A FALSE ECONOMY

Jamal Elmellas *looks at whether the short-term fix of cutting costs could have harmful long-term consequences*

Over the course of the past year, we've seen businesses look to make the security function more efficient and streamlined which has inevitably led to cutbacks. Contraction in spend has also hit vendors, some of which have cut their workforce by between 10-20 percent (most recently Sophos cut back its global workforce by 10 percent in January), but security professionals across the board are now beginning to feel the pinch.

The ISC2's Cyber Workforce Study 2023 found almost half (47 percent) of respondents had experienced layoffs, budget cuts and hiring or promotion freezes. The top ways of making cutbacks included delayed purchasing/implementing new technology (53 percent), cutting training (35 percent) and not renewing cyber software licenses (24 percent). But could these steps to conserve spend end up doing more harm than good?

The sector is in a highly unusual position. It's experiencing an economic downturn while, at the same time, cyber security skillsets are in high demand. Usually, the market swings either in the hirer or the candidate's favour but here there is almost a case of stalemate. Most cyber security personnel are staying put, but those that are laid off – who would normally expect to see salaries take a dive – are finding remuneration remains fairly buoyant due to companies competing for a scarce resource. CISO's, for example, have continued to see salaries increase by 11 security professionals across the board are now beginning to feel the pinch over the course of the past year, according to the IANS 2023 Security Organisation and Compensation Study Benchmark Summary Report.

Security professionals are beginning to feel the pinch as vendors cut their workforce by between 10-20 percent

At the time of writing, the IT Jobswatch UK site showed that the number of permanent vacancies had almost halved in the six months ending 2023 compared with the same period a year ago, standing at 3,625 no doubt due to the hiring freeze. But cybersecurity vacancies are outpacing other professions. Demand remains positive, up 15 rankings to year end 2023, and the median salary is at £60,000, down only £5,000 over the past two years. Which begs the question, how are organisations meeting these salary requirements in these cash strapped times?

In some cases, salaries are being paid for by making cutbacks to other elements of the business including investment in the existing workforce's personal development. The ISC2 study reveals that 35 percent have eliminated cyber security training programmes, which are a critical resource for developing skills and closing skills gaps, while *The State of Cybersecurity 2023* report from ISACA found there was a significant increase in those declining to reimburse tuition expenses. With respect to university fees these were down from 33 percent in 2022 to 28 percent in 2023 and certification fees also dipped, but the worrying gap is between those paying for initial certification (65 percent) and their associated renewal fees (55 percent). This signifies that employees will be expected to pick up the tab to keep their certifications current, which is not only liable to hurt the development of certified practitioners but also the advancement of the sector as a whole.

Indeed, the ISC2 study found a correlation between those organisations that didn't pay for renewals and the skills gaps they faced. It turned out that 47 percent of those organisations that did not offer reimbursements for certification courses or exams had significant skills gaps in cyber security, compared with only 38 percent that do offer reimbursements. What this reveals is that the erosion of training and development poses a long-term threat to the ability of the organisation to attract and retain talent.

Another major issue is the immediate threat to business defences by culling staff. The ISC2 report found 57 percent of workers said the shortages were putting the organisation at a moderate or extreme risk of cyber security attack. Half said they no longer had sufficient resource to devote to risk assessment and management, 45 percent reported oversights in process and procedure, and 38 percent said they'd be unable to deal effectively with misconfigured systems, with the same percentage saying teams were now slower to patch critical systems.

Overall, 62 percent of cyber security professionals said that corporate cutbacks like layoffs, budget cuts and hiring freezes reduced their ability to prepare for future threats. So while short term the business may be conserving spend, it could ultimately pay a much higher price due to the financial and reputational loss associated with a breach or compromise.

It's a situation also noted in the State of Security Observability 2023 report, which found that those that do make cutbacks go on to suffer more security incidents per month. Even so, it reports 47 percent of respondents plan to cut cyber security headcount and 60 percent of those also plan to cut spend on security infrastructure.

Yet there's also another cost to the business and that is confidence and morale. Uncertainty over the security posture was found to be higher among those organisations that had laid off cyber security staff over the past year (63 percent) compared with those that hadn't (47 percent) in the ISC2 report. Following such cutbacks, 40 percent reported the security team had either been restructured or moved within the organisation and 71 percent of those remaining reported their workloads had increased, 63 percent that morale was lower and 62 percent that productivity levels had dropped. Moreover, those with staffing shortages and skills gaps said relations between teams and senior management soured as they felt unsupported and undervalued.

IT HAS BECOME CLEAR THAT SIMPLY CUTTING COSTS IS NOT A SUCCESSFUL STRATEGY

The danger, too, is that organisations will assume that they can just build teams back up once the economic situation improves when in reality the skills gap and staff shortages is set to widen. The global cyber security workforce stands at 5.5-million today, estimates ISC2, but the gap almost equals that at 4-million. The workforce is growing at an annual rate of 8.7 percent, but the gap is growing faster at 12.6 percent – which means demand is not only outstripping supply, but is accelerating.

Those organisations that have not cut back sympathetically, have overloaded staff and failed to invest in their professional development are therefore going to find it especially difficult to attract and retain staff when the market returns to normal.

If we look at results from the past year, it was already proving difficult to fill certain roles, with 71 percent reporting unfilled cyber security positions, half of which were for non-entry level roles – ie those that need to have been able to advance their careers which take at least three months to fill, according to the ISACA survey.

Therefore, the long-term repercussions of these cutbacks could well come back to bite the business in numerous ways, from dissatisfied and overworked staff to exposing the business to compromise, to a difficulty to then grow the business when the economy recovers. But there are steps the business can take to help it weather the downturn and to put it in a better position to recruit.

An important distinction drawn in the reports is that there's a big difference between staffing and skills shortages. The former refers to the number of boots on the ground in terms of numbers, but the latter is the skills those team members have. Arguably it's this lack of skills that is more damaging. Over half (58 percent) of those questioned in the ISC2 survey said that they can mitigate shortages if they have an efficient distribution of skills across the team, making training in specific disciplines a priority.

The top skills in demand are in cloud computing security (35 percent), artificial intelligence (32 percent) and machine learning security, and Zero Trust (29 percent). If the business can rationalise staffing numbers while investing in the professional development of those that they retain – ie by really focusing on workforce planning to fill those skills gaps – they can counter the negative effects of the downturn.

BETTER PREPARED

The ISC2 states that those who continued their training, education and certification reimbursement programmes were far better prepared to weather times of economic uncertainty. Even those organisations that made layoffs but kept such programmes running were less likely to experience significant organisational skills gaps in cyber security.

57 PERCENT SAID STAFF SHORTAGES ARE PUTTING THEIR ORGANISATION AT A RISK OF CYBER ATTACK

It's also fair to say the sector does have the capacity to weather this storm. It's not been nearly as hard hit as other industries, with Layoffs.fyi – which charts dismissals – placing security in 15th place, way down the list. Retail, consumer and hardware hold the top three positions losing between 20,000-40,000 personnel in 2023 compared with 5,000 in security. Closer examination reveals most of those security businesses that did let staff go did so as a result of IPOs, funding rounds or acquisitions, suggesting that it was growth rather than contraction in the market that was the primary driver.

Going forward it's vital that these businesses begin to value people as their biggest asset otherwise they can expect staff turnover to increase. A government report, Cyber security skills in the UK labour market 2023, estimates that 11 percent of the cyber workforce within the cybersecurity sector left their posts between January 2021 and July 2023 and has remained fairly consistent over the past three years. However, 9 percent of those, equivalent to 82 percent, chose to leave of their own volition. They were consistently skilled staff such as security architects and so were hard to replace. The reason these professionals voted with their feet was overwhelmingly due to the company offer not being good enough (61 percent), knocking pay and benefits off the top spot. What's more, as it was employers the survey quizzed, not the employees who had left, those doing the hiring are all too aware that a failure to invest in the individual is driving away the talent.

Given the unique pressures bearing down on the cyber security sector, it's clear that simply cutting costs will not be a successful strategy. The increasing demand for certain skills, of which there is a diminishing supply, suggests that those businesses that think ahead, concentrate on workforce planning to spot skill deficits, anticipate future demand and invest in staff will likely emerge in better shape. In contrast, those that have cut investment without carrying out that level of analysis are liable to lose talent that will then be even more difficult to replace. So perhaps if 2023 was the year of the efficiency drive, 2024 should be the year where professionals are put first ●

Jamal Elmellas is Chief Operating Officer at Focus on Security, the cyber security recruitment agency, where he is responsible for delivering an effective and efficient selection and recruitment service. He has 20 years' experience in the field and is an ex CLAS consultant, Cisco and Checkpoint certified practitioner.

The erosion of training and development poses a long-term threat to the ability of an organisation to attract and retain talent