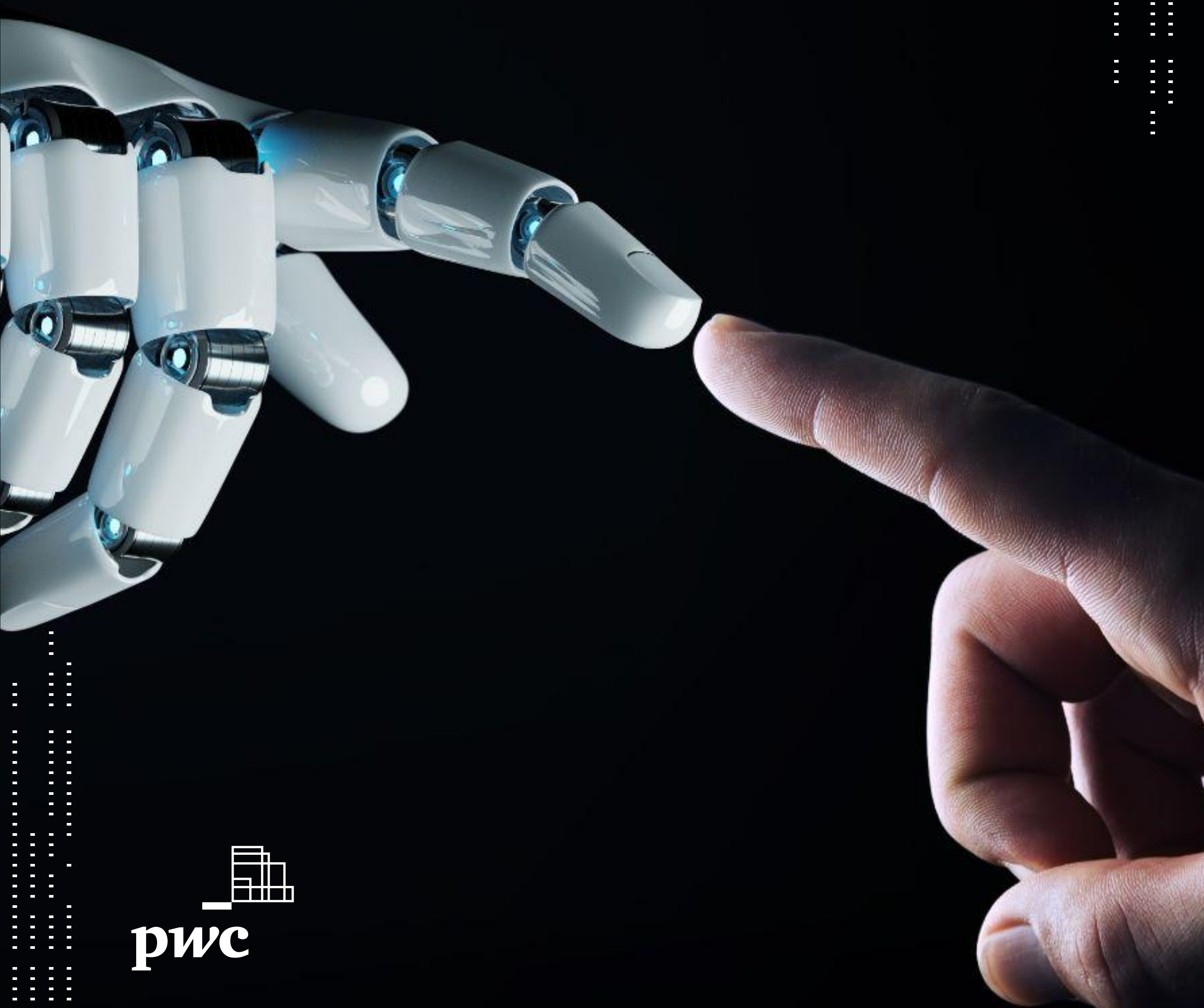
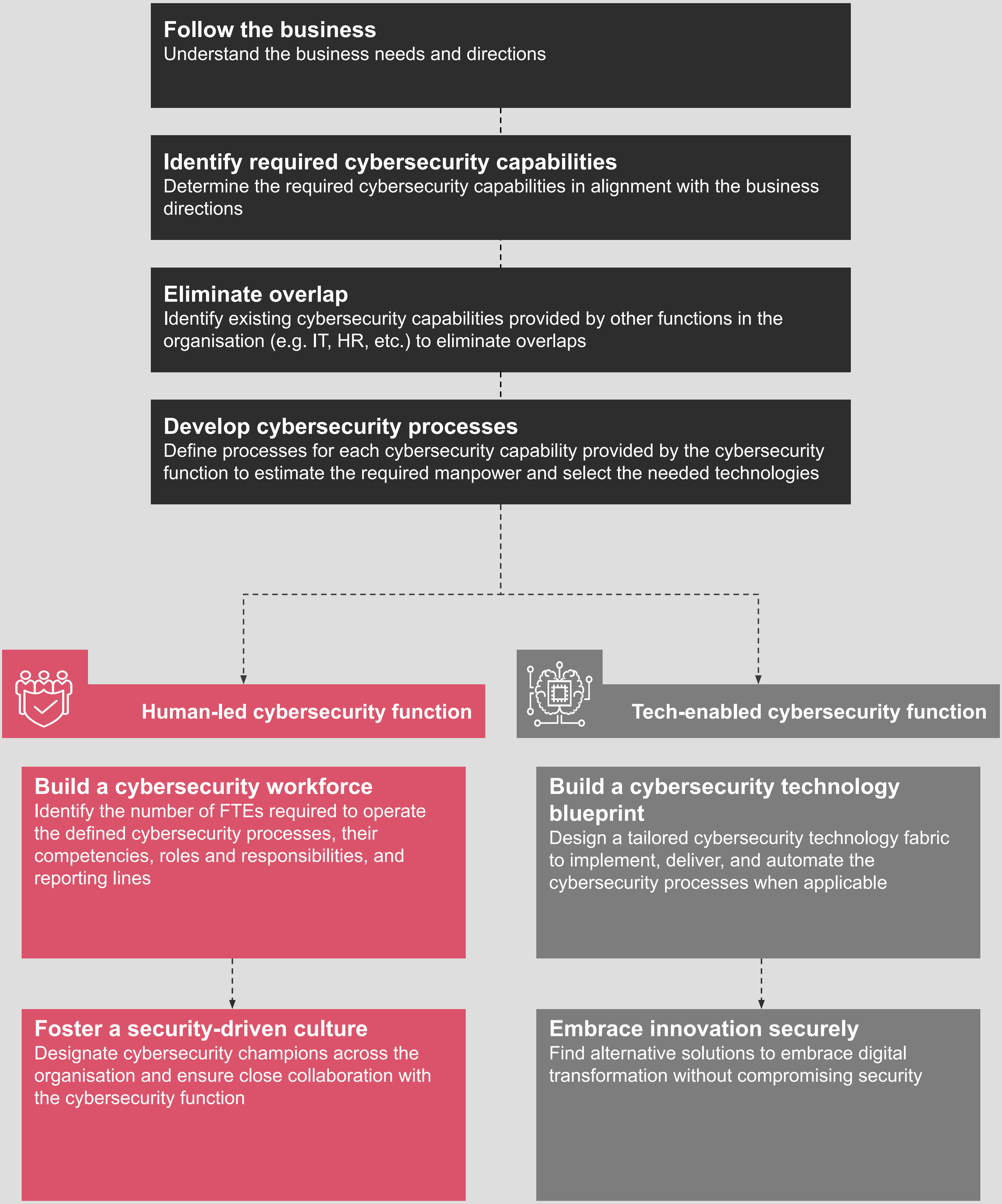
A human-led and tech-enabled cybersecurity function

Building a comprehensive cybersecurity ecosystem



Cybersecurity function 101



Follow the business

Understand the business needs and directions

Identify required cybersecurity capabilities

Determine the required cybersecurity capabilities in alignment with the business directions

Eliminate overlap

Identify existing cybersecurity capabilities provided by other functions in the organisation (e.g. IT, HR, etc.) to eliminate overlaps

Develop cybersecurity processes

Define processes for each cybersecurity capability provided by the cybersecurity function to estimate the required manpower and select the needed technologies

Human-led cybersecurity function

Build a cybersecurity workforce

Identify the number of FTEs required to operate the defined cybersecurity processes, their competencies, roles and responsibilities, and reporting lines

Foster a security-driven culture

Designate cybersecurity champions across the organisation and ensure close collaboration with the cybersecurity function

Tech-enabled cybersecurity function

Build a cybersecurity technology blueprint

Design a tailored cybersecurity technology fabric to implement, deliver, and automate the cybersecurity processes when applicable

Embrace innovation securely

Find alternative solutions to embrace digital transformation without compromising security

Executive summary

In today's rapidly evolving digital landscape, it has become imperative for organisations to establish a mature cybersecurity function to tackle the evolving cyber threat landscape. Cyber attacks can have a significant impact on businesses, particularly as our world becomes more interconnected. Findings from our 27th Annual CEO Survey indicate that cyber risks are a concern for business leaders in the Kingdom of Saudi Arabia, with 40% revealing they were moderately exposed and 20% highly exposed to it in the next 12 months.

During our cybersecurity engagements in the Middle East, we have observed common challenges that organisations face while establishing a cybersecurity function. The key pain points include maintaining compliance with national cybersecurity regulatory requirements, avoiding overlapping roles and responsibilities with other functions such as IT and data management, and identifying the right cybersecurity technologies.

This thought leadership seeks to guide organisations through the process of establishing a robust cybersecurity function that enables the business and protect its crown jewels. It will focus on the prerequisites to building a cybersecurity workforce and selecting the required cybersecurity technologies to establish a human-led and tech-enabled cybersecurity function.

01 Cybersecurity function 101

1.1 Follow the business

The cybersecurity objective for any organisation is to safeguard its critical digital assets. Achieving this requires understanding the organisation’s business needs and directions and translating them into cybersecurity objectives. It's critical to maintain an optimal level of security, striking a balance between protecting vital business assets, without hindering day-to-day operations. Interviews with top management will provide visibility on the organisation's business directions and help identify the cybersecurity objectives and principles the organisations would adhere to for consistent cybersecurity capability design.

In the realm of compliance by design principle, consideration of applicable cybersecurity regulations on the organisation is vital. In case of conflicting requirements between the business and regulations, the Chief Information Security Officer (CISO) should then evaluate the impact of this cultural disconnect between cybersecurity controls and business needs and report it to the top management to drive risk-aware decision making.

1.2 Identify cybersecurity capabilities

Apart from the conventional cybersecurity capabilities, the CISO should identify the required cybersecurity capabilities in alignment with the organisation’s business directions. Different business directions can significantly influence the need for specific cybersecurity capabilities to achieve expected outcomes. Adhering to certain cybersecurity principles will ensure consistent outcomes across the organisation and help mitigate applicable cybersecurity risks. For example, many organisations today plan to host most, or all of their data, on the cloud, emphasising the need for a robust cloud security capability.

Other organisations who outsource software development might require a third-party cybersecurity assurance capability, as opposed to securing it inhouse. Moreover, those that have subsidiaries, might adopt and offer centralised capabilities, including, but not limited to, cybersecurity governance, security monitoring, incident response, and cybersecurity awareness.

1.3 Eliminate overlap

The CISO should evaluate the current state of the cybersecurity capabilities at the organisation and determine whether they should be owned by a dedicated cybersecurity function, IT function, or other functions within the organisation.

If certain cybersecurity capabilities owned by other functions are mature, and do not cause conflict of interest, the cybersecurity function can then establish channels for collaboration and alignment without necessarily transferring ownership. This would minimise overlapping capabilities with other functions and avoid reinventing the wheel.

There are cybersecurity capabilities commonly owned by a dedicated cybersecurity function. For example, cybersecurity governance, risk and compliance (GRC) capability is separate from IT in most organisations as this is crucial to ensure that cybersecurity audit reviews remain independent from the teams implementing the cybersecurity requirements.

1.4 Develop cybersecurity processes

Before delving into conversations around the workforce and necessary technologies for building cybersecurity capabilities, it is crucial to establish well-defined cybersecurity processes for each cybersecurity capability. The capability represents the outcome expected from the cybersecurity function, whereas the process combines the steps, tasks, or activities needed to reach this outcome, their sequential order, the responsible party to complete them, and the expected time to accomplish them.

A well-defined process will provide accurate information for estimating the required manpower and competencies in the cybersecurity function, as well as the needed cybersecurity technologies to implement, deliver, and automate the process when applicable. Some activities within the cybersecurity process may involve human review and approval, require specific skills and knowledge, and leverage certain resources such as equipment, technologies, or documents. In contrast, other activities may simply require automation with no human intervention.

In some organisations, the hiring of cybersecurity professionals and the acquisition of cybersecurity technologies are often done before defining the processes, which can negatively impact productivity and efficiency.

2.1 Build a cybersecurity workforce

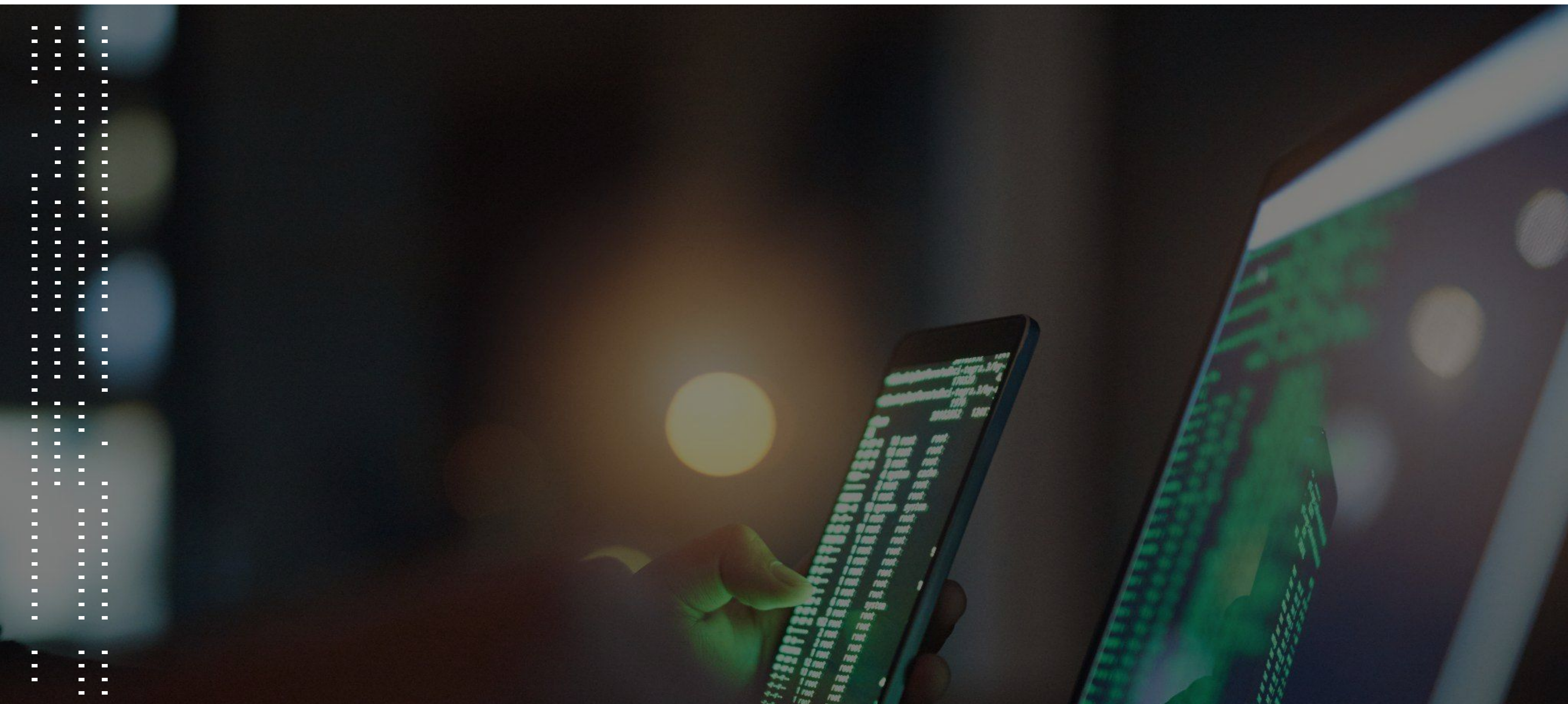
A clear scope of required skills and expertise is critical for building a cybersecurity workforce. The first step is defining the roles and responsibilities for each activity within the cybersecurity process. Factoring in the overall time required to complete the process, the CISO can determine the required number of full-time employees (FTEs).

When organisations plan to establish a new cybersecurity function, it is crucial to prioritise the selection of in-house capabilities and processes based on the nature of their business and the allocated budget. This should be done in comparison with the capabilities and processes that are best suited for outsourcing. For instance, Security Operations Centre (SOC) capabilities, which demand 24/7 operations and resources, are commonly outsourced. This approach provides organisations an immediate access to a pool of talented, certified, and round-the-clock cyber professionals. For organisations with an existing cybersecurity function, it is important to prioritise training and upskilling of current employees and address any gaps in their proficiencies by hiring or outsourcing when needed.

There are published recommendations for structuring a cybersecurity organisational chart in compliance with cybersecurity regulations in the Middle East. For example, in Saudi Arabia, the National Cybersecurity Authority recommends organisations establish a direct reporting line from the head of cybersecurity to the leadership. This underscores the importance of leadership overseeing the organisation's cybersecurity stance.

2.2 Foster a security-driven culture

To enhance cybersecurity within an organisation, it is recommended to assign cybersecurity champions across business functions. This will increase awareness of cybersecurity, promote a security-focused culture, and encourage close collaboration with the business. There are common overlaps in cybersecurity roles and responsibilities across different functions in the organisation such as IT and HR. These functions need to work closely with the cybersecurity function through well-defined working groups and unified cybersecurity objectives and metrics.



3.1 Build a cybersecurity technology blueprint

With the CISO's aim to translate business, technology, and cybersecurity regulatory requirements into best-fit, sustainable, and future-proof cybersecurity processes, it becomes critical to design a cybersecurity technology fabric that supports the implementation and delivery of each activity defined within these processes. Some activities can be further broken down into technology features and components. Factoring in the cybersecurity principles the organisations adhere to, the CISO can determine the cybersecurity technologies needed to complete the activities within a cybersecurity process and evaluate vendors respectively. For example, leveraging the Accountability and Traceability principle, the organisation would need to consider recording and monitoring the digital user footprint and authenticating data provenance, which would influence the choice of the cybersecurity technology fabric as per the below:

Tool	Activity
Security Information and Event Management (SIEM) tool	**A centralised security log collection activity**
Threat intelligence platform (TIP)	**A threat intel aggregation activity**
Endpoint Detection and Response (EDR) tool	**A continuous end-user devices monitoring activity**
Network detection and response (NDR) tool	**An advanced network traffic monitoring activity**
Database activity monitoring (DAM) tool	**An active database monitoring and analysis activity**

This approach provides full justification for each and every component of the cybersecurity technology fabric – it is always based on business, digital transformation, or compliance requirements. This way cybersecurity is no longer treated as an afterthought, cybersecurity budgets are no longer questioned with value and impact concerns, and CISOs are no longer focused on one-off, siloed cybersecurity technologies that resolve specific problems when they arise.

Today, cybersecurity technologies play an increasingly vital role as a powerful enabler for continuous process improvement. Some activities within a cybersecurity process may require human intervention while others are automated. The user access management process, for example, can have legacy and manual activities to grant and revoke access rights based on business needs, or modernised activities with automated provisioning and seamless workflows with the use of technology to streamline the process of giving users access to resources based on their role and permission levels within their organisation.

3.2 Embrace innovation securely

With technology becoming more integral to businesses, innovation across various industries is driven by generative AI, predictive AI, and other macro-technology trends. Echoing sentiments of our 2024 Global Digital Trust Survey "Innovation means making bold moves, and there's nothing more empowering than ensuring safety", modern cybersecurity technologies are now a necessity to safeguard and protect organisations. In our **27th Annual CEO Survey,** more than half of the leaders surveyed in the region indicated that GenAI is likely to increase cybersecurity risk in the next 12 months. Much like traditional software, the macro-technology trends adopted by the organisation must be secured, and the first step towards a secure implementation is not about adding one-off point solutions as this might increase complexity and lead to even higher cyber risk exposure. Instead, the first step is to reevaluate the cybersecurity technology fabric to integrate unconventional cybersecurity components to secure growth and innovation built on Zero Trust principles, powered by AI, and continuously aligned with changing business requirements.

In our report, **Fighting Cybercrime in the Age of Quantum Computing** we have explained that quantum computing can compromise the foundations of cybersecurity, primarily through its impact on encryption and public key infrastructure (PKI) encryption in particular. Organisations should take proactive measures to mitigate these threats as they threaten the integrity of digital documents and the confidentiality of sensitive data like government intelligence, digital payments, blockchain transactions, health records, and national infrastructure. Proactive cybersecurity planning for new technology ventures might influence the CISO’s decision to outsource the technical delivery of some cybersecurity capabilities to Managed Security Service Providers (MSSPs) or transfer some of the cybersecurity risks associated with potential future breaches to cybersecurity insurance companies.

However, growth and innovation are not the only factors that drive organisations to choose alternative solutions to acquire cybersecurity technologies in-house, such as outsourcing to Managed Security Service Providers (MSSPs). The persistent security skills shortages, budget constraints, limited cybersecurity posture and readiness levels and the organisation’s overall culture undermining cybersecurity activities, might also affect the CISO’s decision. An outsourced SOC, for example, overcomes the biggest challenge of assembling a skilled team, while granting the organisation immediate access to shared threat intelligence, optimised and integrated services, streamlined scalability, reduced implementation costs, and lower ongoing operational and management costs.

Conclusion

As organisations reinvent themselves and develop new lines of business using macro-technology trends, it has never been easier to erode trust. The result of the ever-evolving and sophisticated threat landscape implicates brand reputation, operations availability, financial stability, individuals health and safety, and compliance status. To prevent this, cybersecurity should be at the forefront of innovation while balancing asset protection and business enablement. The cybersecurity function of an organisation should identify the required cybersecurity capabilities that align with the overall business vision, digital transformation ventures, and regulatory requirements.

It's important to leverage existing functions within the organisation to eliminate overlaps and duplicate efforts. For each cybersecurity capability, well-defined cybersecurity processes should be developed to accurately estimate the required manpower and establish a clear scope for the cybersecurity workforce. Additionally, these processes influence the design of a tailored cybersecurity technology fabric that supports the implementation, delivery, and automation of these processes when applicable.

The immediate goal of every cybersecurity function is to provide cybersecurity capabilities effectively and efficiently. It involves operating and continuously improving processes in response to changes, nurturing cybersecurity skills, fostering a security-driven culture, and unleashing the power of cybersecurity technologies while harnessing their potential. The long-term goal, however, is to proactively secure the organisation's lofty ambitions and protect its crown jewels from threats by following a "tomorrow today" approach.

Contacts

Haitham Al-Jowhari
Partner, Cybersecurity
haitham.al-jowhari@pwc.com

Samer Omar
Cybersecurity & Digital Trust Leader
samer.omar@pwc.com

Mohammed Ayesh
Director, Cybersecurity
mohammed.ayesh@pwc.com

Ali Mouslmani
Senior Manager, Cybersecurity
ali.mouslmani@pwc.com

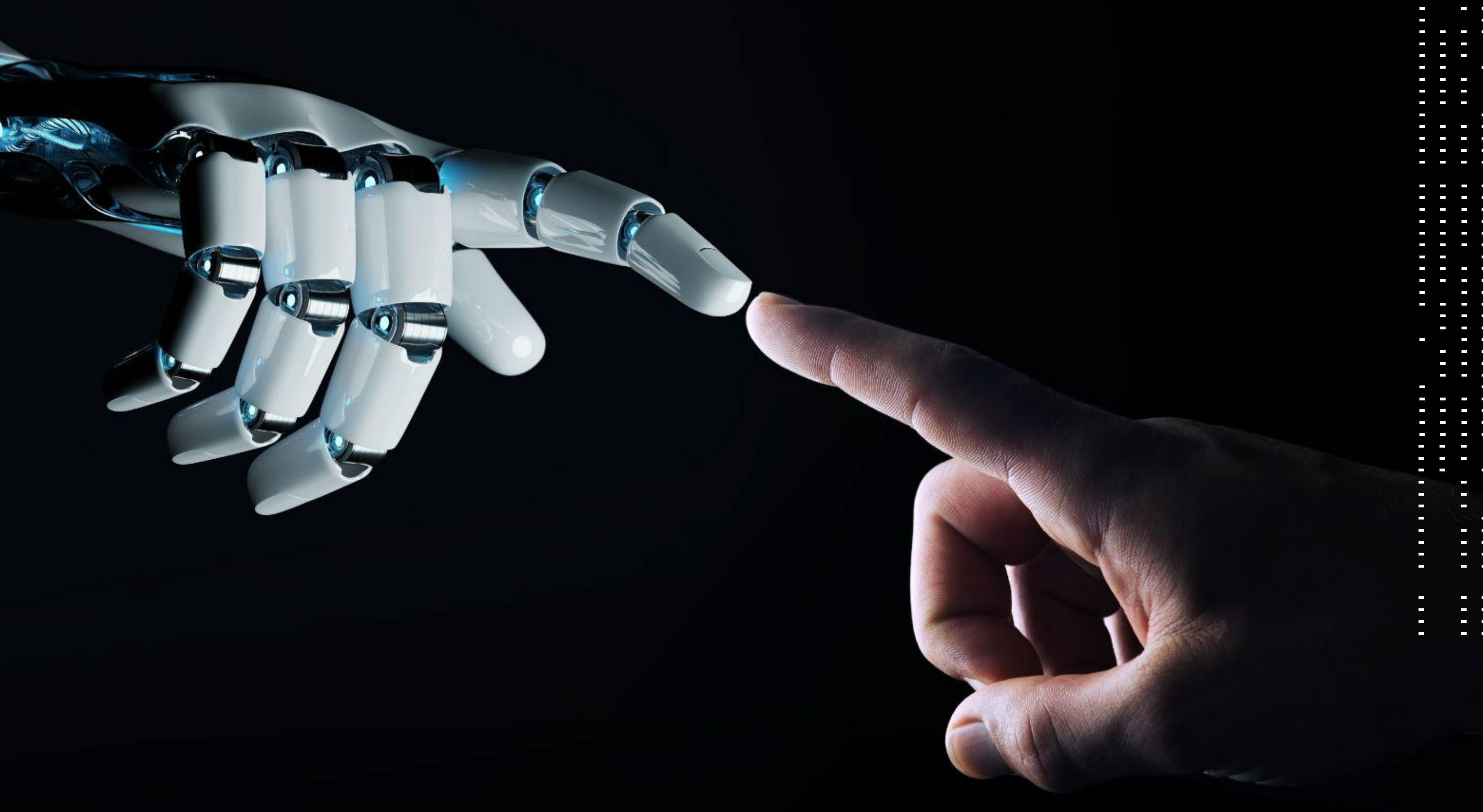
Abdulrahman Kurdi
Senior Manager, Cybersecurity
abdulrahman.kurdi@pwc.com

Sylvia Elferkh
Manager, Cybersecurity
sylvia.elferkh@pwc.com

Kholoud Alqahtani
Manager, Cybersecurity
kholoud.alqahtani@pwc.com

Abdullah Albahdal
Partner, Cybersecurity
abdullah.albahdal@pwc.com

Thank you



About PwC

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries. As a community of solvers, with 8,000 people across the region, we bring the right combination of people, technology and expert capabilities from Strategy, through Advisory and Consulting to Tax and Assurance Services, to solve the region's most pressing challenges (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.