Deloitte.

Future of Cyber Survey Report – Middle East Findings

MAKING AN
IMPACT THAT
MATTERS
since 1845

What does the future of Cyber look like in the Middle East?

These five highlights provide a glimpse into where Middle Eastern Organizations are now – and where they are going.

Modernization

52%

of Middle East respondents said that cybersecurity impacts the success of digital transformation to a large extent

Resilience

61%

of Middle East respondents said that the success of cybersecurity supports planning for business disruption to a large extent

Business-driven

55%

of Middle East respondents on average report positive business and organizational contributions as a result of implementing cybersecurity initiatives
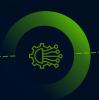
Funding

51%

of Middle East respondents cite lack of funding as the top challenge for managing cybersecurity when compared to 36% Globally

Talent

69%

of Middle East respondents said that offering training and certification programs is key in engaging, retaining, and developing cyber talent

Becoming Cyber-ready

How can organizations in the middle east prepare for an evolving cyber landscape? The following five insights and five corresponding actions, based on Deloitte's experience and our survey findings, can provide a starting point for navigating the future of cyber.

Insights to Inspire

1. Organizations are on a never-ending digital transformation journey. Modernizing and replacing legacy systems is a constant priority as organizations adapt to an increasingly digital world while also seeking new efficiencies and speed. Cloud initiatives, upgrades for operational /industrial control systems, and Internet of Things are among the top digital priorities of organizations within the middle-east.

2. Be fit for the future. Recognize the importance of planning for disruption and dealing with complex and severe events as a strategic priority. This requires a need for more proactive, forward-looking, and strategic approaches to resilience in order to be prepared for business disruption and to adapt and thrive in changing environments.

3. Cyber as a business enabler. Organizations are reaping the organizational benefits of cybersecurity including improved brand reputation, operational efficiency, digital trust, improved customer trust/brand impact, and improved confidence in tech integrity.

4. Funding will shape the future of cyber. Funding is the engine that supports cybersecurity transformation as organizations embark on with their digital transformation journeys. Budgets for cyber can be nebulous or ill-defined as it has been cited as one of the top challenges for managing cybersecurity. As a result, organizations may not be able to make the cyber investments they need to keep up with a changing threat landscape and organizational priorities.

5. The need to find and nurture cyber talent is becoming more critical. Finding talent is a massive and growing challenge for organizations within the middle-east. The lack of skilled cybersecurity professionals is making it harder to manage cybersecurity within organizations and employee retention and development is now more urgent.

Actions to Consider

Embed cyber consistently **across the board to protect the organization's most critical assets.** Cyber must not be an afterthought as you deploy new systems and upgrade old ones. Weave cyber tools and practices into your IT and business process landscapes. Make it foundational and ensure that your cyber capabilities can evolve in lockstep with your organization.

Future-proof organizations through building resilience and placing it at the core of the organization's strategy**. Cyber resilience risks must be understood to build robust and future-proof defense mechanisms to effectively prepare, respond, and recover from cyber disruptions. Conduct regular cybersecurity simulations and exercises targeting operations up to C-Suite to strengthen incident response and minimize business disruption.

Change the traditional perception of cybersecurity **being a cost center to a business enabler bringing value and supporting strategic objectives.** Demonstrate cybersecurity as a value center through setting the right tone at the top, embedding it into the organization's business strategy, and cascading that into detailed cybersecurity initiatives that enable the business through people, process, and technology.

Demonstrate the return on investment from cybersecurity initiatives. Showcase and justify to top management and decision makers the real value of cybersecurity through measuring the return on cybersecurity investments by employing top-down and bottom-up risk quantification tools, benchmarking, and conducting maturity assessments. A business-driven approach can help CISOs secure a more constant and dependable source of funding.

Address talent needs through an ecosystem approach. In the near term, outsourcing offers a pressure release valve for talent challenges. But what comes next? What constraints will you face 10 or 20 years from now? Nurture cyber talent and make your organization a more attractive place to work through a tailored talent and development program aimed at continuous learning including certification programs and training curriculums.

Deloitte.

This presentation has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved. Deloitte & Touche (M.E.) LLP (DME) or its affiliated entities would be pleased to advise readers on how to apply the principles set out in this presentation to their specific circumstances. DME accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this presentation.

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

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

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 130 countries and territories, serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 410,000 people make an impact that matters at www.deloitte.com.

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

DME provides audit and assurance, consulting, financial advisory, risk advisory and tax services through 29 offices in 15 countries with more than 5,900 partners, directors and staff.