TRIDENT SEARCH

How to tackle the staff retention issue in Cyber Security

Within the cyber security sector there is a commonplace trend that people tend to move between roles fairly frequently. For employees this offers continuous exposure to new challenges but for an employer losing staff is a costly, time-intensive and culturally impacting exercise.

As a cyber security specialist recruiter, Trident Search is uniquely positioned with a holistic view of the industry and can offer deep insight into why this market is so kinetic and what employers can do to improve retention rates.

Disclaimer: there is no silver bullet solution that will see an organisation retain all its best employees, but if an environment is cultivated that offers continuous opportunity for growth and new challenges then that's a job well done.

"A total of 4 in 10 cyber firms expect at least 1 member of staff in a cyber role to leave within the next 12 months."

"The vast majority (74%) of this group of firms are confident that they will replace the skills lost when these staff leave. However, the remaining 23% are not confident."[1]

When speaking to candidates the most frequent responses to the question 'why are you looking to move?' are:

- **Career progression**
- **Compensation**
- **Burnout**
- **Cultural fit**

Beyond these popular answers there are additional reasons for leaving outside a candidate's control, such as lack of stability, a change of office location or perhaps other personal reasons. However, let's focus on the most common responses for now, around which Trident can offer industry-specific advice to improve on employee retention within the cyber security industry.

Career progression

Career progression is the most common reason we see cyber professionals looking to move jobs. Delving deeper, some of the more specific restrictions employees come up against include:

Glass ceiling effect: A phenomenon preventing well-qualified and experienced individuals from career progression due to factors outside of their control.

Lack of L&D: Cyber professionals are passionate and hungry to continuously learn as technology is always advancing in this sector. Providing little to no technical training or support to gain certifications is a growing problem amongst organisations.

[1] www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020

Trident Advice:

- Organisations need to foster an environment of transparency with their employees that encourages honest conversations around progression and promotions. Open discussions will allow both parties to understand better what each side needs and the other can deliver, ensuring realistic expectations are set.
- Lack of technical training is inexcusable; employers simply need to make time to invest in their employees. “We were too busy” or “lack of resources” are not acceptable answers if companies wish to improve retention.

Compensation

This can be an awkward one to tackle. If someone is looking to move on solely for money, then you must ask the question ‘are they the kind of person that I want in my team/organisation?’.

However, there is a vast difference between being greedy and wanting to be recognised for a good ol’ honest day’s work at the fair market rate.

Delving deeper, a sudden desire for greater financial compensation may be the result of:

Recruiters: Uneducated headhunters inflating salaries to make an opportunity seem attractive and ill-advising your staff how much they should be earning.

Sector specific: It is no secret that working for a global bank pays more than a startup or a not-for-profit.

Trident Advice:

- It is in an organisations interest to keep up to date with the market compensation levels and engaging in a continuous dialogue with recruitment partners is the easiest way to achieve this.
- Whilst SMEs cannot necessarily compete with the salaries of big banks, demonstrating to employees the value of their work and their contribution to an organization can be just as rewarding as financial compensation. Providing an employee with more responsibility and flexibility is not to be underestimated as a key factor in retaining employees.
- If an organization cannot match that of a competing financial offer there are alternative ways to add value to an employee’s role. Investing in technical training, supporting accreditation, implementing bonus schemes, and offering flexible working can bring just as much value.

Burnout

This is an ever-growing issue within any high-performing industry, and cyber security is no different. At CISO level burnout is a very serious issue, with the average tenure just 26 months.

We often see the dilemma of a cyber practitioner demonstrating their best octopus impression and managing the workload of multiple people. For a manager to have an employee who is willing to go the extra mile on their professional duties can seem like a dream; however, employers should be very mindful that this imbalance of responsibility rarely ends well over long periods of time.

Trident Advice:

- Managers should take time to work on interpersonal leadership qualities, conducting 1-2-1s regularly, and being attune to behavioural changes. An open and trusting dialogue with employees will allow managers to better understand individual motivations.
- Frequently review individual and team workloads – should one member have considerably more work than the rest of the team it is down to the manager to look deeper into the reasoning for this. Is it poor work delegation or eagerness on the employee's behalf?
- Build a good relationship with the budget holders and demonstrating commercial value to invest in additional resources.
- Ensure that the importance of a work/ life balance is prevalent and emphasised within the team environment. Additionally, organisations should only require office presence from employees when necessary.

Cultural fit

A timely topic to discuss. With a global pandemic restricting in-person interaction, maintaining a culture within teams has become increasingly hard, and on-boarding new starters even more so. Cyber security is a small sector and having a negative reputation regarding workplace culture will affect a firm's ability to hire and retain.

The below stats were taken from a relevant gov.uk report which was published in 2020:

- *"15% of the cyber security industry workforce are female"*
- *"16% of the cyber security industry workforce come from ethnic minority backgrounds."*

Trident Advice:

- Having a mission and a vision that everyone understands and can be brought into. The aim is to have the team all pulling in one direction as a cohesive unit.
- Organisations receive better quality of work from employees who feel like they are respected, trusted and valued. Rewarding employees financially, socially or professionally will demonstrate investment from a company in their workforce and create a positive work culture.
- Working with recruitment partners is the optimal way for an organization to put processes in place to encourage a more diverse workforce, e.g. anonymous CV applications.

In summary, organisations that invest in their staff, on both a personal and professional level, and demonstrate real leadership qualities, such as empathy, integrity and will stand out as desirable employers within the cyber security sector. Cyber practitioners are highly intelligent, motivated individuals, so by giving them a purpose, within a great culture and fairly rewarding them will see an increase to retention rates for employees in this industry.