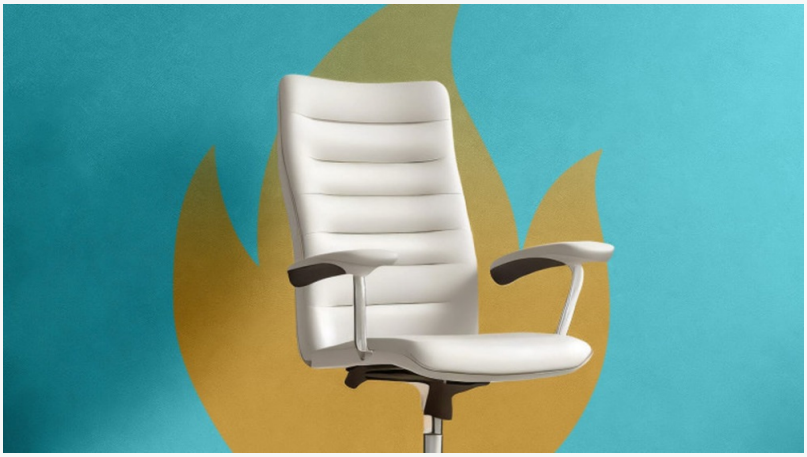
The buck stops here: Why the stakes are high for CISOs



DUBAI, UNITED ARAB EMIRATES, February 15, 2024 /EINPresswire.com/ -- Phil Muncaster, guest writer at ESET talks about the heavy workloads and the specter of personal liability for incidents that take a toll on security leaders, so much so that many of them look for the exits. What does this mean for corporate cyber-defenses?

Cybersecurity is finally becoming a board-level issue. That's as it should be, given the increasingly important role cyber-risk management plays in strategic decision making. Cyber-risk is fundamentally a core business risk with the potential to make or break an organization. That's certainly the thinking behind new regulatory rules in the US.

But by recognizing its importance, boards and regulators are also heaping more pressure on CISOs, without necessarily giving them suitable recognition and reward. The result: surging stress, burnout and dissatisfaction. Three-quarters (75%) of CISOs are said to be open to a change, up eight percentage points on a year ago. And 64% are satisfied with their role, down 10%.

These challenges have serious implications for cybersecurity within organizations. Addressing them should be an urgent priority.

An increasingly stressful role
CISOs have always had a stressful job. Among the drivers recently are:

- Surging cyberthreat levels, which leave many organizations in continuous firefighting mode
- Industry skills shortages that leave key teams understaffed
- Excessive workload due to increasing boardroom demands
- A lack of adequate resources and funding
- Workload that forces CISOs to work long hours and cancel holidays

- Digital transformation, which continues to expand the corporate cyberattack surface
- Compliance requirements that continue to grow with each passing year

It's no surprise that a quarter (24%) of global IT and security leaders have admitted to self-medicating to alleviate stress. The mounting stress levels don't just increase the likelihood of burnout and/or early retirement – they could lead to poor decision-making (as noted by this study, for example), as well as impact cognitive skills and the ability to think rationally. Indeed, It's been suggested that even the anticipation of a stressful day ahead can impact cognition. Some two-thirds (65%) of CISOs admit that job-related stress has compromised their ability to perform at work.

Scrutiny exerts further CISO pressure
On top of this baseline of stress has come extra regulatory, legal and board scrutiny over recent months. Three recent events are instructive:

- May 2023: Former Uber CSO, Joe Sullivan was sentenced to three years' probation after being found guilty of two felonies related to his role in an attempted cover-up of a 2016 mega-breach. Supporters claim he was scapegoated by then-CEO Travis Kalanick and in-house Uber lawyer Craig Clark, with Sullivan explaining that Kalanick had signed off on his controversial $100,000 payment to the hackers.
- October 2023: In a first, the SEC charged SolarWinds CISO Timothy Brown for downplaying or failing to disclose cyber-risk while overstating the firm's security practices. The complaint refers to several internal comments made by Brown and alleges he failed to resolve or elevate these serious concerns within the company.
- December 2023: New SEC reporting rules go into force, requiring publicly listed firms to report "material" cyber incidents within four business days from the determination of materiality. Firms will also need to describe annually their processes for assessing, identifying and managing risk and the impact of any incidents. And they'll need to detail board oversight of cyber risk and its expertise in assessing and managing such risk.

It's not just in the US where regulatory oversight is building. The new NIS2 directive set to be transposed into EU member states law by October 2024 puts a direct responsibility on the board to approve cyber risk management measures and oversee their implementation. Members of the C-suite can also be held personally liable if found negligent in cases of serious incidents.

According to Enterprise Strategy Group (EST) analyst Jon Oltsik, the increasing pressure such moves are placing on CISOs is making their core job of responding to threats and managing cyber risk more challenging. A recent ESG study reveals that tasks such as working with the board, overseeing regulatory compliance, and managing a budget are turning the CISO role from one which is technical to business-oriented. At the same time, the growing dependence on IT to power digital transformation and business success has become overwhelming. The survey claims 65% of CISOs have considered leaving their role due to stress.

Takeaways for CISOs and boards

The bottom line is that if CISOs are struggling to cope with workload, and in fear of regulatory reprisals and even criminal liability for their actions, they're likely to make worse day-to-day decisions. Many may even leave the industry. This would have a hugely malign impact on a sector already struggling with skills shortages.

But it doesn't need to be this way. There are things that both boards and their CISOs can do to alleviate the situation. It's in both of their best interests to find a way through this. Consider the following:

- Boards should assess CISOs' mental health, workload, resources and reporting structures to optimize their effectiveness. High attrition rates can lead to long gaps without a full-time CISO, which demotivates teams and impacts security strategy.
- Boards should remunerate their CISOs in line with the elevated risk their role now entails.
- Regular board-CISO engagement is essential, with direct reporting lines to the CEO if possible. This will help improve communication between the two and elevate the position of the CISO in line with their responsibilities.
- Boards should provide their CISOs with directors and officers (D&O) insurance to help insulate them from serious risk.
- CISOs should stick with the industry they love, and embrace greater responsibility rather than run away from it. But they must also remember that their role is to advise and provide context for the board. Let others make the big calls.
- CISOs should always prioritize transparency and openness, especially with regulators.
- CISOs should be mindful about what they circulate internally and ensure contentious decisions or requests from the C-suite are always recorded in writing.

When finding a new role, CISOs should hire a personal lawyer to run through their prospective contract in detail.

To optimize cybersecurity strategy, boards should start by reassessing what they want the CISO role to be. The next step is to ensure the cybersecurity professional in that role has enough support and sufficient reward to want to stay there.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

---

in today's world. Please see our Editorial Guidelines for more information.