Company boards lack deep security knowledge - survey

According to a recent National Association of Corporate Directors (NACD) survey, although almost 90% of directors at public companies claim their board discusses cyber risk regularly, only 14% have deep knowledge of the topic.

© JavadR via pixabay.com

Lutz Blaeser, MD of Intact Software Distribution, says that 60% of respondents said they find overseeing cyber risk a challenge. “Just over half of publicly listed companies, reported that cyber risk oversight falls on the audit committee, and 96% of directors that took the survey said the full board takes on the big picture risks that could impact their organisation’s strategic direction.”

The survey, says Blaeser, also highlighted that the most common board cyber-risk oversight practices are reviewing the organisation’s approach to protecting its most critical assets, followed by reviewing the technical infrastructure used to protect those assets.

Alongside all of this, the study showed the cyber threat landscape is becoming more complex and challenging, with a rise in nation-state attacks targeting both public and private sector organisations.

What to focus on in the event of a breach

“In the event of a breach, the Association recommends that executives focus on several areas. Firstly, discussions around which data and how much data the company is willing to lose or have compromised are important, as it will help establish risk tolerance and identify how much risk the organisation is willing to accept. Key to this discussion is identifying which information is crucial to the welfare and survival of the business, and which isn’t that important,” he says.

Next, they need to decide how cyber security investments and mitigation solutions should be allocated among basic and advanced defences. “When thinking about how to get a handle on more serious and complex threats, executives should train their most sophisticated defences on the company’s most critical data.”

At the same time, for less important data assets, businesses should consider accepting more risk than for higher-priority assets, as the costs of defence will more often than not exceed the benefits.

“Boards should encourage management to look at infosec investments in terms of their ROI, and should also relook at ROI on a regular basis, as the costs of protection and the company’s asset priorities will change over the months and years.”

The importance of value-added services

Blaeser adds that businesses across all industries and of all sizes have a plethora of security solutions available to them, all aimed at mitigating cyber risk and preventing breaches. “Add to this staff training, infosec and expert response services, which will add another layer of protection and expertise.

“It’s important to include these value-added services, and they highlight the necessity to move the cyber security discussion outside the IT department, and include the entire organisation.”

He concludes that there is also cyber insurance these days, which helps to meet some of the costs associated with a breach, including financial losses, damage to equipment and similar. “It is very hard, however, to put a price tag on a security incident. Conducting an assessment is not easy considering the sheer number of factors involved. It’s hard to quantify what a loss of confidence will truly cost the business, or a loss of future business.”