HealthManagement
Promoting Management and Leadership

Want to think like a cybercriminal?

A new KPMG study reveals that a good number of businesses worldwide, including healthcare organisations, are "unprepared" to deal with a cybersecurity emergency. While the majority of these businesses (94 percent) are aware that they are actively being eyed by cybercriminals, only 22 percent said they are fully prepared to combat cybersecurity breaches.

The study "Taking the Offensive: Working Together to Disrupt Digital Crime" covered IT decision makers, including directors responsible for IT, resilience and business operations. Nearly half of these business executives admit they do not have a strategy in place to prevent cyberattacks, according to the study conducted in collaboration with BT Group, a British multinational telecommunications company,

The study also found that 51 percent of business executives do not have a strategy to deal with digital blackmail, such as ransomware attacks.

Nevertheless, cybersecurity issues are being raised at the highest level, with 73 percent of the business executives noting that digital security is on the agenda at board meetings at least quarterly, if not more so, according to the study.

“We live in a world where technology is all pervasive: Every aspect of human activity – business, defence, healthcare, education, to take but a few examples – is now underpinned by complex interconnected technologies and communications systems,” said Sir Michael Rake, chairman of BT Group. “Our dependency on technology raises significant governance issues with directors constantly having to balance questions of cost, risk and resilience. Today, digital security sits right at the top of the boardroom agenda. Directors are all too aware of the risks, regularly discussing them with their colleagues.”

However, as organisations implement increasingly sophisticated cybersecurity technologies, criminal organisations continue to find vulnerabilities to exploit.

As Rake noted, the sheer scale of digital criminality raises major questions as to how businesses can manage risk and defend against hackers whose strategies and technologies are constantly evolving.

“New thinking is required, and the first is to understand the digital criminal in terms of motive, modus operandi and how they intend to cash out," Rake pointed out. "The next step is to turn that understanding into a cohesive and effective response.”

Source: Healthcare IT News

Published on : Wed, 17 Oct 2018

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.