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?

<table>
<thead>
<tr>
<th>Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Above average</td>
<td>44%</td>
</tr>
<tr>
<td>Average</td>
<td>41%</td>
</tr>
<tr>
<td>Below average</td>
<td>12%</td>
</tr>
<tr>
<td>Very poor</td>
<td>3%</td>
</tr>
</tbody>
</table>

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

- **Preventative technologies**: 48%
- **Identity and access management technologies**: 58%
- **GRC technologies**: 32%
- **Response technologies**: 39%
- **Threat intelligence technologies**: 42%
- 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.
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?

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

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
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.

Which functions suffer most from a skills shortage in your company?

<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>

Multiple response

95% of CISOs agreed that overall cybersecurity headcount is likely to continue to increase.
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.

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

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance, risk and compliance</td>
<td>72%</td>
</tr>
<tr>
<td>Improving security controls</td>
<td>69%</td>
</tr>
<tr>
<td>Cyber security innovation</td>
<td>52%</td>
</tr>
</tbody>
</table>

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 cyber attacks 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
Global situation

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.

Technology impact

**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
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