HealthManagement
Promoting Management and Leadership

Improve Cybersecurity: Fire CEOs?

With healthcare cybersecurity taking a series of hits in recent months and the problem on the rise as hackers become more sophisticated, one expert says it is time to examine the administration of hospitals and incentivise employees to create a culture of security.

“Many executives have taken the view that cybersecurity is control of people, limiting people’s use, essentially telling people they are dumb, that they cannot use technology, that their ability to load software on their computers will be disabled,” said Mansur Hasib, a cybersecurity professor at the University System of Maryland. “Most companies run IT and cybersecurity where IT professionals live in these hallowed halls and they do not share knowledge.”

The *Healthcare IT News* report said that Hasib ran a pan-U.S. study across a wide range of organisations and made a disturbing discovery: half the healthcare sector operates IT and cybersecurity efforts through non-experts such as the CFO or the chief administrative officer.

Even more concerning is one-third of healthcare organisations do not even have a CISO and 20 percent have no intention of hiring one in the near future.

“Anthem, which had the biggest security breach in healthcare, runs IT through its chief administrative officer,” Hasib said in the report. “These executives, with their MBA backgrounds, have no clue about IT and security, so why is this person in charge of it? Yes, they have a CIO, but no real CIO should work for a CFO or CAO. If I am a CIO and I am not reporting directly to the CEO, then I am not a CIO.”

Hasib said that IT and cybersecurity education is lagging in graduate schools and this is contributing to the problem. At the same time, employees have daily access to technology and usage is increasing.

“That’s why there is a massive failure – the trust divide between executives and the common people,” Hasib explained. “Employees realise they do not have access or a role. But the reality is everyone handles data and technology, therefore the ultimate cybersecurity posture of any organisation depends on people. Behavior of people determines ultimate success.”

Hasib’s solution to is to the point: fire some CEOs. “If any CEO thinks their CFO can run their IT and cybersecurity, then that CEO does not belong in the CEO role.”

He added that, on the management front, there needs to be more emphasis on cultivating loyalty and incentivising employees to implement best practice in IT security.

“A company that does not have the loyalty of the people in its organisation will never have cybersecurity,” Hasib said.

He compared team management in healthcare to that of a nuclear power station he has studied. “There, safety is the culture,” he explained. “Every employee is incentivised. Their business is based on how many hours they can go without a safety incident. In healthcare, does any organisation give incentives for how many days without data loss? You can certainly have a goal of zero data loss, that is easy enough. What if you rewarded people for that? Everything is negative today, and people are not excited about negative stimulus. Leaders should give people incentives and reward innovation.”

Source: Healthcare IT News

Image Credit:Twitter

Published on : Mon, 4 Apr 2016