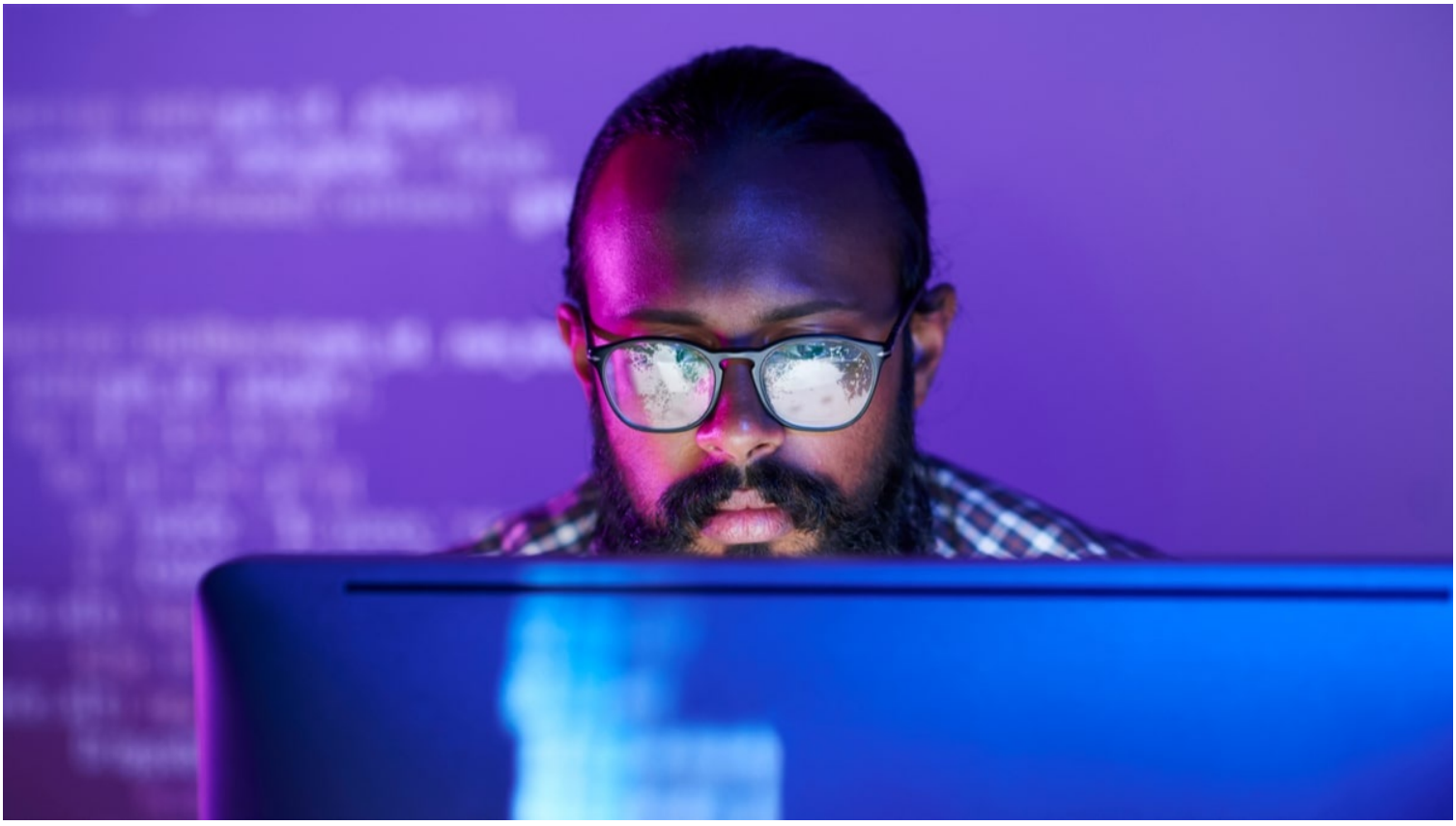
CISO churn – why it's happening and how to stop it

Only a quarter of chief information security officers (CISOs) last a year in the role. We look at the reasons behind this high turnover and ask what can be done to prevent it?

Technology

Aug 31, 2021 Christine Horton



Recent research has revealed that a staggering **24% of Fortune 500 chief information security officers (CISOs)** last just one year in the role, with the average tenure being just **26 months.** C-level positions necessarily involve higher levels of stress and responsibility than other roles, but why is it so much worse for security executives than for their peers in finance, HR or marketing?

The answer is that security teams undoubtedly face an incredible amount of pressure, arguably more so than any other department. A typical data breach today can cost organisations **over £3m,** which could cripple some completely or set them back years in terms of financial performance. That's a lot of weight for CISOs to carry, particularly if they're constantly fighting against the rest of the business.

"The high churn among CISOs is no surprise," says Anthony Young, co-CEO at security and risk consultancy Bridewell Consulting. "It's a very difficult position, with typical challenges including lack of authority, budget, and buy-in from the executive team who still see security as a cost rather than an enabler."

Young sees four main factors as driving churn among CISOs: fear of a breach and inability to do their job successfully, stress and burnout or being tempted elsewhere by better money and working conditions.

"Many leave an organisation because they feel they don't have the tools or support they need to do their job properly and that a breach is inevitable. They want to leave before this happens and it tarnishes their career," he says. "It's also quite common for organisations to hire a CISO and expect them to solve all their security problems, effectively pitching them as a lone superhero. This pressure and the expectation for CISOs to take responsibility for aspects such as system configuration, risk assessments and vulnerability scanning can cause high levels of churn among CISOs, who are unable to meet unrealistic expectations."

Never off-the-clock

Young says getting the board to understand the return on security investments can also be an uphill struggle.

"This results in fear and stress among CISOs who are fully aware that their current security solutions aren't sufficient and are working all hours to protect the business. The weight of this responsibility means it's not uncommon for CISOs to find their personal lives hugely affected by the stress."

"Hackers don't choose their hours and this tends to ripple into security teams and their leaders; you are never truly 'off-the-clock' as a CISO," says Paul Watts, who is now group CISO at data analytics and brand consultancy Kantar, following tenures at Domino's Pizza and Network Rail.

"In 2020, CISOs were working, on average, **10 hours per week beyond their contracted hours**; in lockdown, this appears to have increased for a number of CISOs. I was regularly working 12- to 14-hour days, certainly during the first lockdown. This puts strain on personal commitments and family dynamics; I've heard numerous examples of relationship problems with partners and children. This is amplified for CISOs who work for multinational organisations – where there is an expectation that the security lead is always available."

Hackers don't choose their hours and this tends to ripple into security teams and their leaders; you are never truly 'off-the-clock' as a CISO

Additionally, Watts says that in terms of rewards and benefits, CISO salaries are low in comparison to those of similar senior roles, especially when the levels of responsibility and stress are factored in.

"CISOs can feel very vulnerable and lonely in their roles – it can be seen as a thankless job. They are also at moderate risk of becoming the immediate scapegoat if a security breach occurs, even though it's highly unlikely that the fault was directly theirs, especially if the root cause was underinvestment, poor culture or poor business-risk choices."

Regarding responsibility, Watts also points out that there is a noticeable difference between the CISO and CIO (chief information officer) when a cybersecurity incident occurs. "How many CIOs lose their jobs when an organisation suffers a major outage? The answer is not many!"

Affecting mental health

Even before Covid-19, the CISO's role was fraught with challenges, says clinical psychologist Dr Nick Taylor, CEO and co-founder of workplace mental health platform Unmind. He points to **a recent report** that shows a staggering 88% of CISOs feel moderately or tremendously stressed dealing with their high-pressure, high-demand and high-stakes job.

"The pandemic compounded this already high level of stress and the risk of burnout," he says. "The move from office to working from home has created uncertainty alongside the constant responsibility of keeping their company safeguarded from security threats. In fact, almost half of CISOs said work stress has had a detrimental impact on their mental health."

With CISO churn rates of less than two years, it also means you never get to the bottom of some of the more fundamental security challenges

Killian Faughnan is group CISO at online gambling company **William Hill** and has been in the role for two years and eight months. He believes a large part of CISO churn is due to frustration with progress.

"Many CISO activities are long-term, iterative improvement programmes, solving fundamental problems that were never addressed properly, with the occasional firefighting thrown in for good measure. It can be challenging to feel a sense of accomplishment without stopping to deliberately take stock," he says.

The churn becomes a bigger problem when each new CISO demands a reset of strategy, priorities and commitments, with old roadmaps torn up and new ones established. "While a refresh of strategy and roadmaps is often necessary, with CISO churn rates of less than two years, it

also means you never get to the bottom of some of the more fundamental security challenges," says Faughnan. "What I've found is that most roadmaps from the last CISO's term were not too far off the mark, so I prefer to fight to keep those same fundamentals. Then, the CISO after me shouldn't inherit any insurmountable challenges."

Lack of business commitment

"Where I've seen CISOs have short tenures, it's often because the business isn't fully committed to security as an ongoing programme of work," says Tash Norris, head of cybersecurity at online greeting card and gifts firm Moonpig. Norris has been in her current role for nearly two years, leading the security team and wider technology function through a demerger and IPO.

"A lot of CISOs are really at the mercy of the product and technology teams who prioritise and implement security fixes, and quite often, the prioritisation of those fixes are either not well understood or well communicated," she says. Norris adds that this can lead to security teams finding themselves responsible for security events that they not only foresaw but that they actively lobbied to fix.

"I believe it's this pressure that causes many CISOs to feel like they don't have the right level of influence within their organisation to be effective and successful in their role. So, ultimately they choose to leave.

"CISOs require accountability and authority to be effective, not just accountability."

Norris says that security is considered an enabling function at Moonpig. "This not only helps to ensure a secure product but also my enjoyment of my role, which ultimately reflects in tenure," she says. And while she agrees that other C-suite positions experience elevated stress levels due to lack of resources, for the CISO this issue could ultimately lead to significant negative media coverage, regulatory action and worse still – it could have a negative impact on or even harm their customers.

"The success of your CISO very much depends not only on the financial investment in their function but also the support from their peers across the business," she says.

Stopping the churn

So is there anything businesses can do to help stop the churn? Unmind's Dr Taylor says when it comes to employee retention, there aren't really any shortcuts.

"Principled leadership, inclusive cultures, accessible and empathetic support, and openness around mental ill-health are all fundamental factors for creating engaged, healthy and happy cultures, particularly at a C-suite level," he advises. "Employers can take practical steps to support these areas among their workforce and provide tools to help them nurture their own mental health. But the problem of high churn rates among CISOs won't go away until businesses tackle the root causes of unhealthy levels of stress head on."

Watts believes that company boards should give the CISO impartiality and independence, allow them direct access to the board and audit committees, as well as recognising them as trusted advisers.

"Regulators and governments should continue to reinforce with business leaders that the buck stops with them when it comes to security and risk management, and ideally legislation should support the CISO in being fully effective in their role and not the sacrificial lamb," he says.

Watts also advocates for CISOs to spend more time connecting with and getting the support of the business. Ideally, too, those holding the purse strings should give the CISO the headcount and bandwidth they need to do their job effectively: finance, people, tools and resources. But, in return, CISOs should be more articulate about their vision statements and be able to express these in language that resonates with the board. And if they can, CISOs should recruit people into specific leadership positions within the security team, and trust and empower them.

Embedding change and improvement requires a consistency that could be lost with a regular 'changing of the guard'. Businesses need to therefore ensure that CISOs have the right authority, budget, team and technology stack to do their job effectively – and help to stop the churn.

Written by
Christine Horton

Long-term contributor to specialist IT titles, including Channel Pro and Microscope, she writes about technology's impact on business

Related Articles

RACONTEUR

Raconteur Media, 2nd FloorPortsoken House,
155-157 Minories, Aldgate, London, EC3N 1LJ