Securing tomorrow

Accelerated path to Artificial Intelligence integration for enhanced cognitive cybersecurity

Introduction

In today's digital landscape, the significance of a mature cybersecurity function is rapidly evolving due to growing threats, resource constraints, and technological advancements that introduce additional threat vectors. This makes it imperative for organisations globally and specially in the Middle East to take proactive security measures to protect their digital assets.

Findings of our latest 27th Annual CEO Survey have indicated that leaders in the region see cyber risks as a key threats, as organisations are exposed to new vulnerabilities in emerging digital economies. Setting an effective approach to cybersecurity and digital trust is, therefore, now more important than ever.

PwC's Middle East findings of the 2024 Global Digital Trust Insights survey has also revealed that the discussion around cybersecurity now needs to move from the IT and security teams to the boardroom where leaders need to make cybersecurity a priority and strengthen the culture of cyber preparedness.

The impact of cybersecurity functions extends beyond the scope of solely identifying, preventing, detecting, protecting, remediating and recovering from cyber attacks. They are essential in building trust in our daily ecosystem by ensuring the safety of human lives, securing health information, and facilitating safe financial transactions. As digital transformation accelerates in the Middle East, the region will increasingly require sophisticated cybersecurity measures that can ensure the safety and security of our lives in an effective and efficient manner.

Safeguarding children

Cybersecurity functions across multiple sectors help secure our children's data and shield them from growing cyber attacks that target children.
72% of children globally have been victims of cyber threats*

Protecting our health

Healthcare providers and other related entities poses critical information about the wellbeing of millions of individual across the globe. Cybersecurity functions are on full duty to help maintain such data away from bad actors.

Safeguarding our financials

In today's world, Fintech is helping us transform how we do finance but on the same time exposes us to new cybersecurity risks. Behind every transaction, cybersecurity function need to be alert to countless fraudulent activities.

Due to the above mentioned challenges and the increasing impact of cyber attacks, multiple cybersecurity functions in the Middle East are struggling to keep pace with such momentum, leaving them and their organisations prone to cybersecurity breaches every day.

This whitepaper aims to delve into these challenges and explore possible solutions, considering the recent advancement in cognitive technology. By leveraging such technologies organisations can enhance their cybersecurity capabilities, automate tasks, and improve their cyber defences specially in detection and response.

Source:The Global Cybersecurity Forum (GCF)

The challenge for cybersecurity teams to handle emerging threats

Finding and maintaining resources

Cybersecurity is a relatively new domain that hasn't been around for as long as other traditional fields, such as medicine or engineering. Hence, it hasn't had the same level of resources and support that other fields have benefited from over the years. Despite this, significant technological advancements in recent decades have created a high demand for cybersecurity professionals. Given the scarcity of highly skilled cybersecurity resources available, it has made it difficult for leadership within organisations to find and maintain such resources and ensure they upskill their game to match the increasingly advanced techniques and tactics of adversaries. Use of emerging technologies, such as Artificial Intelligence (AI) and Quantum Computing further emphasise the need for cybersecurity professionals to consistently upgrade their abilities to stay abreast with the latest threats.

Time to detect and respond to incidents

Time is another critical factor in cybersecurity. It can significantly affect the outcome of efforts to mitigate cybersecurity threats before, during, and after an attack. For instance, the failure to patch a vulnerability early on, delay in detecting an attack, or slow recovery after a cyber attack can cost organisations a significant amount of money, damage their reputation, and erode customers' trust.

Expanding IT and digital infrastructure

Assuming that cybersecurity functions are able to find and retain the right resources, while having the right procedures in place to swiftly respond to cyber attack, they need to be able to cope with technological advancement. The expansive nature and intricacy of digital landscapes adds more responsibilities on the cybersecurity functions. Almost all organisations now have a website, many have their own mobile applications, few have already established their presence on the metaverse and some are even developing their AI models. While such advancements help organisations improve the lives of their customers, they also attract the attention of malicious actors. It is important to ensure that all technological advancements are vetted by the cybersecurity function. An ineffective and inefficient cybersecurity function can become a bottleneck for organisations ambitions to progress.

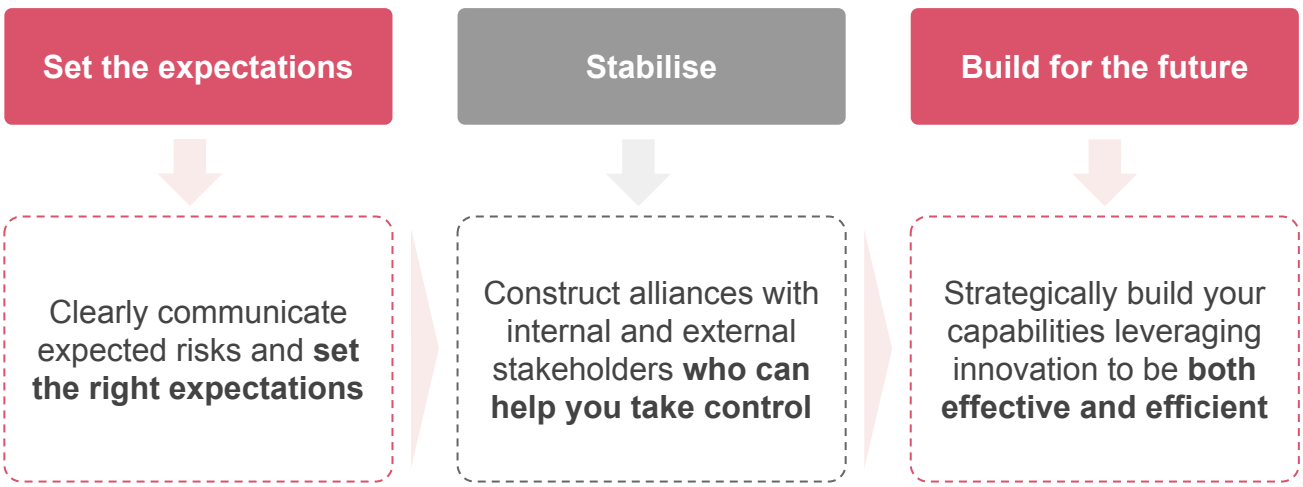
All these changes will not only impose high demand on the cybersecurity function but will also require other organisational departments to expect clearly communicated Service Level Agreements (SLAs) that are achievable by the cybersecurity function.

How can cybersecurity functions take control?

To effectively address cybersecurity challenges, organisations must first ensure their leadership understands and sets the right expectations. It is critical to communicate clearly that these challenges are global and are not unique to their organisation. Cybersecurity functions need to quickly understand and prioritise areas of significant value, taking into account the intersection between the organisation's top valued assets and its weakest cybersecurity controls, whether technical or administrative. Such prioritisation should be clearly communicated to organisation's leadership to collaboratively determine an acceptable level of risk tolerance.

Considering the challenges around resource, time and technology extensiveness, cybersecurity functions should establish strong alliances and partnerships. This will help to prioritise the development of basic capabilities, while strategically improving its overall cybersecurity posture. The establishment of such capabilities should be done in collaboration with the organisation's existing resources. This approach ensures that internal teams can quickly absorb the necessary expertise from partners and alliances.

As organisations implement basic cybersecurity capabilities, the involvement of their cybersecurity resources should gradually increase. Involvement in the establishment phase positions them excellently to maintain and improving on their capabilities by learning how to tackle daily challenges. Meanwhile, cybersecurity functions should continue filling the gaps by adding more qualified cybersecurity resources to the team, in alignment with organisational growing demand for cybersecurity services and capabilities. This approach will allow for a smooth transition towards a robust and permanent cybersecurity capability that brings the best of both worlds: external expertise and perspectives blending into internal understanding of organisational needs and context.



What role can AI play in helping the cybersecurity function take control ?

AI played great role over the recent past years in the cybersecurity arena, with multiple technologies leveraging its capabilities to help organizations detect malwares faster, analyzing users behaviours, detecting cyber fraud, in addition to other use cases. However, with GenAI now in the scene, other cybersecurity function can be further improved. In this section we will look at some examples focusing on cybersecurity GRC, SOC and IT asset monitoring.

- The introduction of cognitive technology has the potential to dramatically improve the Cybersecurity Governance, Risk, and Compliance (GRC) activities. An example would be to automate the review and update of key cybersecurity artefacts such as policies, procedures, and architecture designs. This does not only enhance efficiency but has the potential to enable organisations to maintain regulatory compliance seamlessly with fewer resources.
- Another key aspect of cognitive cybersecurity lies in transforming the Security Operations Center (SOC). The SOC team, armed with advanced cognitive capabilities, would be capable of identifying and responding to cybersecurity threats more efficiently. By combining the expertise of human analysts with AI technologies, decision-making can be accelerated, which is crucial in a landscape where timely and effective threat mitigation is paramount. This dynamic integration can break the time constraints that organisations often struggle with, ensuring swift responses to emerging threats. Real-life examples of this can be observed through the implementation of new GenAI tools for security, where AI technology supports SOC teams in their cybersecurity operations.
- The use of AI in the continuous review of cybersecurity, can provide great advantages in monitoring and maintaining continuous visibility into the IT landscape. AI can be leveraged to analyse users' behavioural patterns and anomalies optimising the detection of malicious activities in a timely manner. This enables review teams to focus on proactively monitoring and identifying the possibility of new vulnerabilities being introduced when scaling IT and digital infrastructure. A proactive stance, coupled with an intelligent approach, can help cybersecurity functions to be better prepared against the increasingly sophisticated AI-powered attacks.

What role can AI play in helping the cybersecurity function take control ?

As AI and cognitive technology continues to be applied in more cybersecurity scenarios. Chief Information Security Officers (CISOs) have a unique opportunity to prepare and build the right AI capabilities to efficiently manage the growing demand for cybersecurity services within the organisation. CISOs can also implement a chargeback model to enable business functions to leverage the services and service packaging provided by the cybersecurity function. This approach optimises the utilisation of limited cybersecurity resources, addressing the persistent scarcity of qualified professionals proficient in countering evolving threats.

Below is an illustrative example of a next generation cybersecurity service delivery model utilizing strategic partners and alliances for building capabilities rapidly. It clarifies the interaction with different stakeholders through security by design and continuous monitoring concepts:

What to consider when building your AI model for cybersecurity?

Define the objective

Crafting a resilient cognitive cybersecurity model requires a systematic and meticulous approach to meeting several critical requirements. At the beginning, organisations must articulate the model's objectives, establishing overarching goals that guide its implementation. This sets the stage for aligning the cognitive model with specific cybersecurity needs and strategic priorities of the organisation. Precision in key in presenting key data, as this enhances the ability to detect threats and provides the bedrock for leveraging AI capabilities.

Analyse cybersecurity demand

In alignment with the defined objectives, cybersecurity team must align the model to where it can help the most by analysing the demand for cybersecurity services from internal and external stakeholders and understanding where the model can be most helpful. This step is crucial to selecting and building the right AI model.

Select and build the right AI model

Selecting an optimal AI model is pivotal, necessitating the consideration of cybersecurity goals and the evolving threat landscape. Different AI models provide different capabilities, that can be more effective in some scenarios than others. When selecting an AI model for cybersecurity, there are key elements to consider, for example model speed, accuracy, reliability, reasoning capability, scalability, etc.

Feed the model with the right data

Building the right data foundation for the AI model can make or break the entire model. Leveraging the huge amount of internal data collected through the years will help build a model that is more aligned to the organization context and values, while selecting the relevant external data sources will be key to provide the right external context. An intuitive model interface and user experience are also essential, enabling cybersecurity professionals to interact seamlessly with insights, thereby enhancing team efficiency and effectiveness.

Monitor and improve

Building an AI model for cybersecurity is a journey that would go through ups and downs, hence, continuous monitoring and fine-tuning of the AI model performance is important to progress toward the right direction. Cybersecurity leaders can also leverage the expertise of experienced entities to help them throughout the journey, this can be in the form of a managed service agreement that minimizes the tactical and operational efforts to keep them focused on results.

Pioneering a new era with integrated cognitive cybersecurity

As highlighted in PwC Middle East's GenAI Spotlight, although GenAI and other emerging technologies might lead to sophisticated cybersecurity attacks, survey respondents expressed confidence in GenAI's potential to strengthen cybersecurity measures. Large Language Models (LLMs) can be powerful tools in detecting cyber threats and simplifying complex data and security engineering processes. A significant 83% of Middle East respondents (including 92% in the UAE and 87% in the KSA) said their organisation would deploy GenAI tools for cyber defence within the next 12 months, compared to 69% globally. In risk awareness, 34% of regional respondents (33% in KSA and 45% in the UAE), almost the same number as global, reported that their organisation recognised the cyber risks associated with GenAI, and included them in their risk management plan, continually updating it. Additionally, around 28% said their organisations monitored GenAI risks, aligning closely with the global average. So although it could take some time before we see broad-scale use of GenAI in cyber defence, the three most promising areas, for now, include threat detection and analysis, cyber risk and incident reporting and adaptive controls.

In navigating the complex cybersecurity landscape, marked by rapid technological advancements and a scarcity of skilled professionals, organisations are urged to prioritise establishing foundational security measures rapidly through strategic partnerships and alliances. This critical first step will not only ensure a robust baseline defence, setting the stage for the seamless integration of advanced technologies like AI and cognitive tools, it will also enable the organisations' cybersecurity team to explore more innovation. Such partnerships not only bolster immediate security needs but also equip organisations with the flexibility to evolve, embracing AI-enhanced capabilities on a secure and optimised platform. This approach enables a strategic, phased advancement in cybersecurity posture, preparing organisations to meet future threats head-on with a blend of foundational strength and innovative technology.

Illustrative Service Operating Model

Authors

Salam Shouman

Partner
Cybersecurity,
PwC Middle East

Walid El Sayed

Partner
Egypt Consulting Leader,
PwC Middle East

Mohammed Saty

Senior Manager
Technology Consulting,
PwC Middle East

Eyad Haddad

Senior Manager
Cybersecurity and
Digital Trust,
PwC Middle East

Sanad Al-Alam

Manager,
Data Privacy and
Cybersecurity,
PwC Middle East

Thank you

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for over 40 years, PwC Middle East has 30 offices across 12 countries in the region with around 10,000 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.