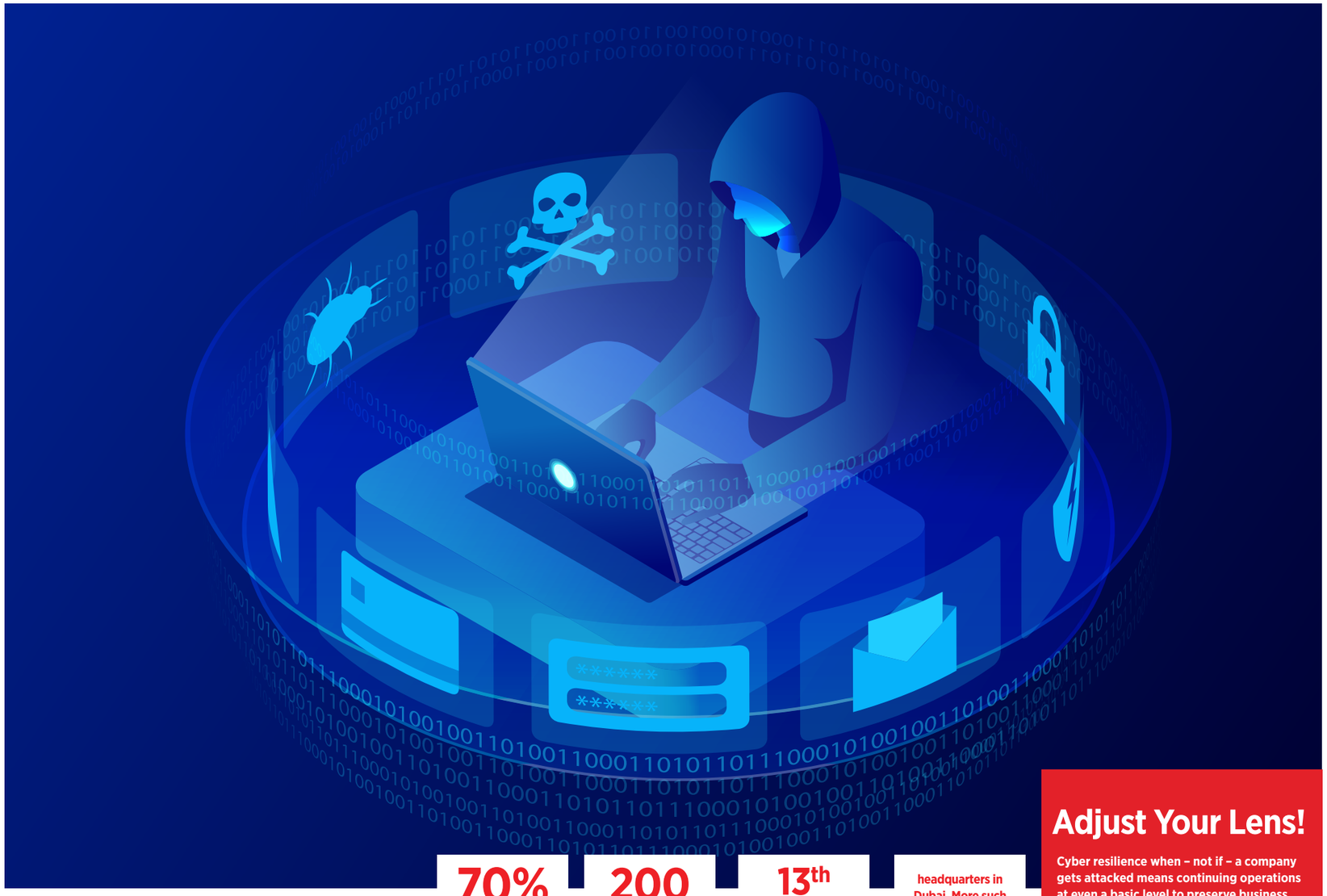
CYBERSECURITY

Think Hackers Out of the Game

BY RONNIE RAHMAN
Director of Cyber Security, Honeywell EMEA & APAC



The world's new, largely invisible and well-armed cyber "mafia" has its eyes on the mountains of hackable data being generated every millisecond in the energy industry, spurred by the 4IR. Energy stakeholders must master three defensive skills quickly: coordination, cooperation and speed.

The 4IR is not just a case of purchasing digital protection and injecting it into the operational fabric of a company. The response to cyberhackers, armed with deep pockets and sophisticated capabilities, must be far more sophisticated to safeguard Saudi Arabia, a regional hegemon and one of the world's biggest energy producers.

This is especially pertinent as threats worldwide escalate from online harassment that may have once temporarily shut down a website, to advanced cyber weapons that can paralyze a nation's energy grid. Attacks on cross-border digital infrastructure could also trigger a domino effect.

It pays to think long-term, which means building cybersecurity indigenously into the system now with the acceptance that you can't escape working with multiple vendors later. Nobody has the full spectrum of protection, so collaboration gives companies as much of an educated view as possible. Key questions that companies new to the cyber game need to ask include: What are the cybersecurity consequences for the technology the company has adopted and is it enough to buy insurance as protection, especially as it is increasingly part of regulatory compliance? Or must I do more?

> **"We all have the same problem; hackers do not respect budgets or borders. Our combined minds must be brighter than theirs."**

Collaboration also creates a more centralized view. The more data you have, the more you can correlate trends targeting certain sectors at certain times. Some attacks target organizations on Friday afternoon. Why? Because the staff has gone to Friday prayer. A centralized security intelligence center can address more predictable attacks, allowing resources to focus on preventing the most damaging digital assaults.

Communication is key to our defensive ability and speed of innovation. Feedback from clients, knowledge-sharing within industry and engagement with academia on skill development must be continual efforts. It also pays to learn from other sectors that have already had decades of trial and error, such as banking.

This is not a sprint nor a marathon; this road has no end and one solution does not fit all. But we do all have the same problem; hackers do not respect budgets or borders. Protection means working together; our combined minds are brighter than theirs. ■

70%
The percentage of Saudi citizens who rely on a fast and reliable internet connectivity to access government and business services, communicate socially and for education, according to the kingdom's National Cyber Security Center (NCSC). Persistent defense of this infrastructure is essential to a productive and secure economy.

200
The National Cybersecurity Authority (NCA) held a workshop in Riyadh with more than 200 governmental and representatives of vital sectors last December to discuss the state of cybersecurity in the kingdom and to showcase projects and initiatives. Reducing opacity through knowledge-sharing is essential to building companies' cybersecurity confidence.

13th
Saudi Arabia's ranking in the UN Global Cyber Security Index. This is especially impressive considering the kingdom only started taking significant action in recent years. This is a good start; the challenge of staying safe will only intensify.

1st
Honeywell opened its first Industrial Cybersecurity Center of Excellence (COE) at its Middle East headquarters in Dubai. More such centers are integral to combating the fast-moving mafia.

3.5mn
There is a global shortage of cybersecurity staff; 3.5 million such jobs will open globally by 2021, said Cybersecurity Ventures. The career path needs a marketing campaign to transform the perception that it means being lost.

Adjust Your Lens!

Cyber resilience when – not if – a company gets attacked means continuing operations at even a basic level to preserve business continuity while the disaster recovery gets underway. Building this resilience is not an overnight effort; it requires proactivity. Managers' viewfinders tend to be restricted to the cost implications of training, installation and monitoring, especially as there is no direct return on investment (ROI). But the negative financial impact of a cyberattack on an organization's health and safety executive (HSE), reputational value and the willingness of other companies to partner could easily exceed the cost of installing defensive measures now. Plus, the complexities of operational technologies (OT) will exponentially grow alongside intensifying market pressures and energy demand. Laying a solid foundation now will pay dividends in the 2020s and beyond.