pwc

When offence becomes the best defence

How to gain the cyber advantage

01 A strategic necessity

Cyber threats are evolving faster than most organisations and businesses can respond. The frequency, sophistication and scale of cyberattacks are projected to surge over the next decade – posing an especially acute challenge for the Middle East, a region undergoing rapid digital transformation against a backdrop of complex geopolitical dynamics. Its vulnerability to cyber threats is amplified by a unique convergence of factors: The region is home to critical oil and gas assets, financial hubs, and government systems; its accelerated economic growth and technological advancement here often outpace regulatory and security frameworks; escalating geopolitical tensions make cyber warfare into a key tool of destabilisation. In 2024, 25% of all cyberattacks in the region targeted government institutions, underscoring how state infrastructure has become a frontline in the evolving threat landscape.[1] As the Middle East accelerates its digital ambitions, building collective cyber resilience will be essential - to safeguard national security, ensure economic continuity, and maintain public trust.

Traditional defences are no longer enough. Attackers now use agile, adaptive tactics that bypass conventional security and exploit hidden vulnerabilities. The result? Financial loss, operational disruption and reputational damage.

> “The solution?
> Think like the attacker.”

Why offensive cybersecurity is now a business imperative

Offensive cybersecurity (OffSec) gives organisations a strategic edge. By simulating real-world attacks, it helps identify and mitigate vulnerabilities before adversaries can exploit them. Techniques such as penetration testing, red teaming and attack simulations mirror the tools and behaviours of threat actors - transforming risk into actionable insight.

This shift from reactive to proactive security is not just a tactical upgrade, it's a necessity. OffSec empowers organisations to continuously assess, test and improve their defences. These exercises not only uncover technical gaps, they also reveal weaknesses in processes, protocols and human behaviour - areas that attackers often target.

Offensive tactics strengthen overall resilience by challenging assumptions and highlighting blind spots. They expose gaps in employee awareness, incident response and system readiness. By addressing both technical and human vulnerabilities, organisations can build a more adaptive and comprehensive defence strategy.

Chief information security officers (CISOs), chief technology officers (CTOs) and other decision-makers need more than perimeter defence - they need foresight, flexibility and confidence. Offensive cybersecurity delivers that by integrating technology, strategy and service into a foundation for long-term resilience.

This shift from reactive to proactive security is not just a tactical upgrade, **it's a necessity.**

Cyber threats are not slowing down. In Saudi Arabia alone, there were over 110m cyberattacks in the last few years across a range of industries, including healthcare, finance and oil, underscoring the critical need for more proactive security measures.[2]

Threat actors are using increasingly sophisticated methods to exploit vulnerabilities faster. **The average time-to-exploit (TTE) for a vulnerability has decreased from 32 days in 2021-2022 to just five days in 2023.[3] Attackers are skilled at bypassing established security protocols, mimicking legitimate online activities or behaviours.** This ability to blend in with normal traffic makes it harder for traditional security systems to detect their malicious actions.

With the average cost of a breach at US$4.45 million globally - and US$7.2m for larger organisations[4] - the stakes are too high to rely on reactive defences alone. With attack methods evolving and becoming harder to detect, organisations cannot afford to rely solely on traditional, reactive security strategies. A shift to offensive cybersecurity is now not only a strategy to stay ahead but a necessity to mitigate significant operational and financial risks.

These limitations underscore the urgent need for a shift towards proactive cybersecurity strategies. Designing a strategic offensive cybersecurity programme involves shifting from a reactive to a proactive approach, enabling organisations to anticipate and mitigate threats before they manifest.

02 How does it benefit an organisation

Offensive cybersecurity proves crucial when aligned with business goals. By proactively identifying vulnerabilities and simulating real-world attacks, organisations can not only protect their assets and ensure operational stability but also build trust and enhance their competitive edge.

Importantly, offensive cybersecurity strategies often intersect with regulatory frameworks. While compliance requirements can drive the adoption of such approaches, a well-aligned offensive programme does more than just meeting standards - it actively shapes resilient compliance practices. This alignment ensures organisations remain resilient while adhering to evolving regulations, creating a synergy between proactive defence and legal mandates.

A strategic offensive cybersecurity programme incorporates several key methodologies that enhance an organisation's security posture while aligning with business goals and compliance needs.

First, establishing a dedicated threat-hunting team is essential for identifying anomalies through advanced detection tools such as security information and event management (SIEM) systems. Red teaming and regular penetration testing simulate real-world attacks, helping organisations to uncover and remediate vulnerabilities.

For example, a healthcare provider improved its security posture and Health Insurance Portability and Accountability Act (HIPAA) compliance by addressing critical vulnerabilities. This involved a systematic program to identify, assess, and remediate security weaknesses across their patient data systems, leading to a demonstrable reduction in breach risk and successful audit outcomes. Continuous vulnerability management programmes help prioritise and automate assessments.

Incident response drills refine response strategies, minimising reputational damage during actual incidents. Along with drills, employee training programmes that simulate phishing attacks have proven effective in reducing vulnerability to social engineering threats. A recent study highlighted that human error was a significant contributing factor in 74% of all cybersecurity breaches.[5]

Finally, collaborating with regulatory bodies ensures that offensive cybersecurity strategies meet evolving compliance standards.

01 Improving continuity, resources and financial protection

Aligning offensive plans with primary goals helps organisations thrive. Offensive methods, such as threat hunting and adversarial simulation, detect flaws early, blocking major risks before they materialise. These measures save money while reducing reactive costs from cyber damage.

The financial costs of breaches emphasise the value of being proactive. According to PwC 2025 Digital Trust Insights, 15% of organisations in the Middle East region have suffered data breaches costing more than US$100,000. Offensive strategies significantly reduce risks, strengthening systems and saving millions.

With well-balanced budgets, organisations allocate resources effectively. Industry guidelines generally suggest spending 30% on protection, 30% on detection, and 30% on response efforts. Offensive actions optimise investments by targeting the highest risks, ensuring better results.

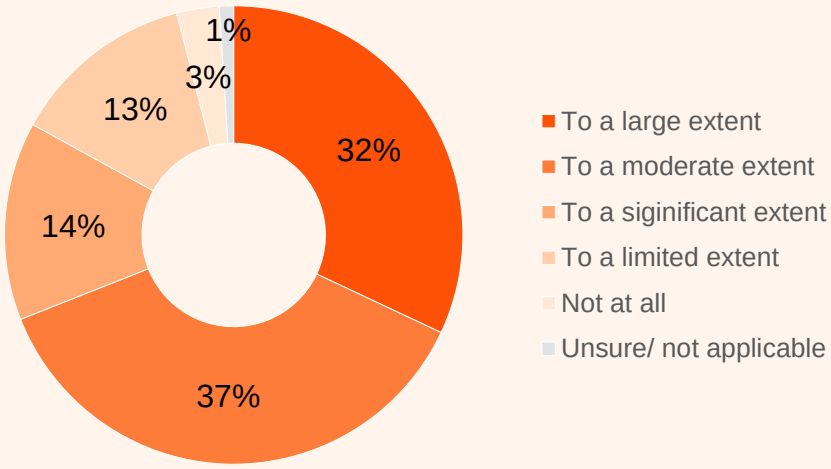
02 Driving support through compliance and building resilience

Achieving executive trust starts with showing clear connections between security steps and business resilience. Standards, like the US National Institute of Standards and Technology (NIST)[6] back proactive approaches, such as security assessment and intelligence gathering. These efforts help compliance while mitigating key risks, aligning with business needs.

Source: PwC 2025 Global Digital Trust Insights

Offensive cybersecurity also builds resilience. Techniques like ethical hacking and adversary emulation simulate realistic attacks, revealing potential flaws. Such exercises accelerate system improvements, ensuring the organisation reacts effectively to evolving threats.

Question: To what extent, if at all. Have cybersecurity regulations increased your organisation's cybersecurity investment over the last 12 months?



Source: PwC 2025 Global Digital Trust Insights

Furthermore, compliance remains a major factor in increasing cybersecurity investments. Nearly 96% of firms report higher budgets due to regulatory demands according to the PwC 2025 Global Digital Trust Insights study. By aligning efforts with these demands, businesses meet standards while building industry trust.

03 Earning trust and standing out in competitive markets

Linking cybersecurity plans with core goals not only secures assets; it also fosters confidence. Customers, partners, and investors value strong commitments to safeguarding data. According to PwC 2025 Digital Trust Insights, 57% of businesses invest primarily to protect customer trust, while 49% focus on loyalty and brand safety.

Question: Which one statement, if any, best reflects the impact of new cybersecurity regulations on your organisation over the last 12 months?

Cybersecurity regulations helped 78% of organisations

24% challenged our organisation to strengthen the current cyber risk management program, processes and governance approaches.

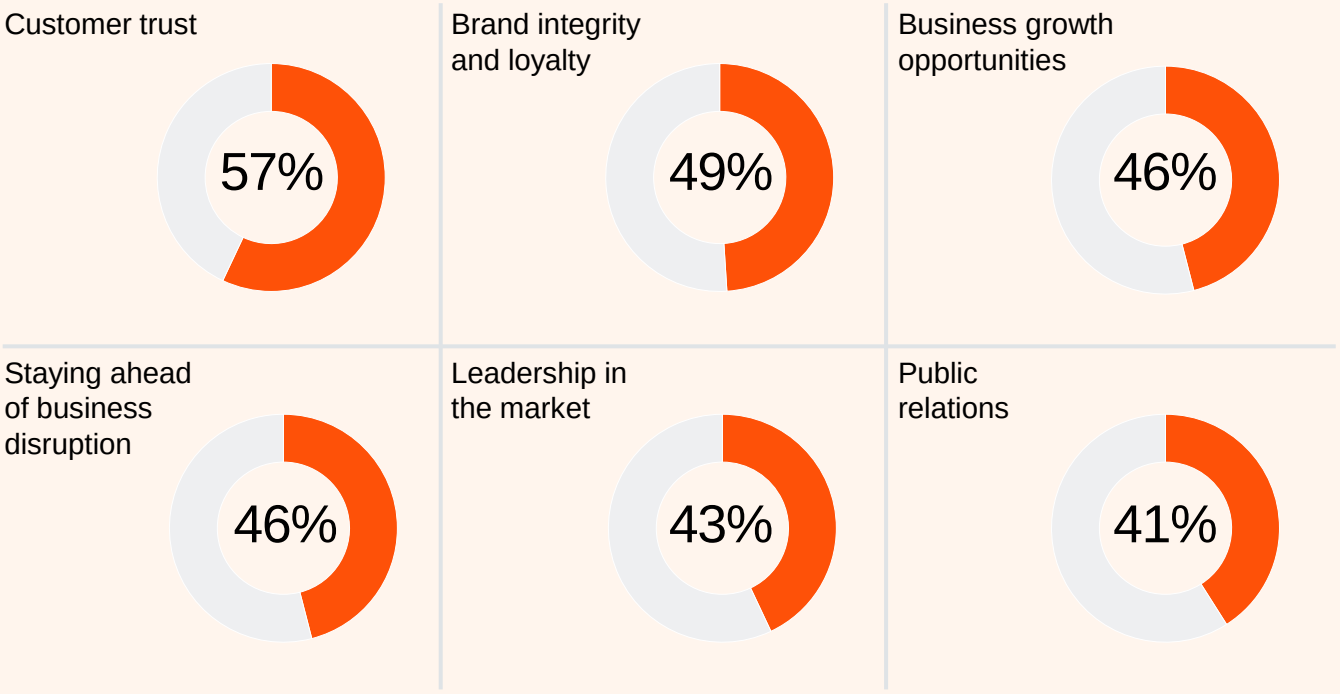
20% helped establish guardrails for technology innovation and transformation efforts.

19% helped become more resilient by mandating an industry-wide framework.

15% led us to consider cyber managed services to address regulatory requirements

Source: PwC 2025 Global Digital Trust Insights

Question: To what extent does your organisation position cybersecurity as a competitive advantage in these areas?



Source: PwC 2025 Global Digital Trust Insights

Tailored tactics deliver critical insights into sector-specific needs. For example, 47% of healthcare organisations report million-dollar breaches,[7] underscoring the importance of customised strategies. Offensive measures ensure organisations meet industry-specific needs, building long-lasting trust.

04 Strengthening resilience through compliance and standards

Adopting offensive strategies aligned with NIST, the Open Worldwide Application Security Project OWASP, and the Center for Internet Security (CIS) provides organisations with better tools for success. Techniques like attack surface analysis and threat simulations offer robust protections. Aligning offensive tactics with global frameworks ensures cybersecurity efforts deliver real value.

Continuous assessments and adapting to new challenges help organisations stay secure. Tailored strategies and constant testing reinforce systems, ensuring resilience while supporting key business goals.

03 How to design a strategic offensive programme

This framework is built on three key pillars:

01 The offensive cybersecurity lab:

This provides a secure space for organisations to simulate cyberattacks and identify vulnerabilities within their systems and processes. Techniques like penetration testing and red teaming allow for a comprehensive assessment of security measures. Insights gained from these simulations can inform GRC teams about compliance requirements and help streamline risk assessment processes, ensuring that policies align with the actual threat landscape.

These simulations inform GRC teams about compliance needs and streamline risk assessments, ensuring policies match the actual threat landscape.

Additionally, this programme fosters collaboration with departments such as Governance, Risk, and Compliance (GRC) and Incident Response (IR). For GRC, a proactive approach enhances risk management by identifying threats early and aligning policies with current threat landscapes, ensuring regulatory readiness. For IR, it improves preparedness by providing insights into attack vectors, refining response strategies through simulations, and enabling faster recovery from incidents.

02 Proactive threat intelligence platforms:

These platforms leverage advanced data analysis to predict and identify emerging threats. By monitoring global threat trends and attacker behaviours, they provide critical insights that can enhance collaboration with IR teams. For example, the intelligence gathered can be shared with incident response personnel to refine their strategies and improve readiness for real-world incidents, ensuring a unified approach to threat management.

03 Employee training and awareness:

Training programmes teach employees how to recognise and respond to cyber risks, such as phishing and social engineering. By incorporating simulated attacks and continuous education, these initiatives not only prepare staff but also create opportunities for GRC and IR teams to engage. Regular training sessions can include scenario-based exercises that involve multiple departments, fostering a culture of collaboration and shared responsibility in cybersecurity efforts.

By integrating these components, a strategic offensive cybersecurity programme not only empowers organisations to stay ahead of cyber threats but also promotes interdepartmental collaboration, enhancing overall resilience and adaptability in the face of evolving risks.

Next steps

To move from resilience to readiness, organisations must operationalise offensive cybersecurity. Start by establishing a dedicated OffSec lab, embed threat intelligence into core operations and make cyber training a continuous, cross-functional priority. The next step isn't to wait for threats - it's to simulate them, learn from them and lead through them. This is how cybersecurity becomes a catalyst for trust, innovation and long-term advantage.

References

1. SentinelOne
2. Offensive Cybersecurity Maturity eBook
3. MDPI Research Article
4. Aligning Cybersecurity and Business Objectives - Business Chief
5. PwC Global Digital Trust Insights. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
6. SANS Institute. Threat Hunting Survey: Hunting for Normal within Chaos. https://www.sans.org/white-papers/sans-2024-threat-hunting-survey-hunting-normal-within-chaos/
7. Jackson, N. (n.d.). Going on the offence: A Primer on an offensive security strategy. Bitdefender Blog. https://www.bitdefender.com/en-us/blog/businessinsights/going-on-the-offense-a-primer-on-an-offensive-security-strategy/
8. Hinojosa, G. (2024, November 12). From Compliance to Proactive Defense: How Regulations Are Driving the Shift Toward Offensive Security Governance. Cobalt. https://www.cobalt.io/blog/how-regulations-are-driving-the-offensive-security-shift
9. Accenture State of Cybersecurity Report 2021. https://www.accenture.com
10. Aligning Cybersecurity and Business Objectives - Business Chief. https://www.businesschief.com
11. Kim, A. (2023, December 18). SANS 2024 Threat Hunting Survey: Hunting for Normal within Chaos | SANS Institute. https://www.sans.org/white-papers/sans-2024-threat-hunting-survey-hunting-normal-within-chaos/
12. Enterprise, B. (n.d.). Going on the offense: A primer on an offensive cybersecurity strategy. Bitdefender Blog. https://www.bitdefender.com/en-gb/blog/businessinsights/going-on-the-offense-a-primer-on-an-offensive-cybersecurity-strategy
13. Mandiant. (2024, October 15). How low can you go? An Analysis of 2023 Time-to-Exploit Trends. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023
14. Navigate cyber risks with a tech-enabled approach. (n.d.). https://riskproducts.pwc.com/insights/three-cybersecurity-plays-to-help-meet-the-challenges-of-increased/
15. PricewaterhouseCoopers. (n.d.-a). A C-Suite Playbook - Bridging the gaps to cyber resilience. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
16. PricewaterhouseCoopers. (n.d.-b). Cloud attacks are top cyber risk concern: PwC 2024 Global Digital Trust Insights. https://www.pwc.com/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html
17. PricewaterhouseCoopers. (n.d.-c). Cyber Risk Strategy. https://www.pwc.nl/en/topics/digital/cybersecurity-privacy/cyber-risk-strategy.html
18. PricewaterhouseCoopers. (n.d.-d). Cybersecurity transformation. https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/transformation.html
19. PricewaterhouseCoopers. (n.d.-e). Offensive and defensive security. https://www.pwc.nl/en/topics/digital/cybersecurity-privacy/offensive-and-defensive-security.html
20. PricewaterhouseCoopers. (n.d.-f). Only 2% of businesses have implemented firm-wide cyber resilience, even as cyber security concerns are top-of-mind and the average data breach exceeds US$3m: PwC 2025 Global Digital Trust Insights. https://www.pwc.com/gx/en/news-room/press-releases/2024/pwc-2025-global-digital-trust-insights.html
21. PricewaterhouseCoopers. (n.d.-h). Rethink your cyber budget to get more out of it. https://www.pwc.com/mu/en/services/consulting/global-digital-trust-insights/cyber-budget.html
22. PricewaterhouseCoopers. (n.d.-i). Strategy, risk and compliance. . https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/strategy-risk-compliance.html

Contact us:

Raddad Ayoub
Partner, Cybersecurity
PwC Middle East
raddad.ayoub@pwc.com
linkedin.com/in/raddadayoub

Mohammed Ayesh
Director, Cybersecurity
PwC Middle East
mohammed.ayesh@pwc.com
linkedin.com/in/mayesh001

Waad Albayyali
Manager, Cybersecurity
PwC Middle East
Waad.albayyali@pwc.com
linkedin.com/in/waad-albayyali

Nayef Alaqeel
Senior Consultant, Cybersecurity
PwC Middle East
nayef.alaqeel@pwc.com
https://www.linkedin.com/in/nayef-alaqeel/

Raghad Al Sagga
Consultant, Cybersecurity
PwC Middle East
raghad.al.sagga@pwc.com
linkedin.com/in/raghad-al-saggaqa

Noura Alluhaidan
Consultant, Cybersecurity
PwC Middle East
noura.alluhaidan@pwc.com
linkedin.com/in/noura-alluhaidan-capm-84890023b

Fatemah Alrais
Senior Consultant, Cybersecurity
PwC Middle East
fatemah.alrayes@pwc.com
http://linkedin.com/in/fatemah-alrayes-83a329160

Joud Almazyad
Senior Consultant, Cybersecurity
PwC Middle East
joud.almazyad@pwc.com
https://www.linkedin.com/in/joud-almazyad/

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 149 countries with more than 370,000 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 12,000 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.