Trustwave®

The Trustwave Difference: Your Trusted Partner in Cyber Security

Chief Information Security Officers (CISOs) need help. The average tenure of a CISO is 26 months, and nearly a quarter of Fortune 500 CISOs leave the position after less than a year. Suffice it to say, it's an extremely challenging, stressful position.

In being responsible for the security of their organization's data, CISOs bear an enormous burden, and many are not consistently provided with the tools they need to succeed.

Chief among those tools is alignment with the company's overall business goals. CISOs must also have buy-in from and the endorsement of both their CXO peers and the board. While this support should be table stakes, it can be surprisingly difficult to get.

In identifying their role and responsibilities, CISOs face the key question of who owns risk within the organization.

Is there a Chief Risk Officer? If not, does the CFO own risk?

Because cyber risk is a young field, the CISO must advocate for cyber/digital risk mitigation to both the board and whomever owns overall risk—and in some organizations, this question has not been fully answered.

While tackling these foundational challenges, CISOs also face a pair of ongoing problems that aren't going away anytime soon: budget, and the talent/skills shortage. Cybersecurity is a highly technical field that evolves quickly and constantly. Hiring and retaining top people has always been a vexing proposition, and will continue to be so for the foreseeable future. Few organizations have in-house all the expertise required to provide sound, holistic cybersecurity defenses 24/7.

Facing all these challenges, it's little wonder that CISOs have such short tenures. Fortunately, there is a solution at hand that provides industry-leading knowledge, budget flexibility, and a history of safeguarding business data.

The Trustwave Approach

When choosing a partner to ensure the security of your data, CISOs have a pair of goals. It's vital to address tactical needs that bring quick, quantifiable wins; these are results that CXOs and boards can understand and appreciate. At the same time, CISOs want to establish a stable, multi-year relationship with a partner that understands their long-term protection needs.

At Trustwave, we're proud of our 25-year record of success. We've been here for a quarter-century, and we'll be here next year. Companies we partner with consider Trustwave a long-term extension of their business. Unlike others in this crowded space, we are not a "popup vendor." And in today's uncertain environment, our global presence gives CISOs and their CXO peers confidence that we can grow and evolve with them through any future acquisitions and partnerships.

Additionally, CISOs appreciate the fact that Trustwave is a cybersecurity pure-play. This is our DNA, our muscle memory. We are hyper-focused on protecting our clients. We zero in on protecting their data and ignore any noise that would distract from that mission.

Trustwave isn't tied to any specific technology platform. We put our clients' needs first, helping them leverage their existing tech platform. We can do this because we're sophisticated enough to work well with any technology. Moreover, we help not only with threat detection/SOC analysis, but with projects: build, plan, test, run. We look at the lifecycle of your organization—and indeed at your entire supply chain ecosystem.

SpiderLabs

One of Trustwave's signature attributes is SpiderLabs. This industry-leading group, comprising four teams that are in constant communication with one another and with clients, brings those clients access to specialized world-class experts with decades of experience tracking threat groups, dissecting their tactics, and issuing alerts.

The Research Team maintains an extensive database of known threats while keeping a constant eye out for emerging threats.

The Penetration Testing Team includes some 120 professionals who help clients find vulnerabilities in their infrastructure. This team helps clients continually refine their defenses to improve their cybersecurity maturity through vulnerability assessments, penetration testing, and red/purple team exercises.

The Global Digital Forensics and Incident Response (DFIR) Team provides 24/7 on-call response services for retainer-based clients, and handles emergency situations for any company. The DFIR Team strives to quickly identify the source of the breach and the extent of the damage. We'll learn the origin of the breach and how it spread. We'll explain its consequences in terms of compromised resources and will recommend remediation procedures.

Finally, the Global Threat Hunting Team conducts deep threat investigations; its mission is to identify active adversaries in your environment using threat intelligence, threat actor TTPs, and cyber kill chain acumen to guide hypothesis-based hunts.

In the worlds of cybersecurity and of business in general, there's little that is certain—but one thing CISOs can be sure of is that new digital threats will emerge continuously. Trustwave's intent focus, long experience, and roster of highly trained experts offer security leaders the opportunity to focus on other aspects of their challenging job.

To learn more, visit our website or contact us.

CISOs Face Too Much Work, Too Much Stress

95% of CISOs work more than their contracted hours, on avg. $30,319 of extra time per year

88% consider themselves to be under moderate or high stress

48% said their stress level has impacted their mental health

40% said their stress levels affected relationships with partners or children

Source: "CISO Stress" report, based on survey of 800 CISOs and C-suite executives, by Nominet Cyber Security

Trustwave®

www.trustwave.com