HealthManagement.org
Promoting Management and Leadership

Cybersecurity: The Need for Clear Standards

The lack of standardisation regarding security frameworks – and the implementation of those frameworks – is the biggest weak spot in cybersecurity today, according to a security expert with the FBI.

See Also: No Time to Lose: Get Serious About Cybersecurity Education

Malcolm Palmore, FBI assistant special agent in the cyber division in San Francisco, says there are many security frameworks available, there are recommendations from the government, but there are no required standards for the entire private sector landscape.

“Healthcare has sets of rules mostly governed by HIPAA that require them to put into place security levels of protection and to advise when those levels of protection have been violated. But outside of healthcare and the payment card industry, most companies are left to their own devices to figure this landscape out,” Palmore points out.

The FBI agent also shares some insights on how organisations can better protect their systems against cybercriminals.

“Information sharing is one of the key mitigation strategies that any information security practice can employ to enhance their security posture,” Palmore said. “There are a number of groups out there that provide intelligence on the cyberthreat landscape as it relates to malware, bot-nets and more, and the more entities that avail themselves of the information, the better the overall posture will be.”

He emphasised the importance of adhering to the fundamentals of information security.

“No matter how complex the impact, oftentimes what we find at the end in a post-mortem is information security fundamentals are not being adhered to,” he said. “Log management, auditing, identity access management, training personnel on awareness and social engineering and spear-phishing, and inoculating employees to these vectors so they are more aware – these all are key.”

He says that healthcare organisations should make use of the FBI to better prepare them to ward off cyberattacks. Most FBI field offices have an cyber-outreach composed of the management personnel in that field office responsible for cyber matters, according to Palmore.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 18 Apr 2017