Anticipate today, protect tomorrow

UAE CISO survey 2020
When KPMG’s inaugural UAE chief information security officer (CISO) survey was launched, little did we expect the challenges the world would face in 2020.

The pandemic has forced organizations to rapidly adapt to new ways of working, while simultaneously aiming to ensure adequate security measures are in place. Businesses – particularly their technology-related functions– are grappling with rapid implementation of remote access solutions, collaboration tools and cloud-based services.

Coinciding with this vast operational shift is a five-fold increase in cyberattacks\(^1\). Perpetrators have quickly begun to exploit new vulnerabilities – both technical and human in nature – laid bare by the pandemic. UAE-based organizations’ cybersecurity strategies are being put to the test by new threats and a dizzying array of vulnerabilities not previously considered by CISOs.

As organizations adjust to this new reality, agility is an important factor. Each organization is only as secure as its employees, applications, or third parties, and must pivot accordingly.

Based on KPMG’s experience and input from local CISOs, we have highlighted key cybersecurity-related challenges faced across sectors within this publication.

We hope you find this year’s report informative and insightful. Please feel free to contact us with any comments or queries.

\(^1\)https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
Contents

Foreword .......................................................... 2

Executive summary ........................................... 5

1. The cybersecurity landscape ......................... 9

2. CISOs are evolving ...................................... 13

3. The CISO of the future:
   adaptive and augmented............................ 23

Conclusions ..................................................... 29

Methodology ................................................... 31

About KPMG ............................................... 32
Fending off threats

A majority of chief information security officers (CISOs) we surveyed in the United Arab Emirates (UAE) believe cyber criminals to be one of the biggest risks they currently face. 2020 has seen a significant increase in phishing and ransomware attacks, as described in our recently released report on the ongoing 2020 ransomware campaigns. Indeed, 88% of CISOs see phishing as one of the biggest cyberattack threats.

CISOs are not the only members of the C-suite to be concerned about cybersecurity. More than a third of those surveyed (39%) stated that minimizing the impact of a cyber-attack on the availability of customer or citizen services is a concern for their organization’s board. Indeed, according to the research, cybersecurity spending has increased in recent years and CISOs predict the trend will continue. As adoption of new technologies and digital platforms accelerates, so too will the cyber threat.

As the digitalization race becomes a marathon, the UAE continues to take steps to adopt appropriate legislation and regulations with respect to cybersecurity and data protection. The objective of these regulations and legislation is to protect citizens as well as organizations operating in the country, often building on international best practice, such as the General Data Protection Regulation (GDPR).

These regulatory changes have prompted a shift in many companies’ information security agendas. In fact, nearly half of respondents stated their security posture had improved due to the advent of new cybersecurity laws.
Addressing the new cybersecurity landscape

Ninety percent of UAE-based CISOs expressed confidence in introducing cloud technologies and 44% are confident their organization has prepared above the industry average to effectively respond to cybersecurity incidents.

CISOs’ priority areas include:

- **72%** Strengthening cyber defense and threat management activities: 72% have an established computer security incident response team (CSIRT) to respond to incidents.
- **80%** Ensuring comprehensive application and infrastructure security assessments are performed. This is true for 80% of organizations.
- **40%** Testing incident response capabilities: 40% of respondents currently perform cyberattack simulation exercises.

Planning ahead, CISOs are looking to automate their organizations’ activities. Future investments will primarily focus on:

- Identity and access management
- Security orchestration, automation and response (SOAR)

Finding the right cybersecurity skillset is key to addressing current and future challenges. CISOs listed two profiles and skillsets that seem difficult to find:

- Cyber incident response: threat intelligence and SOAR
- Security and privacy by design: secure DevOps (the combination of development software and IT operations) and data privacy

Agility and optimization will likely be key

In terms of cybersecurity investment, organizations in the UAE have seen budgets increase over the past two years. However, it is unclear whether this trend will continue, given potential Covid-19-related budget cuts. Organizations are faced with the challenge of optimizing cybersecurity costs and performing cost-benefit analyses, while simultaneously innovating and adopting new technologies at breakneck speed.
Key figures from our survey

39%
Minimizing the impact of a cyberattack on the availability of customer or citizen services is a concern for the boards of 39% of organizations.

23%
... Yet only 23% of respondents have embedded security and privacy by design into their waterfall and agile project methodology.

47%
of organizations in the UAE believe cyber criminals to be one of the biggest threat.

94%
of CISOs believe that protecting customer data is vital in gaining consumer trust....
40% of CISOs believe that cybersecurity technologies that improve compliance against regulatory requirements are more likely to obtain management approval than other promised business benefits.

$1,791m

SOAR is a key area of investment in cybersecurity innovation. The SOAR market is projected to grow to USD 1,791 million by 2024.2

79%

of CISOs have seen their cybersecurity spend increase over the past two years.

44%

of respondents do not conduct a cost-benefit analysis when deciding how cyber risk should be treated.

The murky world of cybercrime is inhabited by various actors that play by different rules from the rest of society and are driven by conflicting motivations. Identifying threat origination is key to predicting future attacks and protecting organizations against their tactics.

Nearly half (47%) of CISOs in the UAE perceive cybercriminals to present one of the biggest threats. Such concerns are underscored by the rise in ransomware and phishing attacks seen in the UAE over the past few months, as described in our recently released report on the ongoing 2020 ransomware campaigns, accentuated by the Covid-19 pandemic. This also includes advanced persistent threat (APT) groups WildPressure and Anonymous, which respectively are driving malware and doxing campaigns (“dropping dox” is an online attack in which hackers publish personal information and documents about an individual to expose the internet the identities of people wishing to remain anonymous).

What cyber attack group do you believe is the biggest threat to your organization?

<table>
<thead>
<tr>
<th>Attacker Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber criminal</td>
<td>47%</td>
</tr>
<tr>
<td>Nation state</td>
<td>19%</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>19%</td>
</tr>
<tr>
<td>Insider</td>
<td>16%</td>
</tr>
</tbody>
</table>

Single response

Of less – but still significant – concern are nation-state actors, hacktivists, and insiders. These segments are less motivated by monetary gain and more by disruption or exposure. They are also more likely to target individual organizations, increasing the need for sophisticated defense tactics.
Amongst the various types of attacks, phishing is considered the biggest threat (88%), followed by malware (56%) and ransomware (53%). Phishing campaigns have become progressively more widespread, with a significant number of cyber criminals leveraging the ongoing Covid-19 pandemic. APT groups, such as Mustang Panda (based in China) and others, have been exploiting pandemic themes as a lure. Phishing often serves as the first step in a well-organized attack chain, frequently followed by more sinister attacks, such as ransomware and data exfiltration.

Our recent report on 2020 ransomware campaigns finds an uptick in the deployment of ransomware, such as REvil/Sodinokibi and Defray. These are widely linked to ongoing malicious attacks in the oil & gas and healthcare sectors, as well as recent global attacks on the public sector. Wannacry is still active, largely due to the widespread use of legacy systems. There is no immediate solution, as cybercrime actors are well-coordinated and highly organized.

Cybersecurity is a board-level concern

Business leaders across the UAE increasingly find cybersecurity to be high on their agenda, with a majority of CISOs (66%) providing cybersecurity updates directly to their organization’s board. Greater board-level awareness may be a key factor in explaining increased cybersecurity budgets among local companies.

While the majority of boards view cybersecurity as an enabler for growth, the function is also viewed as a cost of doing business – particularly in a post-Covid-19 world. This equation may be key in future cost-cutting decisions. If boards continue to view cybersecurity as an enabler for growth, they may be inclined to sustain its funding and find other cost centers to trim. However, as the pandemic weighs on organizations’ financial well-being, many are faced with tough financial decisions.

System availability versus data protection

Our survey found a perceived divergence in cybersecurity-related concerns. According to CISOs, approximately one-third (39%) of boards in the UAE are primarily concerned about the impact of cyberattacks on the availability and integrity of critical customer—or citizen—facing systems, with 24% being concerned about the theft of customer data. Two-thirds of CISOs (67%) believe that managing and protecting customer data is as important as delivering a product or service.
Regulation on data protection backs the CISO agenda

According to this year’s survey, 77% of CISOs agreed they are accountable for protecting customer data, confirming that privacy sits within their remit.

Locally, we have seen the data protection regulatory regime shifting, as organizations strive to comply with requirements established by freezones, emirate and/or federal directives and at a global level. For instance, in the financial sector, Dubai International Financial Center (DIFC) and Abu Dhabi Global Market (ADGM) have issued data protection laws. The DIFC’s revised Data Protection Law 2020, ADGM’s Data Protection Law and the Federal Law No. 2 of 2019 are codifying and mandating the protection of personal data – steps that the majority of CISOs already agree are necessary.

Other recent legislation includes:

- National Electronic Security Authority (NESA) Information Assurance (IA) standards, relevant to the financial and oil & gas sectors
- Abu Dhabi Healthcare Information and Cybersecurity Standard (ADHICS), to ensure security in the healthcare sector
- Dubai Electronic Security Center (DESC), covering industrial control systems standards

The UAE is one of the Middle Eastern region’s largest trading partners with the European Union (EU); 40% of UAE-based organizations are subject to EU General Data Protection Regulation (GDPR).

If a local organization processes personal data of subjects located within Europe, not only do they have to comply with the conditions set out in the GDPR, they must also appoint an EU-based representative in order to comply with Article 27 of the regulation.

Global standards have shaped reforms, such as those implemented by the DIFC and the ADGM, and encouraged compatibility.

Thus far, it appears such reforms have had a positive impact, with the vast majority of CISOs (89%) stating their security posture has improved due to the advent of new cybersecurity regulations.
Data protection principles such as transparency, individual rights and accountability have become key pillars within any effective data governance programme. The way in which your organisation manages, processes and shares personal data is likely governed by global data protection laws, privacy obligations or consumer expectations.

Sami Mohammed
Head of The Office of Data Protection, Abu Dhabi Global Market
Internal personnel and testing capabilities are key

Given the rapidly changing technological environment, it is important to highlight that 72% of CISOs have a computer security incident response team (CSIRT) in place. While this indicates an appetite for maintaining internal cyber capabilities, outsourcing and managed services remain a necessity for many organizations in order to either address existing deficiencies or to boost defenses. Indeed, fewer than half (44%) of surveyed CISOs described their organization's cyber-attack preparedness as “above average.”

How would you describe your organization’s preparedness to effectively respond to a cyber attack?

- Above average: 44%
- Average: 41%
- Below average: 12%
- Very poor: 3%

Single response
In the new reality, organizations must be resilient and flexible. They must be able to run their operations from their physical headquarters, but also support highly flexible remote working practices with no impact on their security, resilience and continuity requirements. In fact, Dubai ranks second globally among the largest cities in the world for remote working. Our focus at Dubai Tourism is on building and testing resilience and continuity over the years has helped us to seamlessly adapt to the rapidly changing situation, enabling a remote working environment and preventing disruption to Dubai’s critical activities. Equally important, is a strong security foundation in safeguarding data, platforms, networks and sector-wide services.

Ayesha Bin Lootah
Director Internal Audit, Risk Management & Information Security, Dubai Tourism

Methods vary
Cybersecurity incident response plans can be tested using a variety of approaches – ideally with the involvement of key stakeholders. Forty percent of UAE-based organizations perform cyberattack simulation exercises to test their incident response plans, understand teams’ capabilities, and identify opportunities for improvement. Organizations also leverage other approaches, with 33% of respondents performing red team exercises and 27% undertaking tabletop exercises. Another common (and trending) approach is the use of cyber range gaming simulations.

With the advent of decentralized working styles prompted by the Covid-19 pandemic, inter-department cybersecurity strategies are crucial. Approximately half (53%) of organizations failed to involve stakeholders from security, technology, and other operational teams when testing incident response plans. Without involving all relevant stakeholders, organizations risk contributing to the creation of additional vulnerabilities over time.
Cybersecurity risks are widespread

Just as inter-departmental cybersecurity strategies are important for full organizational buy-in, assessing risks across different organizational elements is key to developing and implementing a holistic cyber defense.

CISOs are most likely to assess the potential for risk associated with infrastructure (86% of respondents) or applications (83%). Given attention to these elements, along with third parties (72%), it appears that CISOs are most wary of threats originating – in whole or part – externally.

Over half of the respondents also stated they perform business process security risk assessments. Other, less common types included those related to industrial control systems (performed by specific industries), as well as network security.

Given the impact of the Covid-19 pandemic, many organizations are likely to increase cyber risk assessments related to remote working infrastructure security, either as a dedicated exercise or as part of a larger analysis.

Innovation is driven by several key technologies

Cybersecurity is a fast-changing domain, with constant technological developments promising better security solutions. Several emerging technologies, such as artificial intelligence, machine learning and robotic process automation, are leading the way.

Advancements such as security orchestration, automation and response (SOAR) leverage some form of machine learning or artificial intelligence to make better-informed decisions on behalf of already overburdened cybersecurity teams.

When asked which technology areas were most likely to receive significant funding over the next 12 months, identity and access management (IAM) stood out as a clear winner.

What type of cyber risk assessments are carried out in your organization?

- Infrastructure security risk assessment: 86%
- Application security risk assessment: 83%
- Third-party risk assessment: 72%
- Business risk assessment: 56%

Multiple response
Which technology areas are most likely to receive significant funding over the next 12 months?

- **Preventative technologies**: 48%
- **Identity and access management technologies**: 58%
- **Response technologies**: 39%
- **GRC technologies**: 32%
- **Threat intelligence technologies**: 42%
- **Detective technologies**: 29%
- **Others**: <10%

IAM investment is timely. The majority of businesses are depending on teleworking and telecommuting infrastructure, requiring staff to gain access to data from multiple devices across diverse locations. If adequate IAM tools are not employed, organizations could be left vulnerable to cyber-attack.

Multiple response
Digital enablement of cybersecurity

As shown in the graphic below, technology solutions such as SOAR will be most transformative for cybersecurity functions in the UAE over the next two years.

Which of the following technologies or solutions do you believe will be most transformative for your cyber security function over the next two years?

- **39%** Security orchestration, automation and response (SOAR)
- **29%** AI-based risk assessment
- **29%** Real-time security configuration monitoring and management
- **29%** AI-based threat analytics and user & entity behavioral analytics (UEBA)
- **26%** Data privacy technologies
- **26%** Cloud delivered security solutions
- **26%** AI-based Malware Prevention and Endpoint Threat Detection (EDR)
- **19%** AI-based data leakage prevention
- **19%** Password-less authentication
- **16%** Cloud access security brokers (CASB)
- **16%** SDLC and SecDevOps

Multiple response

Widespread technology adoption brings big benefits and risks

Technologies such as cloud computing, robotic process automation (RPA), artificial intelligence, big data, blockchain, and the Internet of Things (IoT) are being used across many UAE-based organizations. As stated earlier, CISOs must aim to continuously calculate the risks of rapid deployment against the benefits of technological innovation.

Adoption of cloud and other new technologies requires CISOs to adapt to the new ways of working, and embed security into the organization’s ‘waterfall’ or agile processes. Embedding security from the start of the product or project lifecycle rather than as an afterthought is called “shifting left”.

Enabling new projects

Despite potential threats, 90% of CISOs are more confident with respect to introducing cloud technologies compared to previous years. This increased confidence is likely the result of maturing cloud security standards, as cloud service providers have clearly defined security responsibilities and compliance. Covid-19 lockdowns have also pushed organizations to meet the demands of teleworking.

Although 90% of CISOs are confident about moving to the cloud, only 23% confirmed that security is embedded in the design and acquisition phase of the software development lifecycle (inclusive of both waterfall and agile processes).

This indicates that it is important for CISOs to consider Security and Privacy by Design. This is likely to be key to the successful transition to cloud first and new technologies, particularly as part of DevOps.

Moreover, secure and compliant cloud(s) require a clear understanding of cloud provider, consumer, third party, and broker security responsibilities. Communicating security expectations to all concerned parties can be critical, in addition to developing a target state-operating model that delineates shared responsibilities for securing data across anticipated cloud needs.
“Building security and privacy by design into everything we do at Emirates NBD has been a key focus for me and my team – this ensures that security is embedded throughout our software development lifecycle without losing any of the required agility to meet the business’s needs. This approach has been particularly crucial given our cloud first strategy and innovation agenda across the bank. But more important than any technical initiative, has been the culture change required to put security at the heart of everything we do.

Darwish Azad
Group Chief Information Security Officer, Emirates NBD

Is security integrated into the full software development lifecycle for all of your projects (including third party technology projects)?

- Yes, but on an ad hoc basis: 55%
- Yes, fully adopted secure development lifecycle processes for both Waterfall and Agile projects: 23%
- No, not integrated: 13%
- Not relevant: 10%

Multiple response
Skills gap
Finding people with the relevant skillsets is an oft-cited challenge in cybersecurity functions. Considering the importance UAE-based CISOs have placed on building internal cybersecurity teams, addressing existing and potential skill gaps can be a key success factor.

The cybersecurity skills shortage can be categorized into two main areas:

**Detection capabilities:** threat intelligence, security operations, and incident response are key areas where cybersecurity skills fall short.

**Security and privacy by design:** Next in terms of skill shortage, 24% of CISOs identified a resource shortage in both DevSecOps, and data privacy.

Nearly all CISOs (95%) agreed that overall cybersecurity headcount is likely to continue to increase. This projected trend must be analyzed alongside a continued appetite for managed security services, which are currently used by 61% of respondents. Of those, 30% leverage managed services to “increase capability and skillset” and 25% to “reduce the cost of operations”. Overall, 47% believe that managed security services usage will increase significantly.

<table>
<thead>
<tr>
<th>Function</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC analyst</td>
<td>26%</td>
</tr>
<tr>
<td>Threat analyst</td>
<td>26%</td>
</tr>
<tr>
<td>Data Privacy analyst</td>
<td>24%</td>
</tr>
<tr>
<td>DevSecOps</td>
<td>24%</td>
</tr>
<tr>
<td>Incident response</td>
<td>24%</td>
</tr>
<tr>
<td>Security architect</td>
<td>19%</td>
</tr>
<tr>
<td>Cyber compliance</td>
<td>16%</td>
</tr>
<tr>
<td>Emerging technology risk</td>
<td>16%</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>16%</td>
</tr>
</tbody>
</table>

Which functions suffer most from a skills shortage in your company?
Increasing cybersecurity spend
Cybersecurity expenditure falls into three main areas:

- governance risk and compliance
- improving security controls
- innovation

While more than three-quarters of CISOs (79%) stated that their budgets had increased over the past two years, only about half believe their current cyber innovation budget is sufficient.

Not surprisingly, cyber governance, risk and compliance garners the highest spend – much of this can be attributed to mandated cybersecurity features. To determine budget allocation for other areas, such as security controls and innovation, performing cost-benefit analyses is key for CISOs in the UAE to adapt to the ever-evolving cybersecurity landscape.

However, such analyses are not as widespread as they perhaps should be: approximately 44% of organizations do not evaluate such aspects when assessing how cyber risks should be treated.

Adapting to major changes and disruption: Cybersecurity and Covid-19
The shift to remote working has accelerated the adoption of technologies which are inherently more vulnerable to cyberattacks than their predecessors:

Cloud solutions:
A majority of cloud solution providers have recorded an increase in demand in the UAE, as organizations are prioritizing cloud adoption and large-scale application delivery solutions.

Identity and access management (IAM):
Leading IAM solution providers have recorded upticks in their global adoption rate between Q1 and Q2 2020. This is correlated to the increase in remote access provided to employees and third parties.

Digital transformation:
Locally, interest in digital transformation is growing, which increases organizations’ attack surface.

Do you consider your current cyber security budget sufficient to fulfill your role in the following areas?

- Governance, risk and compliance: 72%
- Improving security controls: 69%
- Cyber security innovation: 52%

Single response
Covid-19

Global pandemic declared

>54m* confirmed cases

>217* countries affected

* WHO data on November 2020

As organizations shift from resilience to recovery and adapt to a “new reality,” CISOs are likely to play a pivotal role in transforming the cybersecurity function.

Teleworking

The pandemic has reduced social interaction, driving a use case for IT and organizations to enable working from home capabilities. The goal is to ensure that operations are not impacted and staff have uninterrupted access to organization data and systems at any time.

Teleconferencing

Social distancing is the norm. This has enabled organizations to seek high bandwidth teleconferencing solutions that facilitate online conference meeting with large audiences.

Cloud

Although not a new technology, there is an ongoing surge in cloud adoption as organizations try to meet teleworking demands and reduce operational costs.
Cyberchallenges

Rapid changes in IT architecture and technology seek to accommodate teleworking demands

Notable rise in phishing attacks – specifically exploiting Covid-19

Cybercriminals now shifting focus to vital sectors

Increase in reported vulnerabilities on teleconferencing solutions

Upsurge in usage of multiple personal devices for business activities

Staff need to access organization data from any geo-location and device
03  The CISO of the future: Adaptive and augmented
Although 90% of CISOs are ready to move to the cloud, it is important for them to:

1. Examine the technologies of tomorrow on a sector-by-sector basis
2. Keep a pulse on the technologies of tomorrow
3. Focus on cybersecurity costs optimization

**Sector-by-sector**

**Infrastructure**
- Growth in smart cities and technology investments
- Quality and availability of supply chain of critical national infrastructure

**Healthcare**
- Shift towards telemedicine and remote interventions
- Increase in data driven healthcare insights

**Government and public sector**
- Move towards citizen-centric public services powered by data
- Data protection and security of citizen data

**Transport**
- Global supply chain boosted by the sector, through data and digitization. Focus on efficiencies and cost savings
Keeping a pulse on the technologies of tomorrow

Over the next five to fifteen years, developments from autonomous vehicles to 4D printing and brain-computer interface may change our lives radically and dramatically.

Source: KPMG Global
Optimizing cybersecurity costs

Important questions remain:

- Where can I reduce costs?
- How do I contextualize this within the broader strategic agenda?
- Where should you start?
- How can I get more visibility and insight into my security spend?
- How can I maximize performance of existing investments?
- How can I get cost containment right—whilst still addressing the ever-changing threat landscape and attack surface?
- How can I rationalize the spend across my projects, security tools and people?
- How can I get cost containment right—whilst still addressing the ever-changing threat landscape and attack surface?
- How do I rationalize the spend across my projects, security tools and people?
- How can I maximize performance of existing investments?
- How can I get more visibility and insight into my security spend?
- Where can I reduce costs?

What to consider as you embark on a successful cyber cost optimization journey:

<table>
<thead>
<tr>
<th>How do you contextualize this within the broader strategic agenda?</th>
<th>Where should you start?</th>
<th>How can cost optimization enable you to embrace digital disruption?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take a holistic view on cost optimization, covering areas such as information technology or enterprise risk</td>
<td>Identify ‘low-hanging fruit’</td>
<td>Shift from a ‘save-to-grow’ to a ‘save-to-transform’ mindset</td>
</tr>
<tr>
<td>Provide a clear vision of the future of cybersecurity</td>
<td>Empower change evangelizers to drive the cost optimization message</td>
<td>Optimal combination of defense (immediate cost takeout) and offense (investment in operational efficiencies)</td>
</tr>
</tbody>
</table>

© 2020 KPMG Lower Gulf Limited and KPMG LLP, operating in the UAE and member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the United Arab Emirates. The KPMG name and logo are registered trademarks or trademarks of KPMG International.
CISOs in the UAE have faced multiple challenges in 2020, including managing the effects of the Covid-19 pandemic, accelerated adoption of cloud, remote working and an evolving compliance landscape.

CISOs aim to adapt by supporting continued change across their organizations and embracing the move to digital. Simultaneously they can maintain an acceptable cybersecurity posture and strive for compliance with regulations in a cost-effective manner. CISOs are likely to adopt new ways of working, shifting cybersecurity left into the organization, and embedding the function into the product and project lifecycle from the start, by implementing security and privacy by design.
The increasing cyber threat

- Businesses are operating in a high-threat environment as 47% of CISOs perceive cybercriminals to be the biggest threat actors to their infrastructure; while many organizations have experienced increases in ransomware and phishing attacks, according to our report on the ongoing 2020 ransomware campaigns. Enhanced cybersecurity and privacy regulations are in line with the UAE’s vision to enforce best-in-class legislation and attract investors.

- The majority of organizations have experienced rapid adoption of digital, accelerated by the pandemic.

CISOs are embracing counter measures

Chief information security officers are confident in their ability to address cyberattacks, with 44% of surveyed CISOs describing their organization’s preparedness as “above average.”

- A majority of CISOs are embracing the cloud and digital to build future-focused organizations. To remain agile, CISOs may need to leverage managed services to support operational activities, bringing in niche skills and reducing costs, as 47% of CISOs believe that managed security services usage will increase significantly.

- To address security concerns, the function will need to increase focus on security and privacy by design, as only a minority of respondents have already implemented this.

The successful CISO of the future is adaptive and augmented

- Organizations are seeking to enhance the cyber function by incorporating specialist skills and automation.

- UAE-based organizations are actively preserving disruption and proposing cutting-edge cybersecurity solutions, with a majority of CISOs stating that SOAR and AI-based security technologies are likely to be most transformative for the cybersecurity function over the next two years.

- CISOs are likely to examine the technologies of tomorrow on a sector-by-sector basis, while balancing costs and benefits, as today close to half of the respondents do not evaluate such aspects when assessing how cyber risks should be treated.
The research was conducted using an online survey of UAE-based CISOs over the first half of 2020.

Respondents came from across key sectors including financial services, oil & gas, healthcare and government and there was an appropriate spread.

<table>
<thead>
<tr>
<th>Number of employees</th>
<th>% of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000+</td>
<td>12.5%</td>
</tr>
<tr>
<td>500 to 5000</td>
<td>40.5%</td>
</tr>
<tr>
<td>Less than 500</td>
<td>47%</td>
</tr>
</tbody>
</table>
For almost 50 years, KPMG Lower Gulf Limited has been providing audit, tax and advisory services to a broad range of domestic and international, public and private sector clients across all major aspects of business and the economy in the United Arab Emirates and in the Sultanate of Oman. We work alongside our clients by building trust, mitigating risks and identifying business opportunities.

KPMG Lower Gulf is part of KPMG International Cooperative’s global network of professional member firms. Now entering its 150th year, the KPMG network includes approximately 219,000 professionals in over 147 countries. KPMG in the UAE and Oman is well connected with its global member network and combines its local knowledge with international expertise, providing the sector and specialist skills required by our clients.

KPMG is widely represented in the Middle East: along with offices in the UAE and Oman, the firm is well established in Saudi Arabia, Bahrain, Kuwait, Qatar, Egypt, Jordan and the Lebanon. Established in 1973, KPMG in the UAE and Oman employs 1,485 people across four offices, including about 100 partners and directors.

As we continue to grow, we aim to evolve and progress in order to strive for the highest levels of public trust in our work.

Our values are:

- Integrity: We do what is right.
- Excellence: We never stop learning and improving.
- Courage: We think and act boldly.
- Together: We respect each other and draw strength from our differences.
- For Better: We do what matters.

To meet the changing needs of our clients, we have adopted an approach aligned with our global purpose: Inspiring Confidence, Empowering Change. Our three pillars – exceptional quality of service, an unwavering commitment to the public interest, and building empowered teams – are the foundation of our firm.
Contacts

Tim Wood
Partner
Head of Cyber
KPMG in the UAE and Oman

T: +971 4 249 6525
E: timothywood@kpmg.com

Maliha Rashid
Director
Head of Data Privacy
Cyber Lead, Healthcare, Energy
KPMG in the UAE

E: mrashid5@kpmg.com
T: +971 50 608 2013