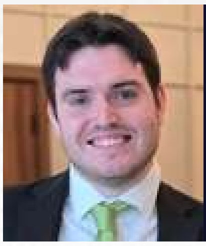
Hence, our goal through our articles and events is to provide the top cyber security experts in the area with a platform to share their knowledge and gain insight from others in order to improve cyber security against threat actors.

We hope you find the contents of the report thought-provoking and exciting. Feel free to get in touch with us at info@qgmedia.io if you have any questions or would like further elaboration on anything in the report

Content Subscription_

For more cyber security insights, interviews and reports, click to subscribe below:

SUBSCRIBE NOW



Annual report written by:
Josh Cunningham-Marsh
CS4CA MENA 2025
Programme Manager
Contact: josh@qgmedia.io

Table of Content_

SECTION	CONTENT TITLE	PAGE
01	*The MENA Region Cyber Security Threat Landscape*	04
02	*Threat Briefing*	09
03	*Part 1: Dissecting the Cyber Security Issues of Today - Third Party Risk and Geopolitical Factors*	13
04	*Part 2: Adapting to Regulations Throughout the Middle East*	20
05	*Part 3: Discussing the Threats Opened by New Technologies*	26
06	*Part 4: Building a Holistic Cyber Security Strategy*	33
07	*Conclusion & Further Readings*	40

Cyber Security Threat Landscape_

A Snapshot of the MENA Region_

The **Middle East** and **Africa** faced a **surge in cyber threats** in **2023**, with a **68% increase** in **ransomware attacks**, illustrating the necessity of being prepared against cyber criminals.

In **2023**, the **Middle East** ranked among the **top 5 regions** with the **highest percentage** of **malware** blocked in **industrial control systems** (ICS), with attacks on **government, services, manufacturing**.

Meanwhile, **Middle East oil & gas operators** will need to be vigilant about the **risk of cyber attacks** as the **Israel-Gaza conflict** continues, security experts warn, or else risk **energy supply disruption** globally.

51%

51% of **Middle East** respondents cite **lack of funding** as the **top challenge** for **managing cyber security**, compared to **36%** **globally**

52%

52% of **Middle East** respondents said that **cyber security impacts the success** of **digital transformation** to a large extent

69%

69% of **Middle East** respondents said that offering **training** and **certification programs** is key to **engaging, retaining**, and **developing cyber talent**

393 DAYS

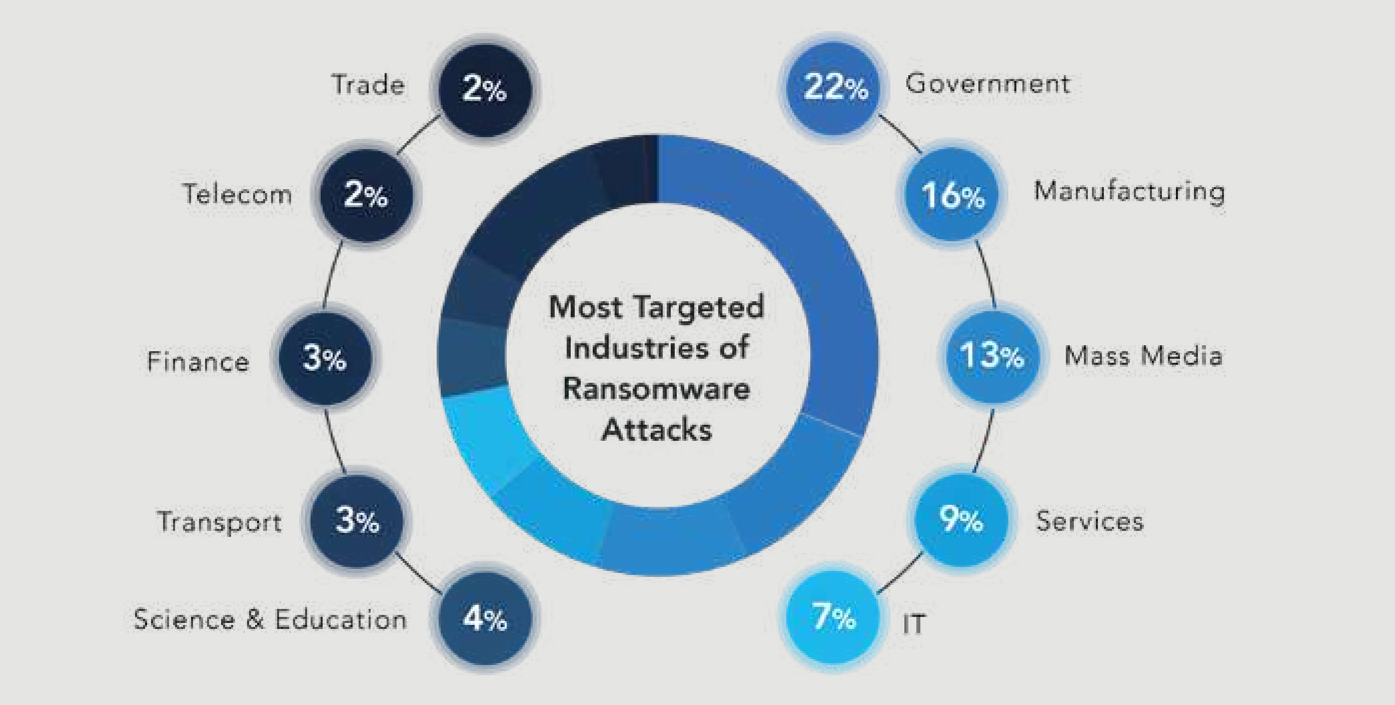
The average **data breach resolution lifecycle** in the **Middle East** spans **393 days**, surpassing the **global average** by **40%**

$8.7M

The **cost of cyber security incidents** in the **Middle East** is **$8.75 million per data breach** (global average cost of $4.88 million per incident)

In 2024, spending on data privacy in MENA is expected to experience the highest growth rate among all segments, surging by 24 percent year-over-year, while cloud security spending is forecast to witness a robust increase of 17.4 percent. This is because an uptick in the use of GenAI will cause a spike in the cyber security resources required to secure it.

Most Targeted Industries By Cyber Attackers



Prominent Cyber Attacks on The MENA Region's Critical Infrastructure_

1 Crowdstrike Outage

When: July 2024

A faulty software update for Microsoft Windows issues by cyber security firm CrowdStrike caused a global IT outage that disrupted airline and hospital operations. It affected approximately 8.5 million machines and cost Fortune 500 companies $5.4 billion, according to reports. A number of airlines at King Khalid International Airport in the Saudi capital Riyadh were affected, while airlines in Morocco and Lebanon were also affected. Despite this, the UAE Cyber Security Council has confirmed no indications of cyber attacks or breaches following the global technical outage with CrowdStrike software that affected electronic systems across various strategic sectors worldwide.

2 Israeli Nuclear Instillation by Iranian Hackers

When: March 2024

An Iran-linked hacking group claims to have breached the computer network of a sensitive Israeli nuclear installation in an incident declared by the 'Anonymous' hackers as a protest against the war in Gaza. This is as geopolitical tensions in the region have skyrocketed since October 7th and Hamas' attack on Israel and the Israeli government's subsequent response in Gaza, leading to the deaths of thousands of Palestinian civilians. The hackers claim to have stolen and published thousands of documents—including PDFs, emails, and PowerPoint slides—from the Shimon Peres Negev Nuclear Research Center. In a social media message explaining their intentions, the group claimed, "As we are not as bloodthirsty as the bloodthirsty Netanyahu and his terrorist army, we carried out the operation in such a way that no civilians were harmed." While the documents that were released suggest the hackers were able to compromise an IT network connected to the facility, there is no evidence they have been able to breach its OT network.

3 Israeli-linked Hackers Target Iran's Gas Stations

When: December 2023

Israeli-linked hackers disrupted approximately 70% of gas stations in Iran. Hackers claimed the attack was in retaliation for aggressive actions by Iran and its proxies in the region, with Hamas seen as one of these proxies. A group called Gonjeshke Darande, meaning Predatory Sparrow in Persian, claimed it was behind the attack, stating, "We, Gonjeshke Darande, carried out another cyberattack today, taking out a majority of the gas pumps throughout Iran. This cyberattack comes in response to the aggression of the Islamic Republic and its proxies in the region," and Iran's leader, Ayatollah Ali Khamenei, said, "Khamenei, playing with fire has a price." Pumps restored operation the next day, but payment issues continued for several days. Nevertheless, this again highlights the nature of cyberwarfare, with critical infrastructure being a key element of modern warfare today.

4 Iranian Hackers Attack Israel's Rail Network

When: September 2023

Iranian hackers launched a cyberattack against Israel's railroad network. The hackers used a phishing campaign to target the network's electrical infrastructure. Brazilian and UAE companies were also reportedly targeted in the same attack.

5 Iranian hacking group targets U.S. entities

When: April 2023

Iranian state-linked hackers targeted critical infrastructure in the U.S. and other countries in a series of attacks using previously unseen customised dropper malware. The hacking group has been active since at least 2014, conducting social engineering and espionage operations that support the Iranian government's interests.

6 Iranian Hackers Leak Saudi Government Data

When: December 2022

The Iran-linked advanced persistent threat (APT) actor known as Moses Staff is leaking data stolen from Saudi

Arabia's government ministries using a recently created online persona, Abraham's Ax. Consequently, Iran-linked hackers obtained and leaked data from government ministries in Saudi Arabia. The group is often linked to anti-Israel and pro-Palestinian activities. However, rather than attacking Israel directly, Abraham's Ax attacks government ministries in Saudi Arabia. This may be in response to Saudi Arabia's leadership role in improving relationships between Israel and Arab nations.

7 Data Leak From Saudi Arabia Government

When: December 2022

The Iran-linked advanced persistent threat (APT) actor known as Moses Staff is leaking data stolen from Saudi Arabia's government ministries using a recently created online persona, Abraham's Ax. Consequently, Iran-linked hackers obtained and leaked data from government ministries in Saudi Arabia. The group is often linked to anti-Israel and pro-Palestinian activities. However, rather than attacking Israel directly, Abraham's Ax attacks government ministries in Saudi Arabia. This is because the group may be attacking Saudi Arabia in response to Saudi Arabia's leadership role in improving relationships between Israel and Arab nations.

8 Data Leak at Saudi Aramco

When: 2021

The world's most valuable oil producer, Saudi Aramco, had its company data leaked from one of its contractors. The files were used in an attempt to extort $50m (£36.5m) from the company. The attack originated in the supply chain, with the company commenting that "we confirm that the release of data was not due to a breach of our systems, has no impact on our operations, and the company continues to maintain a robust cyber security posture,". According to the Associated Press, one terabyte of Aramco's data was being held by extortionists, citing a page on the darknet, a part of the internet within an encrypted network that is accessible only through specialised anonymity-providing tools.

9 Healthcare Entities Targeted by Xing Team

When: December 2022

Some threat actors have gained a lot of notoriety, while others are less known. The "Xing Team." maintains a dedicated leak site. On that leak site were three large data dumps from three different medical and healthcare entities—ttwo in the U.S. and one in Saudi Arabia. The Xing Team claims to have acquired patient data, employee data, and financial reports from GlobeMed Saudi, a healthcare benefits management firm. Saudi Arabia does not seem to have a clear data protection regime of regulations, but there does seem to be a duty to protect patient information. GlobeMed did not answer this site's question about whether it would be notifying patients or how it was responding to this incident.

10 Ransomware Attack at Moorfields Eye Hospital

When: 2021

The ransomware group AvosLocker attacked Moorfields Eye Hospital Dubai in 2021 and successfully downloaded over 60 GB of data that was stored on its servers, including copies of ID cards, accounting documents, call logs, and internal memos. The attackers then encrypted the original information and demanded a ransom, threatening the hospital to leak it if it was not paid. Moorfields Eye Hospital Dubai determined that the ransomware that encrypted its data was either sent in an email or distributed via a malicious ad. As unfortunate as it is, ransomware attacks on hospitals and other healthcare providers are fairly common. Luckily, this particular attack didn't paralyse any critical systems whose unavailability would endanger patients' lives.

11 Sadara Chemical Company Attack

When: 2017

In August 2017, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyberattack. The attack was not designed to simply destroy data or shut down the plant; it was meant to sabotage the firm's operations and trigger an explosion. The attack was a dangerous escalation in international hacking, as faceless enemies demonstrated both the drive and the ability to inflict serious physical damage. Consequently, in January 2017, computers went dark at the National Industrialisation Company, or Tasnee for short, which is one of the few privately owned Saudi petrochemical companies. Computers also crashed 15 miles away at Sadara Chemical Company. Within minutes of the attack at Tasnee, the hard drives inside the company's computers were destroyed and their data wiped clean, replaced with an image of Alan Kurdi, the small Syrian child who drowned off the coast of Turkey during his family's attempt to flee that country's civil war. The intent of the January attacks was to inflict lasting damage on the petrochemical companies and send a political message. The recovery took months. All of the investigators believe the attack was most likely intended to cause an explosion that would have killed people.

So how did the hackers get in? Investigators found an odd digital file on a computer at an engineering workstation that looked like a legitimate part of the Schneider controllers but was designed to sabotage the system. Investigators will not say how it got there, but they do not believe it was an inside job. This was the first time these systems were sabotaged remotely. Investigators believe that the hackers have probably fixed their mistake by now and that it is only a matter of time before they deploy the same technique against another industrial control system. A different group could also use those tools for its own attack. This is significant as tensions between Iran and Saudi Arabia have steadily escalated in recent years, and the conflict has drifted online.

12 Aramco Compromised By Iran

When: 2012

In retaliation against the Al-Saud regime, an Iran-backed hacking group called the "Cutting Sword of Justice" wiped data from approximately 35,000 computers belonging to Aramco, a Saudi Arabian public petroleum and natural gas company based in Dhahran. The hacking group used malware called Shamoon, which is designed to spread to as many computers on the same network as possible and, ultimately, make them unusable by overwriting the master boot record. The attack on Aramco in 2012 demonstrated the potential of nation-states and state-sponsored groups to use cyber warfare to target critical infrastructure and disrupt a nation's economy. Since then, multiple other attacks on critical infrastructure have occurred, perhaps the most notable of which is the Colonial Pipeline ransomware attack of 2021.

Threat Briefing_

The Middle East and Northern Africa's cyber security threat landscape has drastically changed in the last year. Following the pandemic, businesses throughout the MENA region continue to rapidly digitalize. However, through 2024, geopolitical tensions have significantly increased in the region, while further risks have been brought about by new technologies, while traditional ransomware-as-a-service risks remain due to the economic growth many countries in the region experience. Consequently, looking ahead to 2025, both traditional threats and new technologies will remain significant vectors of attack.

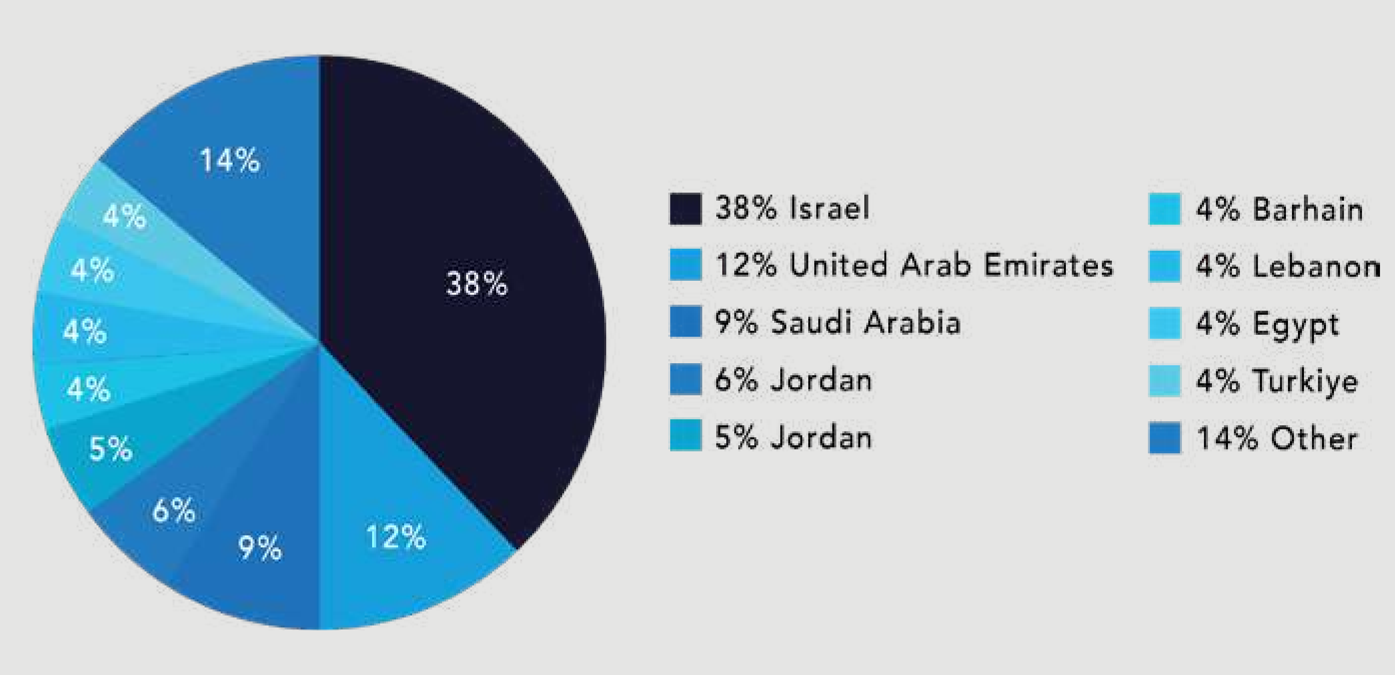
Regarding traditional vectors, ransomware-as-a-service has continued to bring significant threats to the region. Group-IB identified 205 companies in the MEA region that had their information published on ransomware Data Leak Sites (DLSs), which translates to a 68% increase from the previous year when information belonging to 122 victim companies appeared on DLSs. Meanwhile, in 2023, the GCC (number one in the list of most frequent targets, featuring Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates) experienced a substantial 65% increase in ransomware victims published on DLSs, rising from 32 in 2022 to 53 last year. This led Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, to state

> *Ransomware remains a significant threat to our nation. Additionally, cybercriminals are adopting Artificial Intelligence to launch more advanced and sophisticated cyber attacks. This technology, once associated primarily with state and non-state actors, is now employed by a broader spectrum, including hacktivists. We, therefore,*

urge everyone – companies, public sector organisations and regulators, cyber security vendors and law enforcement agencies – to collaborate and take the measures needed to stay ahead of cyber threats”

Consequently, this reinforces the degree to which ransomware affects our critical infrastructure throughout the region. This is only reinforced by the fact that 52% of targets in the region are focused on the education, government, information technology, and communications sectors. Meanwhile, the graph below illustrates the percentage of attacks each country faces, with the UAE and Saudi Arabia making up two of the top three, with Israel seeing the most in the region at 38%.

Breakdown of Cyber Attacks in The MENA Region

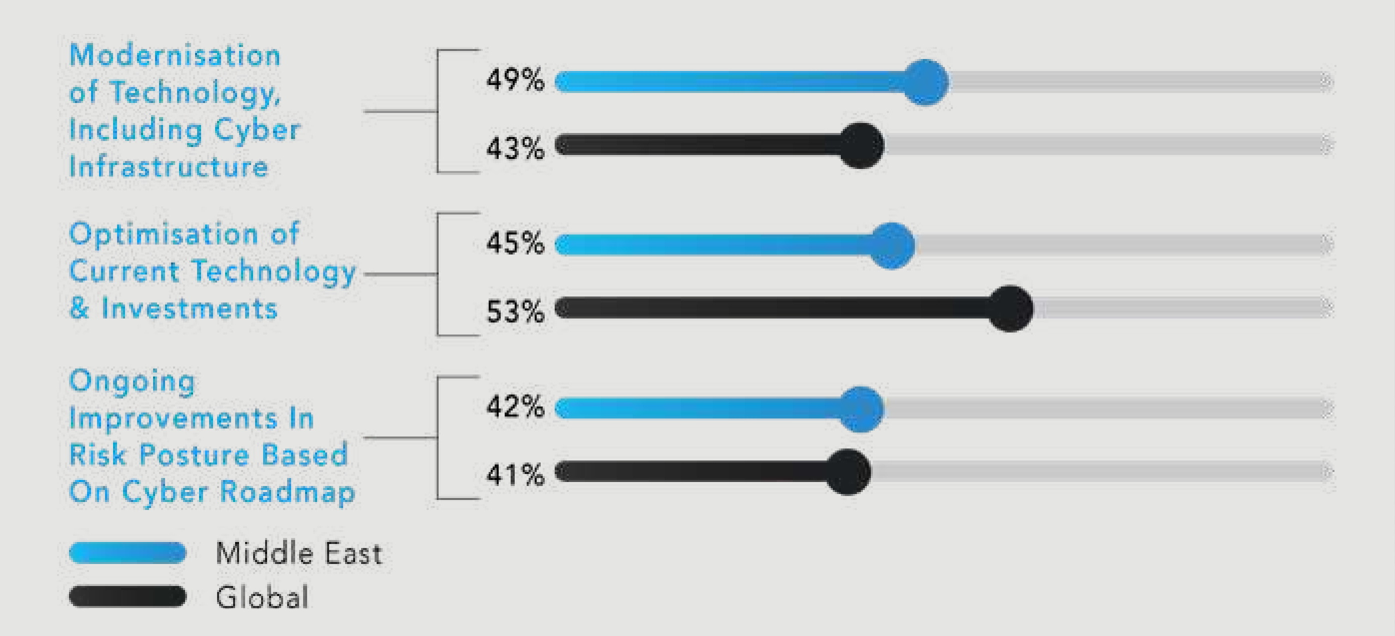


One of these areas where the threat landscape has significantly changed in the region is through an increase in geopolitical tensions. This is as attacks conducted by Iran-linked actors have in the past focused on Israel and those it deemed as supporting such, with Israel often retaliating too. This is through Israel’s war in Gaza, and since the October 7th attacks, beyond the visceral violence lies a hidden layer of the war—an online conflict. Ultimately, this has seen Iranian-based cyber attacks on Israel in support of Hamas, as well as Israeli attacks on both Iran and Palestinian telecommunications and internet providers.

Although these attacks may at first seem diluted to both Israel, Palestine, and Iran, ultimately, all nations in the region are impacted, and this brings with it further cyber risks. In the first quarter of 2024, the Middle East and Northern Africa (MENA) region experienced a dramatic 183% year-on-year increase in distributed denial-of-service (DDoS) attacks, driven by escalating geopolitical tensions and hacktivism, with the main targets being the government and energy sectors. Meanwhile, the UAE at 21 percent, Saudi Arabia at 18 percent, and Iran at 14 percent were the most targeted countries in the region in Q1 of 2024, with the energy sector being the second most targeted vertical, with 18% of all attacks and a 206% year-over-year increase. These increases in attacks by regimes such as the UAE and Saudi Arabia have been attributed to both a hardening of fronts with Iran and its proxies on the one side and Saudi Arabia and Israel on the other, while regimes such as the UAE and Saudi Arabia continue ties with Israel despite the ongoing war in Gaza. This has led to Iranian-based groups and hacktivists continuing to target Saudi Arabia, the UAE, and other GCC countries too.

Consequently, when considering these threats in 2024, 77% of organisations increased their cyber budgets to help deal with these new threats, with 45% of businesses making mitigating cyber risk a top priority. This is because both globally and regionally, breach costs and the number of high-dollar breaches are on the rise. In the Middle East, companies pivot more towards digital business models as more data is generated and shared among organisations, partners, and customers. Consequently, increasing digitisation means companies are exposed to new digital vulnerabilities, meaning that an effective approach to cyber security is more important than ever. Therefore, as modernisation of technology is an area where the region wants more investment than globally, this only reinforces the need to ensure our digital transformation efforts through our OT infrastructure are both adequately invested in and secured. This is reinforced as 89% of respondents believe that new technologies such as generative AI will help their organisation develop new lines of business within the next 3 years, compared to 77% globally.

Top 3 Cyber Security Investment Priorities Over The Next 12 Months



Hence, the need for organisations in the Middle East to address these issues and build up cyber security defences is now more urgent than ever. While solutions have been proposed to help overcome the expanding threat landscape felt by MENA organisations. The Middle East has experienced heightened growth and business activity due to the rise of fintech organisations, private equity firms, sovereign wealth funds, and government-led mega-projects. Added to this, the

Middle East's ambitions to transform into a global hub for sectors like finance, energy, and transportation are driven by strategic initiatives such as Saudi Arabia's Vision 2030 and Abu Dhabi's Economic Vision 2030. Ultimately, however, these developments make the region an increasingly attractive target for cybercriminals.

Hence, moving forward, companies must adopt international cyber security best practices, not only for themselves but also for their supply chains and third-party vendors. Without robust cyber security measures, these strategic plans could be compromised by cyber threats, endangering key sectors and overall economic growth. To improve cyber security in logistics in the Middle East and Northern Africa, the following solutions are suggested:

1 Adopt a Holistic Cyber Security Approach

An effective holistic approach includes four key elements: developing a comprehensive cyber security strategy, focusing on the basics, accounting for regulatory requirements, and developing and implementing an incident response plan.

2 Develop a Comprehensive Cyber Security Strategy

Organisations should evaluate their overall cyber security maturity, scrutinising policies and procedures, and conducting regular assessments to identify vulnerabilities, aligning with external threat assessment and management standards, such as those from NIST or CIS.

3 Focus on the Basic

Organisations should ensure that all employees, from executives to frontline workers, are trained in cyber security awareness, including recognizing phishing emails, using strong passwords, and handling sensitive information. Basic cyber security measures like multifactor authentication (MFA) should be implemented, and software, operating systems, and applications should be regularly updated to protect against known vulnerabilities.

4 Account Regulatory Requirements

As governments refine and strengthen cyber security regulations, organisations must ensure compliance with relevant laws and avoid penalties. This includes tracking the activities of regulatory bodies like Saudi Arabia's National Cyber Security Authority (NCA) and the UAE's Cyber Security Council (CSC) and adhering to data protection laws.

5 Developing Effective Incident Response Plans

A well-structured incident response plan is crucial, mapping out critical systems and data repositories, defining roles and responsibilities, and identifying the organisation's most valuable assets. The plan should align with the comprehensive cyber security strategy and involve all relevant stakeholders. It should cover incident identification, threat containment, cause eradication, and system and data recovery, with provisions for cyber insurance if applicable. Continuous assessment and improvement should be part of the plan to strengthen defences against future attacks.

6 Regional Cyber Security Initiatives

In response to the escalating threat of cybercrime, the Middle East must take decisive action. The establishment of a Council of Ministers for Cyber Security by the Council of Arab Foreign Ministers in 2023 marks a significant step towards enhancing regional cooperation in cyber security. This initiative aims to unify efforts across the Middle East and Northern Africa (MENA) region to address cyber security challenges. Cyber attacks pose a broader threat to the region's economic stability and growth aspirations, and organisations must secure their digital landscapes to ensure continued prosperity.

Ultimately, through evaluating these problems and solutions, this report will dive deeper into the issues discussed in the next section. It will provide a deeper understanding of evaluating common OT security issues while also analysing where regulation and collaboration can support our strategies. It will then consider how new technologies and innovations open up new threats to our OT systems before discussing how we can best build a strategy for the future on both the business and technological sides.

Cyber Security: Key Developments in MENA _

1 Part 1: Dissecting the Cyber Security Issues of Today - Third Party Risk & Geopolitical Factors _

The threat landscape faced by companies operating in the MENA region is considerably expanding. Many of the largest risks from 2024 are predicted to continue into 2025, with an escalation of ransomware attacks, AI-based predictive social engineering opening up new threats, a further amount of organisations being targeted due to geopolitical tensions, and a lack of necessary Zero Trust architectures, meaning these threats remain significant for businesses throughout the region. Meanwhile, due to the recent Crowdstrike Cyber Security outage, cyber security has been elevated to a primary concern for many organisations in the Middle East and Northern Africa. The threat of third-party risk has become an increasingly common discussion point, both in the region and globally. Hence, strengthening the shield that companies use to protect themselves from these cyber threats is becoming necessary through the training of cyber security professionals and adequate legislation. Hence, cyber security has been elevated to a primary concern for many organisations in the Middle East and Northern Africa.

One of these areas where the threat landscape has significantly changed in the region is through an increase in geopolitical tensions. This has only been exacerbated by the shifting political landscape. When it comes to understanding the impact of cyber threats in different parts of the world, no region can afford to be complacent about cyber threats from criminals, "hacktivists," or hostile states. Consequently, this is seen in the region as attacks conducted by Iran-linked actors have in the past focused on Israel and those it deemed as supporting such, with Israel often retaliating too. This is through Israel's war in Gaza, and since the October 7th attacks, beyond the visceral violence lies a hidden layer of the war—an online conflict. Ultimately, this has seen Iranian-based cyber attacks on Israel in support of Hamas, as well as Israeli attacks on both Iran and Palestinian telecommunications and internet providers.

Although these attacks may at first seem diluted to both Israel, Palestine, and Iran, ultimately, all nations in the region are impacted, and this brings with it further cyber risks. In the first quarter of 2024, the Middle East and Northern Africa (MENA) region experienced a dramatic 183% year-on-year increase in distributed denial-of-service (DDoS) attacks, driven by escalating geopolitical tensions and hacktivism, with the main targets being the government and energy sectors. Meanwhile, the UAE at 21 percent, Saudi Arabia at 18 percent, and Iran at 14 percent were the most targeted countries in the region in Q1 of 2024, with the energy sector being the second most targeted vertical, with 18% of all attacks and a 206% year-over-year increase. These increases in attacks by regimes such as the UAE and Saudi Arabia have been attributed to both a hardening of fronts with Iran and its proxies on the one side and Saudi Arabia and Israel on the other, while regimes such as the UAE and Saudi Arabia continue ties with Israel despite the ongoing war in Gaza. This has led to Iranian-based groups and hacktivists continuing to target Saudi Arabia, the UAE, and other GCC countries too.

Meanwhile, the recent Crowdstrike incident has furthered the discussion on how current events affect our cyber security outlook. Here the focus has been opened up to what we can do to protect against the challenges third-party risk brings. Consequently, what happened in July this year was a CrowdStrike Falcon Sensor update that caused some machines to enter a boot loop or encounter the BSOD (Blue Screen of Death). This is as a routine software update by cyber security giant CrowdStrike that triggered a cascading global IT outage. This is because a flaw in CrowdStrike's antivirus software update targeted specifically at Windows devices inadvertently disrupted critical systems worldwide, with payment systems faltering, banks struggling to process transactions, and airports facing operational disruptions. Although this was not a cyber attack, the incident serves as a stark reminder of the vulnerabilities in our system and the potential for malicious actors to exploit such vulnerabilities. It also opened up the conversation about how best we can mitigate against challenges with third-party risk throughout organisations in the Middle East. Some offered solutions to this have included:

Long-Term Cyber Risk Solutions: Quantitative Analysis of Insurable Incidents

- **Operational Impact:** Cyber incidents like CrowdStrike can cause extended operational downtime, leading to financial and legal liabilities, particularly for sectors like airlines and hospitals.

- **Preparedness:** Businesses need to plan for high-risk cyber events, assess liabilities, and ensure cyber incidents align with their insurance coverage to mitigate severe financial impacts.

Long-Term Cyber Risk Solutions: Scenario-Led Cyber Risk Mitigation

- **Proactive Approach:** Understanding and quantifying likely cyber threat scenarios helps organisations mitigate operational and financial impacts.
- **Third-Party Risk:** Businesses that rely on third-party solutions must assess and quantify risks related to cyber disruptions using data-driven, probabilistic models.
- **Financial Safeguarding:** By evaluating the magnitude of risks and financial liabilities, companies can prioritise mitigation strategies and strengthen their resilience against future cyber incidents.

Consequently, in this context, it is imperative that our businesses fully understand the challenges and benefits of both geopolitical challenges and third-party risks faced in the context of Middle Eastern companies. Our experts will consequently explore the challenges opened up by both of these issues and see what can be done to best mitigate against these risks.

INTERVIEW

What Are The Most Significant Cyber Security Issues Middle Eastern Organisations Face Today?

Krishna Dixit, Senior Cyber Security Officer

Schneider Electric

What I would suggest is first considering the global landscape and then narrowing the focus to the Middle East. When we assess the global situation, there are numerous concerns. For instance, devices may be exposed to the Internet, or we see the increasing convergence of IT and OT (Operational Technology) systems globally. Different organisations and regions are at varying stages of this convergence, and the speed of adoption differs across geographies.

Looking specifically at the MENA (Middle East and Northern Africa) region, it's important to note that we are adopting newer technologies at a faster pace—though, of course, this is my personal view. What's significant is the growing adoption of IT-OT convergence and cloud-related technologies, with more cloud deployments happening each day. The public now has access to solutions that allow subscription to cloud services or to use cloud-based platforms that offer various functionalities. From an OT perspective, many vendors provide cloud-hosted solutions for devices used in home automation, utilities, or the grid sector, as well as systems that collect data from remote environments.

However, as the use of cloud environments grows, so too does the potential attack surface. While IT-OT convergence is undoubtedly a step forward, it brings challenges that must be addressed. With progress come risks, and as the industry matures, we're seeing an increase in targeted attacks in the operational technology space.

Operational technology is not limited to critical infrastructure like oil and gas, water and power utilities, or the grid. It also applies to sectors like food and beverage manufacturing, building automation, and the critical systems within airports that safeguard human lives. These targeted attacks tend to be highly focused, sophisticated, and narrowly directed.

In summary, it's essential to concentrate on these two areas—IT-OT convergence and cloud security. As we continue to advance, new concerns will undoubtedly arise, but at present, these are two of the most pressing issues given the rate at which technology is being adopted.

INTERVIEW

What Are The Most Significant Cyber Security Issues Middle Eastern Organisations Face Today?

Muhammad Khurram Khan, Founder & CEO

Organisations in the Middle East and Northern Africa (MENA) are confronting increasingly sophisticated cyber threats that pose significant risks to critical national infrastructure such as government, energy, healthcare, and finance. Ransomware is becoming a rising threat, which can cripple operations by encrypting vital data until a ransom is paid. In addition, phishing campaigns, which exploit human vulnerabilities to steal sensitive information, are another critical threat to organisations and individuals. On the other hand, state-sponsored cyber espionage remains a major concern, particularly for organisations in energy and government, as attackers seek to gain strategic and geopolitical advantages. As these cyber threats evolve, the need for robust cyber security measures has never been more urgent to protect sensitive data, maintain operational continuity, and ensure trust in digital systems.

INTERVIEW

What Impact Do Geopolitical Events Have On Our Organisations' Cyber Security?

Moath Sakaji, MEA OT/ ICS Security Consulting Lead

MANDIANT

Geopolitical events can significantly impact the cyber security landscape for organisations, particularly those operating in critical infrastructure sectors within the Middle East. The convergence of political tensions, state-sponsored cyber activities, and regional conflicts creates a volatile environment where cyber threats are elevated.

For instance, geopolitical rivalries can motivate state-sponsored actors to engage in cyber espionage targeting critical infrastructure to gain strategic advantage or disrupt operations. Another angle is the disinformation campaigns. Political events can be exploited to spread disinformation and propaganda, aiming to manipulate public opinion, sow discord, or disrupt critical infrastructure operations. As a result of misinformation, organisations can find themselves listed in boycott lists that impact their revenue and operations. Mandiant threat intelligence observed and reviewed evidence and reports of propaganda campaigns with the aim of manipulating public opinion and reported these affecting multiple geographies. On the critical infrastructure side and OT systems within critical infrastructure sectors, such as energy, utilities, and transportation, may become targets for cyber attacks seeking to cause physical damage, disrupt essential services, or create economic instability.

Organisations operating in the Middle East need to be aware of the heightened cyber security risks posed by geopolitical events. It is crucial to:

- Proactively assess threats by regularly evaluating your vulnerabilities, especially in light of current geopolitical events.

- Strengthen cyber security posture by implementing robust security measures Enhance threat intelligence by staying informed about emerging threats and tactics specific to the region. Partner with cyber security firms and information-sharing platforms.

- Work and collaborate with government agencies and industry peers to share threat intelligence and coordinate response efforts.

- Develop crisis management plans and prepare for potential cyber incidents, including playbooks, table top exercises, communication protocols, technical response procedures, and public relations strategies.

INTERVIEW

What Impact Do Geopolitical Events Have On Our Organisations' Cyber Security?

Krishna Dixit, Senior Cyber Security Officer
Schneider Electric

I find this question interesting but also tricky, as geopolitical factors, while essential for regional stability, can complicate matters. We've all witnessed the impact of the Russia-Ukraine conflict, and now we're observing the ongoing Israel-Palestine situation. Without focusing on these specific examples, what's important is the growing trend of more targeted and sophisticated cyber attacks.

In some cases, these attacks are alleged to be nation-state-sponsored. What we're seeing is a shift in the balance of power, where countries with significant resources, and those suspected of sponsoring these attacks, may be targeting critical infrastructure of their adversaries. To give an example, imagine an attack on an electricity plant during winter in a country that experiences harsh, snowy conditions. Such an attack could take down the power grid, leaving people without heat, causing widespread disruption, and leading to significant financial losses. The knock-on effects could be severe, creating a domino effect.

While these attacks can directly harm individuals, they also escalate global tensions. Such incidents create divisions, with countries forming alliances and blocks in support of different parties, further increasing tensions until they reach a tipping point.

In the past, cyber security was meant to be a neutral, independent field. However, it has now become a key player in geopolitical conflicts. My hope is that cyber security doesn't become the pivotal factor in global political discussions in the future, although its role is clearly growing.

INTERVIEW

In Light Of The Crowdstrike Outage, How Can We Best Create a Strategy To Prevent Third Party Risk?

Mousab AlSaaydeh, Head of Cyber Security

Confidential

In order to best create a strategy to prevent third-party risk, you will have to:

Explain The Nature Of Third-Party Risks

Covering the potential risks that could arise from the vendors, service providers, partners, and other external entities.

Provide An Overview Of The Crowdstrike Outage Incident

Emphasising the implications and lessons learned from it.

The Risk Strategy To Mitigate Such Risks Could Include The Following Pillars

Conduct Third-Party Risk Assessment:

- **At early stage:** Conduct third party risk assessment before engaging with third parties, including evaluating their security posture, compliance with industry standards, and overall risk profile.
- **Continuous Monitoring:** Conduct continuous monitoring and reassessment of third-party risks, and keep an eye on their risk treatment plan and security posture

Contractual Safeguards and SLAs: Such as including security Requirements in third party contracts and having LSA, include uptime guarantees, response times for incidents, and penalties for non-compliance.

Having Risk Mitigation Strategies, including:

- **Data Segmentation and Access Control:** to limit third-party access to sensitive information
- **Cyber Insurance:** Mitigate potential financial losses through cyber insurance service

2 Part 2: Adapting to Regulations & Building Collaboration Within Our Organisations_

When exploring how we can overcome these challenges due to an expanding threat landscape, standards and regulations can become central to our approaches. Subsequently, in recent years in the Middle East and Northern Africa, governments and organisations have taken significant steps to enhance cyber security measures, collaboration, and regulatory frameworks to address evolving threats and protect businesses across sectors. This has been seen as imperative, as cyber attackss have spill-over effects and cross-sectoral impacts based on the use of the same underlying technology. This section will proceed by highlighting the regulations in each country before discussing the importance of building collaboration too. The legal frameworks across the Gulf Cooperation Council (GCC) countries demonstrate a concerted effort to enhance cyber security, data protection, and the regulation of electronic transactions. The below highlights some initial regulations throughout the region, with their focus, before diving in deeper on a few recent regulations in both Saudi Arabia and the UAE:

1 United Arab Emirates (UAE)

Federal Law No. 2 of 2019

This focuses on cybercrime prevention and the protection of critical information infrastructure, with an emphasis on sectors like healthcare. Hence, the act criminalises unauthorised access, hacking, phishing, spreading malware, and the misuse of technology to invade privacy or defame others. Meanwhile, penalties include: imprisonment and substantial fines for violations.

2 Saudi Arabia

Cyber Security Law (2019)

This aims at protecting critical information infrastructure and ensuring confidentiality, integrity, and availability of data. It hence requires government and critical infrastructure operators to implement cyber security measures, conduct risk assessments, and report incidents to the National Cyber Security Authority (NCA). Penalties include fines and the potential suspension of licences for non-compliance.

3 Qatar

Personal Data Privacy Protection Law (Law No. 13 of 2016):

This bill includes regulating the processing of personal data and protecting privacy rights. It defines lawful bases for data processing, establishes data subject rights, and outlines obligations for data controllers and processors. It also sets up the Privacy Protection Department for compliance oversight. Meanwhile, penalties are imposed for breaches of data protection rules, enforced by the Privacy Protection Department.

4 Oman

Electronic Transactions Law (Royal Decree No. 69/2008)

This provides a legal framework for electronic transactions, electronic signatures, and data interchange. Hence, recognition of electronic records as evidence, confidentiality, and security in electronic transactions. While it is not directly focused on data protection, it influences information security practices. Meanwhile, penalties are specific to electronic transaction violations, reinforcing the legal validity of digital interactions.

5 Bahrain

Personal Data Protection Law (Law No. 30 of 2018)

This regulates personal data processing by public and private entities, protecting privacy rights. It controls data collection, use, disclosure, and transfer and requires security measures to protect data. Establishes the National Data Protection Authority for enforcement. Meanwhile, there are penalties for non-compliance, which are overseen by the National Data Protection Authority.

6 Kuwait

Cybercrime Law (Law No. 63 of 2015)

This combats cyber offences, including unauthorised access, data interference, and cyberstalking. It includes provisions against spreading false information, promoting extremism, and engaging in online terrorism activities. Meanwhile, severe penalties, including imprisonment and fines for cybercrime convictions.

Each country in the GCC has consequently developed specific laws that reflect its priorities, whether that's cyber security, data privacy, or the regulation of electronic transactions. The UAE and Saudi Arabia emphasise cyber security and critical infrastructure protection, while Qatar and Bahrain focus more on personal data protection. As a result of this, despite the aim of regulating data protection and information security, with further regulations expressed through the below:

2022 - OT Cyber Security Controls - Saudi Arabia

The NCA OTCC (Operational Technology Cyber Security Controls) aims to enhance the cyber security of industrial control systems (ICS) within Saudi Arabia, specifically targeting critical infrastructure. It is designed to align with international standards and best practices, strengthening the Kingdom's national cyber security posture. The key provisions include:

- **Governance and Strategy:** Establishes cyber security governance, policies, and strategies for OT environments, including risk management and role definitions.
- **Asset Management and**

Configuration: This involves the identification, classification, and management of OT assets, including maintaining an asset inventory and managing configurations.

- **Threat and Vulnerability Management:** Focuses on identifying, assessing, and mitigating OT-specific vulnerabilities and threats, including threat intelligence and vulnerability assessments.
- **Incident Response and Recovery:** Provides protocols for detecting, responding to, and recovering from cyber security incidents within OT systems, including incident response planning and disaster recovery.

The NCA OTCC

sets mandatory cyber security requirements, with penalties for non-compliance potentially including fines, suspension of operations, or other regulatory actions, particularly for entities managing critical national infrastructures (CNIs). The specific penalties depend on the severity of the violation and its impact on national security and infrastructure resilience. More detail can be found here

The Saudi National Cyber Security Authority Assessments

The authority announced on December 26, 2022, that it had held an introductory meeting with national authorities on the National Plan for Cyber Assessments for 2023, aiming to share its plans for the year. In particular, the NCA stated that it will be conducting cyber assessments for national authorities during 2023, including compliance assessments and technical cyber assessments of sensitive systems, to monitor cyber risks at the national level and measure the level of compliance with the requirements and controls issued by the NCA.

UAE New 2024 Regulations

Recognising the critical importance of securing its digital infrastructure, the UAE is set to introduce new policies and regulations by the end of 2024 that focus on enhancing AI protections, cloud computing and data security, Internet of Things (IoT) security, and cyber security operations centres. The UAE's new cloud computing and data security policy will establish stringent data protection, access control, and incident response guidelines. Meanwhile, its new regulations are also centred around IOT technologies. This is because the UAE aims to mitigate the risks associated with IoT devices and ensure that they can be securely integrated into the digital ecosystem. Furthermore, to enhance the nation's ability to detect and respond to cyber threats, the UAE will establish advanced cyber security operations centres. These will: provide 24/7 monitoring of network traffic and system activities to identify potential threats in real time. They will also utilise threat intelligence feeds to stay informed about the latest cyber threats and vulnerabilities and develop and implement incident response plans to swiftly address and mitigate cyber incidents. All of which will support our critical infrastructure firms' digital transformation efforts. The new cyber security measures will have a significant impact on these sectors by:

Health: ensuring the security of sensitive medical data and protecting healthcare systems from cyber threats.

Energy: safeguarding critical energy infrastructure from cyber attackss that could disrupt supply and operations.

Education: protecting educational institutions and data from cyber threats and ensuring a safe learning environment.

Aviation: enhancing the security of aviation systems and data to prevent disruptions and ensure passenger safety.

Qatar National Cyber Security Agency Recommendations

Qatar's National Cyber Security Agency (NCSA) has announced recommendations for electricity and water utilities in the region to implement ISA 62443 standards. This recommendation is part of a broader initiative aimed at enhancing the security of cyber security across the nation. These will help to mitigate risk and promote best practices and standards. Nevertheless, these regulations do not go to the extent of the UAE and Saudi Arabia's frameworks.

Hence, overall, although regulations can be seen within the more developed GCC countries such as Saudi Arabia, the UAE, and Qatar, more can be done through the region to ensure our businesses are better protected and prepared for cyber attacks. The importance of regulations is expressed as a third of Middle East organisations agree that four types of regulation will be most important to secure the future growth of their organisation. All of this comes together to help reduce the risk of cyber attackss, help better manage cyber incidents, and improve efficiency for organisations by having these processes in place. Consequently, it is essential for leaders to foster collaboration among relevant stakeholders towards the implementation of cyber regulations that promote transparency and accountability while prioritising investments to secure the weakest links against cyber threats. With 77% of regional respondents increasing their cyber budgets, there is positive development in this sector and a clear indication that organisations are taking their cyber security goals seriously to tackle current and future challenges.

Meanwhile, cyber security has become essential in both protecting computer systems and networks from unauthorised access, theft, damage, or disruption, as well as being essential for maintaining trust in the digital economy and ensuring a secure online environment. Hence, collaboration between businesses, government, and academia has been encouraged in the region. In the Middle East and Northern Africa, such collaboration has been seen in GCC countries. On July 1st, Qatar hosted the third meeting of the Executive Committee for Cyber Security in the Gulf Cooperation Council countries, which underscored the importance of fostering international cooperation and partnerships. While, beyond the region, the GCC's new trade deal with the UK 'will open the door for collaboration on cyber security.

In this context, it is imperative that our businesses fully understand the challenges and benefits of new regulations such as those mentioned above. Our experts will consequently explore the challenges opened up by new regulations in the region and how we can overcome them, as well as the benefits of collaboration for organisations throughout the region.

INTERVIEW

What Is The Significance Of Regulations In Ensuring Our Organisations Remain Secure?

Mansoora Shafi Qazi, VP Information Security

Regulations play a crucial role in maintaining the security and integrity of organisations.

Here are the top ten reasons why they are significant:

- **Protecting Sensitive Data:** Regulations like Consumer Protection law, Federal law 45, GDPR, CCPA, etc. ensure that organisations handle personal data responsibly, reducing the risk of data breaches.
- **Ensuring Compliance:** Adhering to regulations helps organisations avoid legal penalties and fines, which can be substantial.
- **Building Trust:** Compliance with regulations fosters trust among customers, Partners, and stakeholders, enhancing the organisation's reputation.
- **Preventing Cyber Attacks:** Security regulations mandate measures such as encryption, access controls, and regular security audits, which help prevent cyber-attacks.
- **Standardising Practices:** Regulations provide a framework for standardising security practices across the organisation, ensuring consistency and reliability.
- **Enhancing Incident Response:** Regulatory requirements often include guidelines for incident response, helping organisations quickly and effectively address security breaches.
- **Protecting Intellectual Property:** Regulations help safeguard intellectual property by enforcing strict controls on access and distribution.
- **Promoting Fair Competition:** By ensuring that all organisations adhere to the same security standards, regulations promote fair competition in the market.
- **Ensuring Financial Stability:** Financial regulations protect against fraud and ensure the stability of financial systems, which is critical for organisational security
- **Encouraging Continuous Improvement:** Regulations often require regular reviews and updates to security practices, encouraging organisations to continuously improve their security posture.

Regulations not only help in protecting the organisation but also contribute to a safer and more secure digital environment overall.

INTERVIEW

What Is The Significance Of Regulations In Ensuring Our Organisations Remain Secure?

Khaled Khaled, OT Security Project Manager

Air Liquide

Adapting to new regulations in the OT (Operational Technology) cyber security world requires a proactive, systematic approach. So the company and it's more here the security leader should not wait the till last days otherwise company could face fine / penalty and also we cannot just start with implementation technical controls

Before any action, we should:

- Consult with your lawyer and understand the risks and impact on the company from a legal standpoint.
- Inform the management and address the topic as business risk and gain the support of the management as sometime the change could be huge and require a lot of energy/budget and without management support we could face blocking points and may even failure. Advice if the change is big and requires a lot of time and investment, better to have a dedicated project/ team to achieve the requirement
- Perform Risk Assessment and gap analysis to know where we exactly stand regarding the new regulation(this should include Identify Critical Assets, Assess Vulnerability and for sure Prioritise Mitigation)
- If a company doesn't have a suitable compliance framework (e.g., NIST Cyber Security Framework, IEC 62443), it's the right time to adopt a framework. Perform a gap analysis between adopted framework and new regulations regarding what it covers and what is missing and the priority point
- Create a roadmap with clear milestones and deadlines for complying, get the needed budget, communicate, communicate and communicate
- Develop and deliver targeted training programs to educate the team who will support new regulations and their roles in maintaining compliance. Everyone should be part of the program, so conduct regular awareness to reinforce the importance of compliance and best practices.
- Update the company policies/ procedures if needed and implement the need of technical controls and solutions and always start with the effortless tasks (low-hanging fruit). Find third party to help in case you don't have the local resources
- Engage with both external and internal auditors to identify potential issues before formal regulatory audits.
- Lastly, promote a compliance culture and ensure continuous monitoring and improvement.

INTERVIEW

What Is The Significance Of Regulations In Ensuring Our Organisations Remain Secure?

Muhammad Khurram Khan,
Founder & CEO

To adapt cyber strategies to new regulations across the MENA region, organisations must first ensure continuous monitoring of evolving legal frameworks and compliance requirements. They should implement flexible cyber security policies that align with region or nation-specific laws, such as data protection and privacy standards (PDPL in Saudi Arabia). Regular audits, training, and updates on regulatory changes are crucial. Collaborating with local authorities and cyber security experts will ensure compliance, while integrating adaptive technologies like AI-driven threat detection can streamline adherence to regulatory shifts. A proactive approach in aligning security practices with legal expectations fosters both resilience and trust.

3 Part 3: Discussing The Threats Opened Up to Our Infrastructure by New Technologies_

New technologies such as AI, machine learning, and quantum computing have the possibility of accelerating the resolution of challenging issues. Nevertheless, key questions remain surrounding how this will affect our cyber security strategies and whether AI will be a force for good or evil moving forward. This is because AI is becoming increasingly prominent, and the risks and rewards associated with it have to be considered. This is as the Middle East is undergoing a rapid digital transformation, with AI at its epicentre. Countries like the UAE and Saudi Arabia have positioned themselves as global AI leaders, investing heavily in research and development, like the Falcon 2 AI model, which rivals global giants in the AI domain. However, this digital evolution comes with its own set of challenges. Cyber Security threats are rising, with countries like Bahrain and Egypt experiencing a surge in malware attacks. While benefits have been expressed as AI-powered systems are becoming indispensable tools for detecting anomalies, predicting breaches, and responding swiftly to cyber attacks.

These benefits are only reinforced as AI can detect and prevent cyber attacks, analyse vast amounts of data, automate threat response, and continuously adapt to emerging threats. Consequently, the use of AI helps in detecting and blocking malware, filtering suspicious emails, monitoring network traffic, and protecting cloud services and endpoint devices. Moving into the future, this can see significant benefits with regards to our organisation's cyber security programs. such as:

- **Advanced Threat Detection and Prevention:** AI uses advanced algorithms to analyse massive data in real-time, identifying anomalies and patterns indicative of potential threats. By learning from historical data, AI uncovers previously unknown attacks, enhancing detection and prevention capabilities.
- **Real-time Monitoring and Response:** By analysing data in real time, AI can swiftly identify unusual behaviours or deviations from normal patterns, enabling prompt responses to potential threats and reducing the window of exploitation.
- **Enhanced Incident Response:** AI can automate and streamline incident response, allowing for rapid identification, analysis, and containment of breaches. This accelerates the investigation and response phases, minimising downtime and limiting breach scope.
- **Adaptive Learning:** AI's adaptive learning refines models based on new data. This continuous learning process helps cyber security systems evolve with emerging threats, improving accuracy and effectiveness.
- **Reduction in False Positives:** AI can accurately discern between genuine threats and benign activities, significantly reducing false positives and allowing security personnel to focus on real threats.
- **Predictive Analysis:** AI analyses historical and real-time data to predict potential future threats. This proactive approach allows organisations to take preemptive measures, like deploying patches, before threats materialise.
- **Identifying Insider Threat:** AI can monitor user behaviour and identify unusual patterns that might indicate insider threats, helping detect unauthorised access or suspicious activities by employees or contractors, and reducing insider threats.
- **Scalability and Efficiency:** AI-powered systems scale effortlessly to process vast data amounts at high speeds, ensuring timely threat identification and response, preventing our teams from being overwhelmed by large-scale attacks.
- **Vulnerability Management:** AI identifies system or network vulnerabilities by analysing configurations, software versions, and other factors. This means it can pinpoint weak points and recommend patches or remediation, reducing the attack surface and strengthening security.
- **Adaptive Access Control:** AI-driven access control systems dynamically adjust permissions based on user behaviour and context, ensuring only authorised users access sensitive resources and reducing the risk of unauthorised data breaches.

At the same time, however, the risks associated with artificial intelligence throughout the Middle East are considerable. AI is predicted to be a major protagonist when it comes to cyber security. As businesses strive to protect their assets and safeguard user privacy, artificial intelligence (AI) has emerged as a new player in cyber security. One of the challenges in striking a balance between security and AI lies in the shortage of professionals capable of developing and managing AI-powered security systems. Some key trends affecting the landscape are:

Sophisticated Social Engineering Attacks & Deepfakes

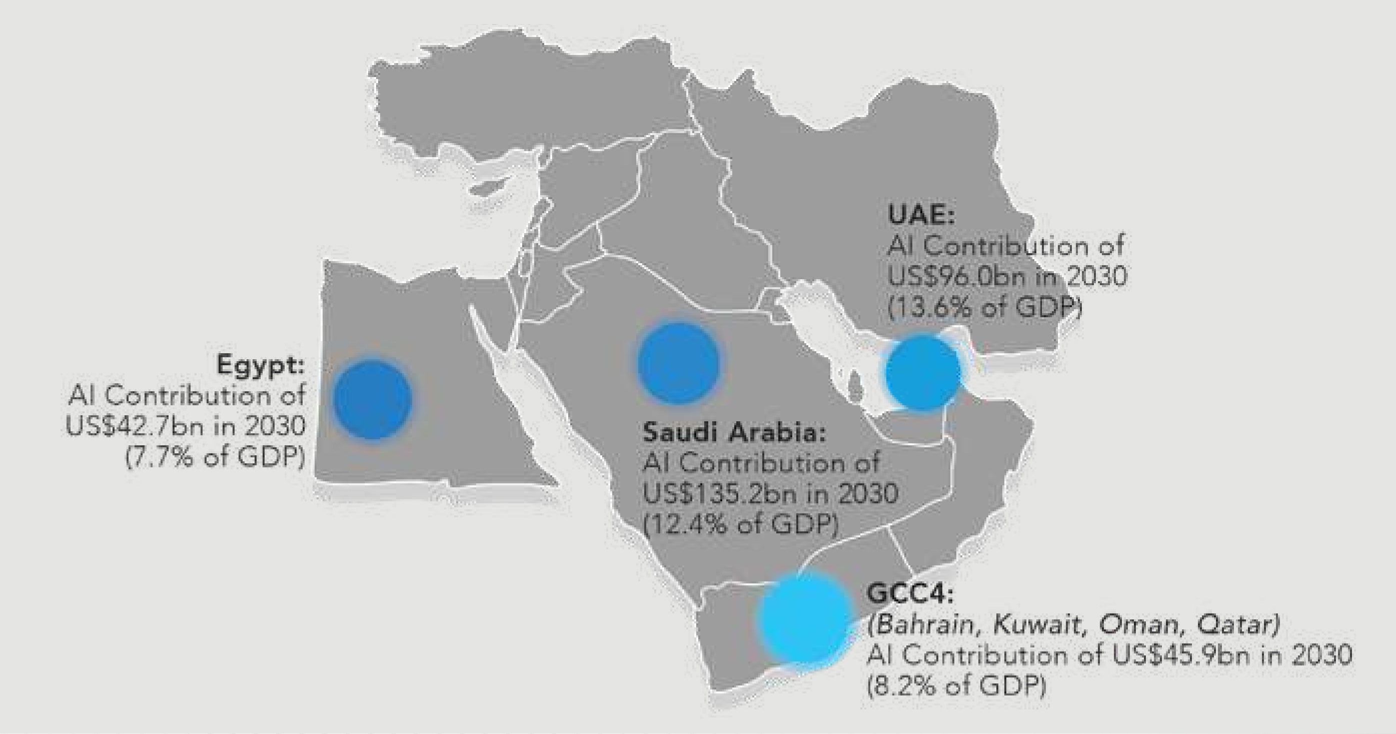
Generative AI will provide threat actors with powerful new tools to conduct convincing social engineering at scale. Advanced natural language models like ChatGPT will enable attackers to churn out personalised, targeted phishing emails and text messages that appear remarkably human. Attempts to manipulate staff via social media are also likely to rise. As this technology advances, we may see threat groups leverage deep fakes to spread misinformation or compromise high-value targets through tailored social engineering attacks across communication channels.

Automation of Cyber Attacks & Compromise of AI Chatbots

AI and machine learning will accelerate and automate repetitive parts of the attack lifecycle, reducing the need for advanced technical skills. From open-source intelligence gathering and vulnerability scanning to credential stuffing and exploit execution, AI will enable faster, cheaper, and more effective threat campaigns. At the same time, AI is powering a new generation of intelligent chatbots and digital assistants designed to engage with customers and staff. These bots have access to troves of personal and corporate data that could prove a tempting target for attackers. Flaws in their design or security could enable cybercriminals to leverage these tools as Trojans to infiltrate business networks.

Considering this in the context of the MENA Region, the benefits and drawbacks are broad. The below graph illustrates the contribution of AI to GDP by 2030, contributing up to $15.7 trillion to the global economy by 2030. The Middle East is expected to accrue 2% of the total global benefits of AI in 2030, equivalent to US$320 billion. While the annual growth in the contribution of AI is expected to range between 20 and 34% per year across the region, with the fastest growth in the UAE, followed by Saudi Arabia.

Contribution of AI to GDP by 2030



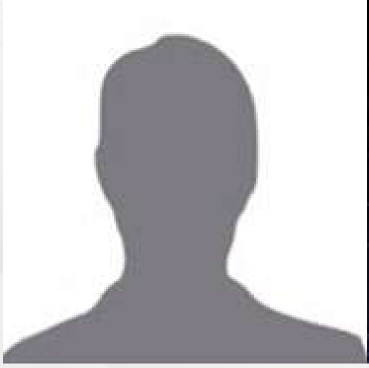
Hence, AI has the potential to fundamentally disrupt markets in the Middle East through the creation of innovative new services and entirely new business models through automation, product enhancement, and an overall increase in security. The below diagram illustrates the contribution of AI to Middle East industry by 2030.

CONTRIBUTION OF AI TO INDUSTRY IN 2030	ABSOLUTE CONTRIBUTION IN 2030 (US$ BILLIONS)	CONTRIBUTION OF AI TO MENA GDP BY INDUSTRY
Construction & Manufacturing	*$99*	*12.4%*
Energy, Utilities & Resources	*$78*	*6.3%*
Public Sector, Including Health & Education	*$59*	*18.6%*
Financial, Professional, Administrative Services	*$38*	*13.6%*
Retail, Consumer Goods, Accomodation & Food Services	*$23*	*19%*
Transport & Logistics	*$12*	*15.2%*
Technology, Media, Telecommunications	*$10*	*14%*

Hence, for our security systems, both benefits and drawbacks are seen, encouraging this spending. There has been a fast-tracked adoption of new cloud and IOT technologies to help fend off the risks brought by AI to our systems, with expected increases of 24% and 17% on spending for data privacy and cloud security for security teams budgets. This is due to the risks such as unauthorised usage by workers, which pose operational risks, while attackers' adoption of the technology means a likely increase to their base technical capabilities and improved social engineering attacks. This is reinforced as Microsoft and OpenAI warned about detected nation-state attackers from China, Iran, Northern Korea, and Russia using the companies' GenAI services to improve attacks by automating reconnaissance, answering queries about targeted systems, and improving the messages and lures used in social engineering attacks, among other tactics.

Meanwhile, where these innovations go beyond AI, similar wariness is necessary. Although IoT devices are revolutionising the way those in the region live and work, whether through seamless transport, enhanced public services, or implementing smart city agendas, risks remain. While businesses in the Middle East, particularly in the GCC region, are rapidly embracing advanced technologies like AI, blockchain, and IoT to propel themselves into the realm of smart, data-driven, and highly automated enterprises, new challenges are opened up when securing our systems, with risks seen through lack of encryption, insecure ecosystems, authentication issues, firmware exploits and software vulnerabilities, DoS attacks, device threats, and ransomware.

In this context, the UAE has introduced new controls to help secure "cloud computing and data security," "Internet of Things security," and "cyber security operations centres". However, more needs to be done. This section will hence examine both the benefits and drawbacks of new technologies and innovations, such as artificial intelligence, in order to build the best processes for the future of our cyber security programs.



INTERVIEW

How Does IoT Expansion Play a Role in Evolving Our Cyber Strategies?

Dr. Albandari Alsumayt, Assistant Professor, Computer Security & Networks, The Head of the Computer Science Department Applied College

IoT growth presents both benefits and hazards; although it can spur efficiency and creativity, it also necessitates a review and reinforcement of cyber security measures. To keep up with the ever-changing IoT landscape, organisations must be proactive, put in place thorough security measures, and exercise constant vigilance. Understanding this environment, making security investments, and getting ready for the always changing nature of cyber threats connected to IoT are essential to striking a balance between the advantages and hazards. Working with subject-matter specialists is more important than ever as businesses traverse the difficult world of cyber security and IoT. Control Audits can provide the strategic knowledge and specialist abilities needed to strengthen your cyber defences in this changing environment with its Cyber Security Governance, Risk Management, and Compliance (GRC) consultation.

INTERVIEW

How Does AI Open Both Opportunities & Threats For Organisations Throughout The Middle East?

Ala' Zayadeen, Head of Information Security and Data Privacy

In general, AI fosters innovation by enabling the development of new products, services, and business models.

From a customer perspective, AI allows companies to deliver personalised experiences to customers by analysing their behaviour, preferences, and interactions. This can increase customer satisfaction and loyalty.

In terms of cyber security, it can enhance cyber security by detecting and responding to threats in real-time, automating routine security tasks, and predicting potential vulnerabilities. However, it also introduces new cyber security risks. Hackers can target AI systems, and using AI in cyber attackss, such as deep fakes and automated phishing, can make them more sophisticated and harder to detect.

In conclusion, while AI offers significant opportunities for growth and innovation, organisations in the Middle East must be proactive in addressing the associated risks to fully capitalise on its potential.

INTERVIEW

How Does AI Open Both Opportunities & Threats For Organisations Throughout The Middle East?

Muhammad Khurram Khan, Founder & CEO

AI plays a pivotal role in modern cyber security strategies, serving both as a powerful defence tool and, paradoxically, a potential threat. On the opportunity side, AI strengthens defences by automating threat detection, analysing vast amounts of data in real time, and identifying patterns of malicious behaviour that would be difficult for humans to detect. AI-driven systems can predict vulnerabilities, thwart phishing attacks, and continuously adapt to new cyber threats, providing organisations with more proactive and efficient cyber security measures. Machine learning algorithms, in particular, enhance intrusion detection systems and help mitigate insider threats by flagging abnormal activities. However, AI also introduces new risks to society. Cybercriminals can exploit AI to launch more sophisticated attacks, such as using deep learning to create highly targeted phishing schemes or evade traditional detection mechanisms. There is growing concern over the use of AI to automate large-scale cyber attacks, develop advanced malware, or manipulate decision-making systems. In essence, AI is both a significant opportunity for enhancing cyber security and a potential enabler of more advanced cyber threats. To maximise its benefits, organisations must not only leverage AI for defence but also anticipate and mitigate AI-driven risks.

INTERVIEW

How Do New Innovations Play a Role In Evolving Our Cyber Strategies?

Ali Ismail Awad, Associate Professor of Cyber Security

One significant technology is AI, which strongly influences the evaluation of cyber strategies. With LLMs models, it would be possible to seek help and support and research quick decisions. AI can contribute heavily to security awareness and training and can be used to check the compliance of current cyber strategies with national and international regulations and standards.

INTERVIEW

How Do New Innovations Play a Role In Evolving Our Cyber Strategies?

Krishna Dixit, Senior Cyber Security Officer

In my view, AI is still relatively nascent compared to its predecessor technologies, some of which have been around for decades. However, the adoption of AI has been much faster than what we witnessed with previous technological waves, such as the dot-com bubble or even the earlier internet boom. What's crucial here is that AI development and implementation must be approached judiciously.

This is why many laws are being drafted globally to regulate AI. While AI can be a powerful tool, it has the potential to become a loose cannon if not properly managed. The goal should be to harness the benefits while mitigating the risks. AI is already being used to improve speed, efficiency, output, and productivity, but at the same time, malicious actors are also leveraging AI to automate attacks and identify vulnerabilities—tasks that would be far more cumbersome for humans to accomplish. AI offers speed and precision, which can be dangerous in the wrong hands.

Although we will undoubtedly need AI, we must approach its use cautiously, applying the necessary guardrails. As the field of cyber security evolves, AI-specific cyber security will become increasingly important. AI applications are being developed at an incredibly fast pace, and just as cyber security guidelines have been established for IT, OT (operational technology), and industrial technologies, similar regulations will need to be introduced for AI.

Some of the larger organisations are already working towards this, but generally speaking, AI applications hold enormous potential. AI could be used to analyse threat intelligence data more effectively, identify attack vectors, and improve efficiency in various domains. For example, in home automation, an AI bot could simplify daily tasks.

However, while there are many advantages to adopting AI, there are also significant risks, and these need to be carefully addressed as the technology continues to evolve.

4 Part 4: Building A Holistic Cyber Security Strategy_

Building for the future and choosing the correct processes are essential to ensuring our organisations stay cyber-secure. The most serious cyber threat to organisations throughout the Middle East and Northern Africa is ransomware attacks, with 83% of successful cyber attacks in the Middle East having been of a targeted nature to government, financial, and critical infrastructure organisations. Meanwhile, in the face of escalating ransomware risks and the need for greater data security, we need to acknowledge the critical importance of strengthening cyber security across the public and private sectors, with a significant push towards building a cyber-resilient culture from the ground up. This is especially important in the context of the fact that in the next few years, approximately 24 billion Internet-connected devices will be installed worldwide. This means that, with the gap for cyber security jobs set to run into several millions, we are putting ourselves at risk in new and unprecedented ways.

Consequently, positive processes are necessary to ensure that our organisations are secure when looking to the future. When considering what positive cyber security processes entail, the below can be used as an outline:

- Organisations need to establish robust cyber security policies and procedures and operationalise them consistently across the organisation.

- Businesses should clearly identify and clarify roles, responsibilities, and protocols for handling sensitive information and responding to threats.
- Regular employee training sessions on cyber security best practices and emerging threats are essential to foster a culture of awareness and vigilance.
- Additionally, we need investment in cutting-edge cyber security technologies such as managed SOC services, intrusion detection systems, encryption tools, and endpoint protection software to safeguard against potential breaches.
- Regular risk assessments and audits to identify gaps and vulnerabilities and promptly address them are essential for our organisations.
- Encourage open communication channels for reporting suspicious activities or potential security breaches is also a necessity.
- Cyber Security is a collective responsibility that requires continuous effort, collaboration, and adaptation to stay ahead of evolving threats.

This can be achieved through a comprehensive cyber security strategy that takes into account all aspects within the organisation that can open up risk. The report has so far explored geopolitical threats, third-party risks, regulations, and new technologies—all aspects that increase the threat landscape. Nevertheless, to ensure we stay secure, we must also:

1 Identify Our Goals

The foundation of a security framework depends on our businesses' industry, location, and tools. Since regulations vary by sector and country, such as HIPAA for US healthcare versus NHS compliance in the UK, our organisation's frameworks must be tailored to their specific needs. Identifying these requirements and goals is essential for creating an effective security solution.

2 Conduct a Thorough Risk Assessment

A comprehensive risk assessment helps identify vulnerabilities in our organisations' current cyber security measures. This includes evaluating potential threats and continuously updating as risks evolve. The assessment provides a clear picture of where improvements are needed and informs the direction of our security frameworks.

3 Mitigate Human-Related Risks

People are often the biggest security risk. Establishing internal protocols around access to sensitive information can help mitigate this. Regularly reviewing who has access, requiring non-disclosure agreements (NDAs), and developing strong security policies ensure that employees handle information responsibly.

4 Adopt Security Standards

Incorporating recognised security frameworks provides structure and consistency. Common frameworks include ISO 27000 (information security management), NIST (cyber security for US federal contracts), CIS (cloud and remote work security), and GDPR (personal data protection in the EU). Adopting these standards helps align your framework with industry best practices.

5 Prepare for Breaches

A breach response system acts as your second line of defence when prevention fails. This system should cover all stages of a breach, from identification to recovery. Regularly updating the response plan ensures it stays effective against evolving threats, and training staff to respond to breaches is key to limiting damage.

6 Secure Your Data

Encrypting sensitive data is crucial, especially with increasing reliance on cloud storage. Robust encryption not only protects against data theft but also builds trust with clients. Implementing strong encryption protocols enhances your company's reputation for handling data securely and prevents our information from being an easy target.

7 Maintain a Recovery Plan

A security disaster recovery plan is essential for minimising the impact of a breach. This plan, separate from our business continuity plans, should outline roles, responsibilities, and procedures for responding to a security incident. Regular drills ensure that employees are familiar with the plan, enabling a quick and organised recovery if a breach occurs.

A part of building this plan and a holistic approach to cyber security through our organisations is to ensure we build a good GRC strategy. Governance, risk, and compliance (GRC) is an operational strategy that helps organisations align IT activities to business goals, manage risk effectively, and stay in compliance with government and industry regulations. The need to manage risk, adhere to regulations, and establish processes to govern those tasks has been part of running an organisation as long as there have been businesses to run; nevertheless, they have now become increasingly essential for our success, especially when cyber security is considered. In the MENA region, despite the importance of such, significant staff shortages have been seen as preventing us from achieving a comprehensive strategy. Meanwhile, this is reinforced as the types of attacks vary through the region, with 29% from eCrime, 14% from Nation States, 36% Unattributed, and 21% from Insider Threats. Hence, this emphasises the significance of creating a good strategy due to the range of threats faced. This can be done through:

- **Ensuring we choose the Correct GRC Software:** GRC software aids in risk assessment, compliance automation, audit management, and document management, allowing organisations to automate manual tasks and focus on strategic work.
- **Fostering collaboration between GRC and cyber security teams:** This can be done in a range of areas to ensure we enhance accountability, threat

intelligence, incident response, and communication, while also ensuring a culture of information sharing.

- **Defining Clear Roles and Responsibilities:** This is through having clear roles in a GRC cyber security team, such as GRC lead, compliance analyst, cyber security analyst, and risk analyst. Through defining these key roles, it can ensure transparency, trust, and efficient issue resolution.

- **Leveraging Technology for Collaboration:** Technology can help facilitate information collection and sharing, thus helping to further collaboration. It also aids in data visualisation, and improves communication within the GRC and cyber security teams.

- **Aligning Business Processes and Objectives:** Aligning operations and objectives with GRC strategies can significantly help to identify and mitigate risks, achieve business goals, manage threats, and adhere to regulatory standards, fostering a culture of risk awareness.

- **Ensuring Continuous Monitoring and Improvement Internally:** Persistent oversight, post-incident reviews, and leveraging insights for refining security measures can ensure an organisation's GRC cyber security framework adapts to changing threats, regulations, and business needs.

- **Implementing Data Security Measures:** Protecting customer data and private information, adapting to evolving risks, and regularly updating the GRC framework aligned with business demands and risk profiles can help to ensure that our business' data stays secure.

Meanwhile, human-centric factors are becoming increasingly significant when considering what can be done to secure our systems. This is because human error continues to contribute to a significant number of security incidents, yet current approaches to mitigating this risk are failing to have the desired impact. Many organisations continue to not prioritise effective management of this risk and have historically relied upon security awareness to influence security behaviour; however, this neglects necessary considerations surrounding awareness and behaviour of our employees to ensure our businesses stay secure.

In the UAE, 83% of CISOs have identified human error as the leading cyber security risk, despite the fact that the number of CISOs that feel their organisation is at risk of a material cyber attack over the next 12 months has fallen from 75% to 70%. Although there's growing optimism in the role of AI-powered solutions to mitigate human-centric risks, we cannot solely rely on this. Hence, more needs to be done to build a human-centric approach to cyber security. Hence, to achieve this, the below recommendations have been made:

- **Recognise Security Weaknesses:** This can be done by adopting an attacker's mindset to identify key vulnerabilities.

- **Enhance Awareness Training:** This can be achieved through comprehensive training methods, including sharing phishing examples and conducting mock attacks, to effectively change employee behaviours and improve vigilance.

- **Boost Security Team Skills:** IT teams need a blend of technical, analytical, and interpersonal skills to effectively protect networks, spot threats, and manage teams without burning out.

- **Cultivate Security by Design Culture:** Embedding security into the organisational culture involves understanding its intersection with other business aspects and empowering employees with contextual knowledge to prioritise protection.

- **Adopt a Socio-Technical Approach:** This can be done through investing in interdisciplinary research to develop more memorable and immersive cyber security solutions, blending psychology and technical expertise.
- **Stress-Test Solutions:** Businesses should not solely rely on normal working conditions to understand cyber risks. Instead, solutions should consider factors like workload, time pressure, and stress, with the workforce fully aware of potential impacts.

Meanwhile, when considering a holistic cyber security approach, ensuring we get the budget necessary, along with communicating with board-level executives, is necessary so we can overcome these challenges in our organisations. This is illustrated as cyber security revenue is expected to show an annual growth rate (CAGR 2024-2029) of 8.50%, resulting in a market volume of US$6.36bn by 2029 in the region. Hence, as our organisations begin to invest more, a comprehensive business plan that considers the "human" aspects is necessary. To ensure a good business case for our cyber security strategies, we must ensure appropriate funding, resources, skills, and time can be allocated to effectively manage cyber security risks. This can be done by setting out:

Strategic Case: Where you demonstrate the need for change and show how the proposal fits with local, regional, and national policies and targets.

Economic Case: Where you will explain how you are providing the best public value to society.

Commercial Case: Where you outline the relationship between the public sector and service providers and how third-party vendors and investment can best help us.

Financial Case: Where you set out the affordability and preferred funding model through setting out protections of how investment can help

Management Case: Where you describe the delivery, monitoring, and evaluation structure through setting out people's roles and responsibilities as well as the processes in place to stay secure.

Therefore, in this section we will walk you through why it is necessary for our businesses to fully understand the risks posed by cyber attacks to build a holistic strategy. This is through exploring how we can best overcome the "people" problem by building a human-centric cyber security strategy ready for tomorrow and where we can build a holistic strategy through our organisations through utilising tools such as collaboration, among others.

INTERVIEW

What Does a Good Comprehensive Cyber Security Program Look Like?

Muhammad Khurram Khan, Founder & CEO

A comprehensive cyber security program integrates key elements like risk assessment, robust security policies, identity and access management, and advanced network protection to safeguard an organisation's data and systems. It includes continuous monitoring, threat intelligence, and incident response plans to ensure swift action against breaches, while security awareness training reduces human error risks. The program also addresses endpoint security, third-party risk management, and compliance with industry regulations, ensuring encrypted data protection across all layers. Ultimately, it's a dynamic, multi-layered defence that evolves with emerging threats to provide continuous protection.

INTERVIEW

Could You Give Us Quick Tips For a Human-Centric Strategy?

Darweesh Al-Buainain, CISO

My top tips for a human-centric strategy would be to:

- Assess and understand the Human Factor in The Cyber Security Threat Landscape
- Monitor and record behaviour changes
- Design and build human centric awareness program
- Get company buy-in
- Monitoring and reporting the results
- Identify gaps and area of improvement

INTERVIEW

How Can We Best Build a Human Centric Cyber Strategy?

Sedat Salman, Global Solution Architect / Technical Manager

Schneider Electric

A human-centric cyber strategy starts with the understanding that people are the first line of defence in cyber security as well as possibly its weakest link. It is about realising and resolving the human variables that affect security results rather than only concentrating on technology.

This entails accepting the part of cognitive biases, social engineering tactics, and human errors in cyber attacks. Organisations can create more user-friendly security products, create a culture of shared responsibility for cyber security, and create more successful security awareness initiatives by understanding the complexity of human behaviour. The significance of individual empowerment is also emphasised by a human-centric approach. This entails offering thorough education and training programs that go beyond fundamental awareness, giving staff members the know-how to recognise and react to.

Furthermore, by giving people thorough training and instruction that goes beyond basic awareness and gives them the knowledge and skills to recognise hazards and successfully respond to them, a human-centric approach empowers people. In order to report security problems without fear of retaliation, it also entails fostering a supportive environment. Active engagement in cyber security initiatives is promoted and a sense of ownership is cultivated when security-conscious behaviour is acknowledged and rewarded. Essentially, people are seen as significant assets in the continuous battle against cyber threats rather than just potential vulnerabilities when employing a human-centric strategy.

INTERVIEW

What Is The Significance Of Collaboration For Our Cyber Security Strategies? How Can We Ensure More Cooperation?

Abhinav Kumar, AVP – Information Security

nmc

Collaboration is vital in cyber security because it enables organisations to share knowledge, resources, and strategies, strengthening defences against evolving threats. Organisations can respond more effectively to incidents and reduce vulnerabilities by pooling expertise and intelligence. Collaborative efforts also help develop standardised protocols, enhancing security and regulation compliance.

Building trust among stakeholders through transparency and reliability is essential to ensure more cooperation. Establishing formal frameworks, such as information-sharing agreements, and creating incentives for participation can also encourage collaboration. Regular communication via industry forums, public-private partnerships, and secure technologies that facilitate information exchange is essential. Continuous education and awareness programs will further reinforce the importance of cooperation in achieving robust cyber security strategies.

We shall also ensure that we create an environment of inclusion for professionals, researchers, students, and people outside IT. If we do not expand the reach of cyber resilience beyond the cyber security team, it will be challenging for the organisation to safeguard itself against all modern-day attacks. We rely primarily on our vendors for innovation, but if we work together, we can develop stringent strategies to counter new-age cyber-attacks.

Conclusion_

Concluding Remarks & Recommendations_

This year's annual study covers a wide range of topics, including various industries' approaches to Cyber security. Even though there are still many threats to contend with, this report has highlighted some of the ways security professionals can adopt a variety of strategies at their disposal to manage cyber risk. We have spoken to a number of specialists from throughout the Middle East and Northern Africa, each with their own unique insight into safeguarding our biggest companies from a range of sectors from both new and traditional cyber threats. Consequently, to summarise what we have discovered through this report.

The first section of this report explored the current threat landscape through the MENA Region and, more particularly, how we can overcome common cyber security threats. It explored the common cyber threats faced and dug deep into the geopolitical issues and their impact. It also explored the new regulatory landscape for the Middle East and Northern Africa and highlighted the areas we need to be aware of to ensure our cyber strategies are up-to-date and prepared for the threats coming our way. It has then explored the state of cyber security in the region from three key angles: people, processes, and technology.

Based on our conversations with our steering committee members and expert speakers, here are our recommendations for overcoming the issues that come with increasingly prominent threats to our organisation's cyber security. They include:

1 Stay Ahead Of The Current Threat Landscape

Moving forward, we must stay ahead of the current threat landscape. Being aware of the threats faced, whether financial or geopolitical, will help us stay one step ahead of potential attackers.

2 Stay Vigilant Of Both The Benefits & Drawbacks Of New Technologies

We must also remain vigilant about the benefits and drawbacks of new technologies such as artificial intelligence.

3 Develop Cyber Security Strategies Considering All Elements Of The Organisation

When developing a cyber security strategy for the future, we must develop one that considers all elements of our organisations. We must place humans at the centre of our strategy while also considering the business implications in order to secure funding. All of this together will help our organisations develop a comprehensive program to ensure our organisations can stay secure.

These guidelines can be applied to both companies across industries. Nevertheless, this ultimately acts as a baseline for what can be implemented, with more tailored solutions required for differing organisations. For a starting point, it can also be useful to consult the NIST Cyber Security Framework, as well as use and read further into the guidelines set by each country's states. Ultimately, this can all help to ensure acceptable baselines are set out within your organisations, with a clear framework for securing our infrastructure moving forward.

Further Readings_

- **Artificial Intelligence for Cybersecurity:** Literature Review and Future Research Directions. Kaur et al, Apr 2023. https://www.sciencedirect.com/science/article/pii/S1566253523001136
- **IBM Security X-Force Threat Intelligence Index 2023:** IBM White Paper. https://www.ibm.com/reports/threat-intelligence
- **PWC Global Digital Trust Insights Report:** https://www.pwc.com/us/en/services/consulting/cyber security-risk-regulatory/library/global-digital-trust-insights.html
- **UAE Cyber Security Council:** State of Cyber Security Report 2024, https://cpx.net/insights/reports-whitepaper/state-of-the-uae-cyber security-report-2024/
- **How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cyber Security Workforce**, ISC2 White Paper, November 2023, accessible here: https://mysecuritymarketplace.com/reports/how-the-economy-skills-gap-and-artificial-intelligence-are-challenging-the-global-cyber security-workforce-2023/
- **Deloitte Cyber Risk Capabilities in The Middle East**: https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/risk/me_risk_cyber-risk-capabilities-in-the-Middle-East.PDF
- **Saudi National Cyber Security Strategy:** https://nca.gov.sa/ar/national_cyber security_strategy-en.pdf
- **UAE National Cyber Security Strategy:** https://tdra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf
- **Qatar National Cyber Security Strategy Outline 2024-2030:** https://www.linkedin.com/pulse/qatar-national-cyber-security-strategy-2024-2030-synopsis-khan-5lzpf/
- **State of the UAE - Cyber Security Report 2024:** https://www.cpx.net/media/hocl331j/state-of-the-uae-cyber security-report.pdf

Special Thanks To Our Contributors_

- Mousab AlSaaydeh, Head of cyber security, **Confidential**
- Ala' Zayadeen, Head of Information Security and Data Privacy, **BinDawood Holding**
- Mansoora Shafi Qazi, VP Information Security, **First Abu Dhabi Bank (FAB)**
- Albandari Alsumayt, Assistant Professor and Head of Department, **Imam Abdulrahman Bin Faisal University**
- Darweesh Al-Buainain, CISO, **Saudi Aramco Total Refining and Petrochemical Company (SATORP)**
- Sedat Salman, Global Solution Architect / Technical Manager, **Schneider Electric**
- Khaled Khaled, Group OT Cyber Security Project Manager, **Air Liquide**
- Ali Ismail Awad, Associate Professor of Cyber Security, **United Arab Emirates University**
- Moath Sakaji, MEA OT/ ICS Security Consulting Lead, **Mandiant**
- Krishna Dixit, Senior Cyber Security Officer, **Schneider Electric**
- Muhammad Khurram Khan, Founder & CEO, Global Foundation for Cyber Studies

MENA Cyber Summit 2025 Steering Committee_

- Albandari Alsumayt, Assistant Professor and Head of Department, **Imam Abdulrahman Bin Faisal University**
- Fatema Fardan, Digital Security Lead, **Bank ABC**
- Ibrahim Jamus, System Engineering Manager, **EVAD-ME**
- Mousab AlSaaydeh, Head of Cyber Security (Vendor), **Confidential**
- Ala' Zayadeen, Head of Information Security and Data Privacy, **BinDawood Holding**
- Vishal Vaghela, Chief Information Security Officer, **Americana Restaurants**
- Mansoora Shafi Qazi, VP Information Security, **First Abu Dhabi Bank (FAB)**
- Ali Ismail Awad, Associate Professor of Cyber Security, **United Arab Emirates University**
- Krishna Dixit, Senior Cyber Security Officer, **Schneider Electric**
- Muhammad Khurram Khan, Founder & CEO, **Global Foundation for Cyber Studies and Research**

UNLOCK A WORLD OF PREMIUM CONTENT

SUBSCRIBE

Access curated content about the lastest developments in the **MENA region cyber security landscape**.

Subscribe now for even more **expert insights, interviews, reports** and **more**:

SUBSCRIBE FOR CONTENT

ATTEND

Join trailblazing **IT security leaders** at industry leading events to **gain more insights** and **knowledge** towards shaping the future of cyber security across the globe.

Check out our **upcoming cyber security events calendar** and **save 30%** on all passes with the code "**CYBER-RESILIENCE**":

VIEW UPCOMING EVENTS

SPONSOR

Showcase your solutions directly to **100s of cyber security decision maker**s at one of our world-renowned events.

Request a **Sponsorship Pack** to discover more about how we can help you tap in to the **APAC, MENA, European, Canadian, North American, ANZ** & **LATAM** markets:

REQUEST A SPONSOR PACK

HOST

Forge new relantionships and **network** in an intimate setting with **IT & OT security budget-holders** from a database of **1.5 million senior stakeholders**.

Target by industry, location, job title and function for **maximum ROI**.

HOST AN EXECUTIVE DINNER

A Report Issued By

#MENA CYBER SUMMIT

MENA Cyber Summit is part of the Cyber Series

Our mission is to empower professionals and organisations with cutting-edge insights, strategies, and networking opportunities essential for navigating the ever-evolving landscape of digital security.

We understand the importance of building and bringing together communities of cyber security experts. We're dedicated to creating spaces where professionals can exchange ideas, discuss challenges, and collaborate on innovative solutions.

cyberseries.io