Information technology leaders feel ill-equipped to handle escalating cyber threats

February 20 2015

While the frequency and severity of cyberattacks against organizations are on the rise, a majority of information technology (IT) leaders do not feel confident in their leaderships' ability to leverage intelligence that can predict a cyber vulnerability and effectively combat threats, according to a new survey commissioned by Lockheed Martin.

A majority of survey respondents noted an increase in the severity (75 percent) and frequency (68 percent) of cyberattacks, but feared that they don't have the budget (64 percent) or the expert personnel (65 percent) to address the threats.

"This survey illuminates areas of concern about cyber readiness across government and critical infrastructure industries," said Guy Delp, director of cybersecurity and advanced analytics for Lockheed Martin. "The results highlight that the challenges in this domain are universal across both industry and government, and therefore our response needs to be equally holistic. The adoption of Intelligence-Driven Defense techniques is critical to ensuring that not only IT officers, but also chief executives, boards of directors and customers have confidence in the security of their information."

Other key findings include:

- **Many organizations are relying on intuition, rather than intelligence, to assess their security levels**: Business and government respondents who felt that they were not presently

being targeted for attack relied on their intuition (35 percent) or logical deduction (33 percent) rather than data or intelligence (32 percent) to justify their beliefs.
- **Whether malicious or negligent, insiders continue to be among the greatest perceived cyber threats**: Thirty-six percent of respondents said that negligent insiders were the most significant network vulnerability facing their organization, and more than half (53 percent) ranked malicious insiders in their top four threats.
- **The most serious risks do not receive the most budget**: The top two factors impacting an organization's cybersecurity posture – employee cyber awareness and supply chain security – receive only four and 15 percent of cybersecurity budgets, respectively. Top budget items, such as mobile and cloud security, are both perceived to be lower threat levels.

"Compliance was rated the top cybersecurity business priority by the survey respondents," added Delp. "Though somewhat surprising, it is a tell-tale sign that organizations feel the pressure to meet industry security compliance requirements. While satisfying compliance standards is important, organizations should view it as a foundation on which to build a more comprehensive security posture."

The Intelligence-Driven Defense survey was independently conducted in November by data security research group Ponemon Institute. It polled 678 U.S.-based senior IT practitioners from a variety of sectors, including financial services, the federal government, healthcare, utilities, energy, pharmaceuticals and chemicals. The margin of error for survey questions ranged from ± 1.1 percent to ± 6.3 percent, with an overall average of ± 3.8 percent.

Provided by Lockheed Martin

Citation: Information technology leaders feel ill-equipped to handle escalating cyber threats (2015, February 20) retrieved 3 May 2024 from https://phys.org/news/2015-02-technology-leaders-ill-equipped-escalating-cyber.html