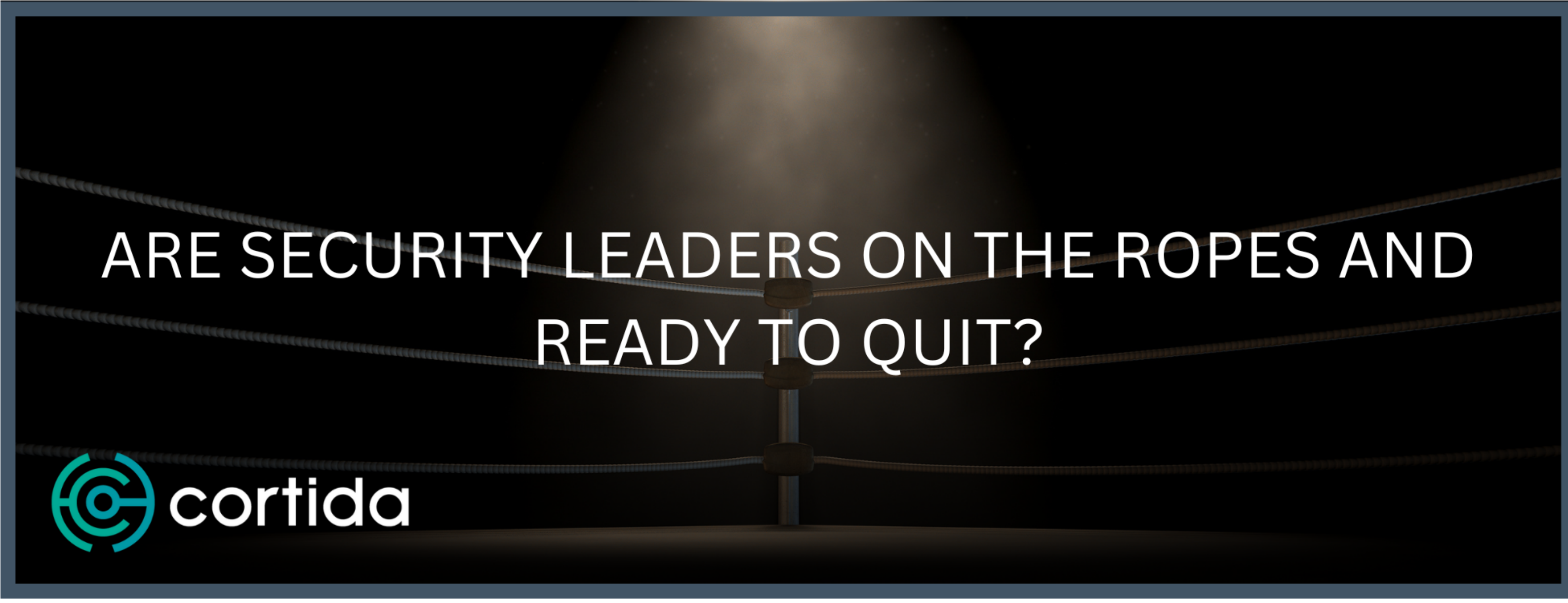

ARE SECURITY LEADERS ON THE ROPES AND READY TO QUIT?

Demand for cybersecurity leaders is outstripping supply and it's going to get worse.

CISOs are stressed out and are looking to quit. That's the key outtake from several recent surveys of cybersecurity professionals. Workplace stress is impacting not only staff health and retention rates but also security programmes and an organisation's ability to protect itself from attacks. In this short article we examine the pressures and what can be done.

For cybersecurity professionals, stress has always been part of the job. Some stress may be helpful or even motivating. But if it starts to negatively impact employee health, productivity or security, then it's time to act.

Gartner predicts that by 2025, 25% of cybersecurity leaders will pursue different roles entirely due to workplace stress. And nearly half will change jobs.[1]

Meanwhile a Cynet survey of small to medium-sized businesses with security teams of five employees or fewer found that 94% of security leaders reported being stressed at work. 65% confided that work stress levels compromised their ability to protect their organisations.[2]

Workplace stress is weakening security, but also driving churn as nearly three-quarters of security leaders had team members quit last year due to on-the-job stress, according to the same Cynet survey.

47% of security leaders reported more than one employee exiting their role. And 38% reported that they themselves were considering or actively searching for a new job. This then becomes a vicious circle, as talent churn adds to the stress of the cybersecurity staff that remain in-post.

What are the pressures?

Mounting threats, growing complexity and responsibilities, increasing compliance pressures and personal liabilities are just some of the factors contributing to workplace stress for cybersecurity professionals.

Security leaders are also having to do more with less as reduced budgets, hiring freezes and lack of qualified resources lead to untenable workloads. It's frustrating as well as taxing to be constantly in 'firefighting' mode, never being able to rest, plan or get ahead, no matter how hard the team works.

This contributes towards burnout and the classic symptoms of stress. These include difficulty concentrating and making decisions, feeling overwhelmed, constantly worrying, being forgetful or irritable. Not to mention also physical indicators of stress, such as headaches, dizziness and chest pain.

What's the impact?

A stressed-out security team is not operating at full capacity. It may be missing key threats and leaving the organisation vulnerable to attacks.

At the same time, the rise in churn rates is leaving organisations with a limited pool of candidates. This is exacerbated by the talent shortage across the cybersecurity industry.

When asked about their hiring process, 83% of security leaders in the Cynet survey said they'd had to compromise on candidate selection. And have hired employees who lacked the necessary skills and capabilities.[2]

What can be done?

With demand for cybersecurity leaders outstripping supply, engaging a virtual or embedded security leader could be a powerful, pragmatic solution to bridging the security gap.

A virtual or embedded security resource gives you access to experienced consultants who understand security and privacy issues and can bridge the resource and skills gaps that will continue to appear. They're able to translate risks into appropriate mitigating measures. And ensure that these are maintained and represented at board level.

Effective outsourcing is an alternative to insourcing, especially if you're recruiting a CISO, waiting for them to start or get up to speed. Or you simply need more security bandwidth and resource on a flexible basis.

Cortida offers a flexible embedded security leader or expert resource service. From short contracts of a few days a month, to longer contracts of five days a week, engagements can be tailored to fit your budget and circumstances.

Some of the support that Cortida has provided on such engagements include:

- Benchmarking current security posture
- Conducting risk, vulnerability and threat assessments
- Prioritising mitigation plans
- Driving improvement plans
- Introducing or managing security governance functions
- Leading standards projects such as IOS 27001, NIST, PCI DSS
- Running assurance programmes
- Reviewing and developing policy and procedures
- Assessing and managing suppliers
- Assisting the board on security and privacy matters
- Leading security teams

For more information on Cortida embedded consultant services please get in touch: info@cortida.com