Middle East highest region prone to cyber threats in the world

Wael Fattouh, PwC Middle East Partner, Risk Assurance Services, talks to Saudi Gazette about cyber-attacks and investing in security

While companies in the Middle East are investing in security technology and protection such as cyber insurance, they are often not supported by the people, processes and governance required to provide real security creating a "false sense of security", according to Mike Maddison, PwC Middle East partner, cyber services leader and head of risk assurance services.

This year's PwC Middle East's Global State of Information Security survey reveals that these challenges are only likely to increase in the region whilst technology sophisticated is continually expanding.

According to the report, businesses in the Middle East suffered larger losses than other regions in the world last year due to cyber incidents, with 85% respondents in the region comparing to a global average of 79%. Around 18% of respondents in the region have experienced more than 5,000 attacks, compared to a global average of only 9% ranking the Middle East higher than any other region.

Many organisations in the Middle East approach cyber security solely as a technology problem and that is "simply not enough," said Wael Fattouh, PwC Middle East Partner, Risk Assurance Services. "Security is an end-to-end issue and ignoring any part of the chain can compromise the effectiveness of the implemented measures," he explains. "Another common misconception is when organisations think that compliance with security standards is the same thing as being secure, which is not accurate. Compliance helps an organisation implement good practices, but they need to fit into a frame that works for the unique nature of the organisation to be effective at securing it."

Despite an annual increase in strategic initiatives to improve security across businesses in Saudi Arabia, it continues to be a "hot target" for cyber criminals given its geographical, political and economic position in the region.

Companies often find it difficult to identify when an attack has taken place. Many only discover it when third parties or clients report suspicious messages or requests for funds. Asked about the challenge to detect early, Fattouh said the reason lies in investing in one aspect of security, such as technology, and ignoring other crucial ones such as people and governance.

He further says, "Early detection and effective handling of incidents requires a comprehensive and integrated security plan that takes into account all parts and stakeholders of an organization.

It would not be sufficient to have the correct tools, governance, and processes in place if the people in the organisation are not trained to deal with the incidents."

The attacks range from the direct theft of data through hacking, to coordinated spam emails and "phishing" attempts. "Attackers are becoming more innovative and are using new kinds of attacks that are constantly evolving, so you can't look for outdated signs of attack any more, your security and detection methods have to also constantly evolve," he said. "Virtually, every type of cyber-attack has been used against organizations in the Middle East and so businesses need to be informed of the latest threats and measures to counter them. This is where global knowledge sharing and threats information become critical."

There is no limit on the negative impact a cyber-incident can have on an organization in today's digital age. From loss of critical client and employee data, to financial losses due to fraud or disruption of business, the list of risks is a long one. Each company has a unique digital risk exposure that is closely linked with the nature of the organisation, and therefore it must be fully and carefully identified and mitigated at all levels of the organisation.

This article first appeared in Saudi Gazette in August 2016.