20 JUL 2017 NEWS

CISO Survey Finds GDPR Interest High

Dan Raywood Contributing Editor, Infosecurity Magazine
Email Dan Follow @DanRaywood Connect on LinkedIn

The top three issues for CISOs in 2017 are GDPR, security awareness and cloud security strategy, with two-thirds citing data breach response as "a major responsibility."

According to a survey of 39 senior security professionals by Club CISO, 78% of company boards still place their focus squarely on prevention capabilities, rather than response (22%). Despite the fact that 63% deem data breach response as a major responsibility.

Marc Lueck, chairman at ClubCISO, said: "It's evident from the research that there's a clear disconnect between expectation and reality of how information security can and should be managed. Despite the majority of CISOs having better lines of communication into boards, CISOs think many of their company boards still have information security priorities in the wrong order.

"Security is undoubtedly important for companies, but the temptation is to deal with tactical and visible threats rather than bake security and recovery into the organization holistically."

The research found that GDPR (79%), security awareness (74%) and cloud security strategy (61%) were the top issues for CISOs.

"In the wake of a growing number of cyber-attacks, an increasingly fragmented (and therefore vulnerable) workforce, and a step-up in the complexity and effectiveness of malware, 78% of company boards still place their focus squarely on prevention capabilities, rather than response," Lueck said.

"At the same time, these same boards contradict themselves by prioritizing breach response very highly. In fact, 63% cite it as a major responsibility of the CISO. In other words, boards want CISOs to clean up the mess after a breach, but they're not necessarily taking a balanced approach in investing in solutions that enable them to do this quickly and effectively."

Speaking to *Infosecurity*, Raef Meeuwisse, author of *Cybersecurity Exposed: The Cyber House Rules*, said that having had the luxury of directly seeing how over 50 different companies approach security, he was able to draw a number of observations that he turned into a set of rules:

- ***Rule 4*** – Security is thousands of times cheaper when it is embedded by design from the earliest stage. Security is not a paint that can be applied at the end. Applying security later on is more expensive than starting over is
- ***Rule 15*** – The extent to which your last lines of cyber-defense get triggered and used (for example incident response, recovery management and data loss prevention alerts) is an effective measure of how many gaps you have in your primary security defenses
- ***Rule 22*** – Fix the causes of security gaps before the symptoms. There is no point bailing water out of a boat that is riddled with holes. Fix key security processes and other root causes first, and then you can address the symptoms permanently, without fear of them returning

"I do not disagree that many boards are asking CISOs to work on papering over the cracks. However, I do think that there is a compelling case for changing the mindset of every executive board towards proactive security management," Meeuwisse added.

"The organizations that are coming through the major cyber-attacks unscathed are not doing anything super-clever, but they are applying all the basic and sensible security basics, such as timely patch management, restricted installation (administration) rights, regular back-ups and AI anti-malware."

Why Not Watch?

15 JUN 2015
APTs: Overhyped or Under-managed?

19 FEB 2015
Secure Data in the Cloud – Learn to Combat Cyber Threats to Protect Your Assets

25 FEB 2016
Protecting Your Moving Data – What to Consider When Implementing IT Controls to Comply with GDPR

8 SEP 2016
In an Uncertain Era of Brexit and GDPR, What is the Best Approach for Protected Data Transfers?

Related to This Story

Cyber-Threat and Regulation Priorities for CISOs
Raising the Stakes: Serious Cyber Security Preparations for 2017
GDPR Compliance: Time to Face Mission Impossible?
EU GDPR Final Countdown: How to Prepare Your Security Program