Beat: Technology

Collaboration for cyber defense

Key to fortifying Iraq's digital future

Iraq, 08.02.2023, 16:53 Time

USPA NEWS - Digital transformation is a crucial pillar of Iraq Vision 2030, which aims to diversify the country's economic growth and accelerate job creation. More specifically, the agenda seeks to develop the ICT infrastructure, increase access to ICT technologies, increase internet connectivity speed, develop a national framework of digital storage and link this data effectively to the internet.
Much has been done already, with the country's carriers investing heavily in the foundational infrastructure for the country to leverage cutting-edge technology such as cloud computing, AI and Big Data. The government has prioritized collaboration with public and private organizations to achieve these goals.

One area that could be revolutionized by digital transformation is the country's critical energy sector. Big data analytics can pinpoint potential malfunctions in oil infrastructure before failure. Meanwhile, AI-driven seismic analysis makes identifying oil fields more effective and accurate, while producers can hit targets more efficiently thanks to data analysis. Research shows that digital technologies in the upstream sector could result in up to 20% savings. Working with the global tech leaders such as Huawei, Iraqi energy companies can build sustainable and intelligent energy infrastructure.

However, as the importance of digital technology continues to rise, so too do cyber risks as cybercriminals try to leverage the expanded threat surface. Therefore, stakeholders must ensure that Iraq's digital backbone is built with security from the ground up for long-term economic development. Failure to do so could severely impact digital transformation stall and socioeconomic progress. The latest PWC CEO Survey reveals that more than half (57%) of Middle East business leaders admit cyber risks will have a negative impact on their company this year, higher than the global average of 49%. As a result, 65% of Middle East business leaders believe cyber risks will limit their organization's ability to innovate, while 59% say these threats will undermine sales of products and services.
Collaboration is vital in tackling these cybersecurity challenges. Cyber defense is a shared obligation, and working within a broad ecosystem bringing together government, industry, universities, customers, and partners can advance cybersecurity and help position Iraq as a trusted, secure destination for investments and residency.

As a global technology and cybersecurity leader, we can help Iraq in this journey. Huawei believes cybersecurity is a shared responsibility that is best tackled through collaboration in an open and transparent platform with all cyberspace stakeholders to ensure end-to-end cybersecurity to support our vision of building a fully connected, intelligent world.
This collaborative stance is exemplified by our work with the Organisation of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT), demonstrating our vision of open collaboration to tackle security challenges. As a member of OIC-CERT, Huawei worked with other stakeholders to develop and deliver the OIC-CERT 5G Security Framework in OIC member countries to help safeguard their journey to 5G. This is especially important because OIC member states need their standards and guidelines to build regional multilateral norms, essential to ensure continuity, availability, resilience and cyberspace sovereignty for Islamic nation-states in this increasingly fragmented world.

Our cybersecurity assurance is also guaranteed through products that are hardened against even the most advanced threats. Our solutions are developed and delivered by observing security-by-design and privacy-by-design principles that empower our customers to safeguard their digital future. Huawei technologies have been deployed in more than 170 countries and regions, supporting the stable operations of over 1,500 carrier networks and serving more than three billion people over the past 30 years. This guarantee results from continuous long-term investment in cybersecurity management practices and technology for more than 20 years. We currently have more than 3,000 cybersecurity R&D personnel, with 5% of our R&D spend focused exclusively on boosting the security of our products.

That said, building a resilient digital infrastructure requires a skilled workforce. The PWC Report shows that a growing proportion of

Middle East business leaders have grasped that success in the digital age requires capable people as well as the latest technologies ? 46% of regional respondents plan double-digit investments in leadership and talent development over the next three years, compared with 30% last year.
The type of knowledge required to tackle modern cyber risks cannot be acquired exclusively in a classroom setting. Real-world experience is needed to expose graduates to the real threats facing Iraqi organizations. Technology companies have a crucial role in instilling ICT skills, including cybersecurity, through collaboration with universities and government agencies.

Huawei has a long and proud history of working with partners to advance ICT skills. The Huawei ICT Academy program, in particular, has made significant inroads in Iraq. In partnership with universities, the Academy aims to help train the brightest undergraduates in the latest technology and practical skills, with real-world work experience and even the chance of employment with Huawei. Students gain recognized Huawei certifications. There is a rich talent pool in Iraq, which needs support and nurturing – most recently, an Iraqi team, comprising students from Ninevah, Salahaddin and Anbar universities, achieved the second place in this year's Middle East Huawei ICT Competition regional finals that concluded in Oman.
The bottom line is that cybersecurity risk is significant, and we need to treat it with the seriousness it deserves. By working together, we can set shared goals and align responsibilities to build a trustworthy digital environment in Iraq that meets today's and tomorrow's challenges.

Article online:
https://www.uspa24.com/bericht-22253/collaboration-for-cyber-defense.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): William Yang

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. William Yang

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619