Majority of CEOs unwilling to share cyber-security information with outsiders

written by admin | February 24, 2016

(ZDNet – Eileen Yu: 2-17-16) Some 55 percent of CEOs acknowledge industry collaboration is necessary in fighting cyber-crime, but only 32 percent are willing to share their company's data on cyber-security incidents with others.

This reticence also conflicted with the fact that 55 percent of CEOs acknowledged industry collaboration was necessary to fight cyber-crime, according to an IBM study, which polled more than 700 CXOs in 28 countries. Some 24 percent of respondents were from the Asia-Pacific region, including Singapore, Australia, China, and India.

"This exposes a resistance to widespread and coordinated industry collaboration, while hacking groups continue to perfect their ability to share information in near real-time on the Dark Web," noted IBM.

The CEOs stressed the need for external parties to do more as well as stronger government oversight, increased industry collaboration, and cross-border information sharing. Asked about an external party's role in addressing cyber-crime, 61 percent of CEOs said governments should play a stronger role, while 53 percent said cross-border information sharing was essential.

"[It's] a dichotomy that needs to be resolved," it said, pointing to further findings that indicated confusion among CXOs about who the real cyber-security adversary was and how to fight them effectively.

For instance, the study revealed that 70 percent of the c-level respondents believed rogue individuals posed the biggest threat to their enterprise. The reality, though, was that 80 percent of cyber-attacks originated from highly organized crime networks in which data, tools, and expertise were widely shared, IBM said, citing findings from a United Nations report.

Some 54 percent of the CXO respondents did highlight crime rings as a concern, but 50 percent also pointed to competitors as equally worrying.

IBM Security's vice president Caleb Barlow said: "The world of cyber-crime is evolving rapidly, but many c-suite executives have not updated their understanding of the threats.

"While CISOs and the board can help provide the appropriate guidance and tools, CXOs in marketing, human resources, and finance–[encompassing] some of the most sensitive and data-heavy departments–should be more proactively involved in security decisions with the CISO," Barlow urged.

Because these business units managed sensitive customer and employee data as well as corporate financials and had access to banking details, they were among the primary targets for cyber-criminals, IBM said.

The study further revealed that 60 percent of CFOs, chief HR officers, and CMOs admitted they were not actively engaged in their company's cyber-security strategy and execution. Only 57 percent of HR heads, for instance, had deployed employee training in cyber-security.

The level of assurance also appeared to vary between the types of c-level executives within the organization. The survey found that 65 percent of CXOs were confident their company's cyber-security plans were well established. But while 77 percent and 76 percent of chief risk officers and CIOs, respectively thought so, only 51 percent of CEOs felt likewise.

"Considering that successful cyber-criminals are known to collaborate among themselves, it stands to reason collaboration on security management and incidents among organizations would contribute to risk reduction," IBM said.

"Among cyber-criminals, that collaboration takes the form of one actor discovering a weakness and making the knowledge available for sale for others to exploit. CEOs of cyber-secured organizations are much more likely to share incident data with external parties. They are three times more likely than others to collaborate with industry competitors, and twice as likely to collaborate with third-party security

services firms and vendors and partners."

Big Blue added that CXOs should recognize the value of external collaboration as a way to combat cyber-crime. As organizations shared more knowledge about cyber-criminals and their activities, including incident reports, the better prepared they would be to implement the necessary mitigation plans.

(Eileen Yu is an independent business technology journalist based in Singapore. In her *By The Way* blog, she covers industry developments in Singapore as well as other Asian markets, and enjoys pushing the line in her discussions about the impact of government regulations and policies.)