SOLVING THE PERSONNEL PUZZLE: WHY CYBER SECURITY RECRUITMENT IS A NEW CHALLENGE FOR HR

Today, Human Resource (HR) teams are responsible for managing staff internal operations and are tasked with the all-crucial role of recruitment. Choosing the right candidate who will align with the organisation's goals and help drive strategic objectives - can be at the best of times - considered a scientific art. This two-fold HR responsibility comes with real and lasting impact on future organisational success.

With such power comes responsibility, especially in recruiting mission-critical roles such as cyber security specialists. The very nature of cyber security roles are specialised, technical and highly dynamic. The rapid pace of change in the industry means requirements are constantly shifting - last year's job description became this year's backdoor vulnerability, and HR need to be aware. And herein lies the HR quagmire.

APPROXIMATELY 289,000 PROFESSIONALS IN THE UK WORKFORCE HAVE JOB DESCRIPTIONS THAT INCLUDE SECURITY RESPONSIBILITIES ACCORDING TO THE 2019 (ISC)2 CYBERSECURITY WORKFORCE STUDY.

LinkedIn figures cited 61% of developer jobs are in organisations outside the actual technology industry, but as every company relies on technology to function, the actual figure is much higher.

This overwhelming mission-critical and security sensitive hiring process means every company needs cyber security staff, yet not every company's HR team is equipped and cyber-savvy. HR face challenges attracting and vetting suitable cyber security talent.

THE 2019 IPSOS MORI SURVEY REVEALED THAT “MORE THAN HALF OF ALL UK BUSINESSES HAD A BASIC TECHNICAL CYBER SECURITY SKILLS GAP.”

Countless studies conclude the same, but businesses have yet to resolve the problem effectively. Budgets for training and development still lag behind, and HR staff are not afforded the time and money needed to hire effectively for cyber security.

One size does not fit all in cyber security recruitment. Complex and extensive recruitment policies that work well for other departments are not fit-for-purpose in the hiring process for cyber security experts. An industry with niche specialisation requires a recruiter with a specialised niche skill set. Most in-house HR teams lack cyber security subject matter expertise.

The ability to develop skills and learn new topics is highly prized, but traditional recruitment policies inhibit such, meaning the best candidates often fail second-stage shortlisting.

A RECRUITMENT MODUS OPERANDI NOT CUSTOMISED FOR CYBER SECURITY PROFESSIONALS STUNTS POTENTIAL, AND LIMITS THE HIRING COMPANY'S ABILITY TO RECRUIT AND RETAIN THE RIGHT CANDIDATES.

The quandary developing for human resource departments: how can you successfully hire the right cyber security staff, whilst reducing costs, quickly resolving staff gaps, attracting higher quality candidates, and satisfying internal and external service expectations?

The Landscape of Cyber Security Recruitment?

Cyber Security has traditionally been viewed as realm for IT departments where senior managers are expected to manage the daily-tasks and activities. With the rise of the internet and online business transactions, the greater reliance on technology for almost every industry has propelled cyber security into a company-wide issue.

While technology like malware protection or anti-virus software was previously deployed to alleviate these issues, they are akin to temporary plasters on a gaping wound of security.

PART OF THE CHALLENGE IS THAT MOST EMPLOYEES ARE BLISSFULLY UNAWARE OF THEIR COMPANY'S SECURITY TEAM ROLE.

When asked, most assume the installation of anti-virus software and the occasional stress-testing for security awareness. They are not to blame, as cyber security teams don't announce new projects or quarterly targets like other departments (such as sales and marketing). Cyber security teams are absent from planning meetings, and they are traditionally positioned away, in different departments, only visible when there's a security issue or a new project is ready to ship.

Companies are recognising the need to hire proper cyber security staff, including Chief Information Security Officers (CISOs) or Chief Information Officers (CIOs), but hiring correctly in this niche is challenging for HR staff who are usually unaware of regulations and the desired skill-set they should seek in a candidate. Consequently, businesses find themselves making poor hires for their cyber security teams which is symptomatic of high staff turnover and low recruitment retention rates.

GETTING IT WRONG IN CYBER SECURITY RECRUITMENT IS EXPENSIVE, WITH THE AVERAGE COST OF STAFF REPLACEMENT £30,614, ACCORDING TO OXFORD ECONOMICS.

How can HR Teams improve their cyber security recruitment process?

There are several key points HR teams need to address for hiring cyber security staff who understand the business needs and are able to make a positive contribution to improve cyber security from day-one on the job.

Education

One of the most challenging aspects facing HR is the understanding of the cyber security ecosystem and staying abreast of the latest market trends and developments. Without this information, HR may be challenged to understand the necessary skills.

Speaking to industry experts can be a valuable exercise in obtaining this information, but it comes at a price, as HR will have to invest considerable time. Efficient HR teams who demand the right hire, the first time, commonly outsource to niche industry recruitment experts who evaluate candidates informally and forward recommendations for next stage interviews.

Accessibility and Responsibility

HR must have full control over user access and work with senior members of the cyber security team to apportion relevant access. When hiring staff members for junior roles, it's critical that HR teams recognise where to set boundaries. It's vital to ensure new hires are genuine candidates and not trying to socially engineer themselves into the role for nefarious reasons - typically to cause damage from within the business.

UNFORTUNATELY IT'S NOT ALWAYS EASY TO DIFFERENTIATE BETWEEN ENTHUSIASM AND AN ULTERIOR MOTIVE WHEN EVALUATING INFO-SEC HIRES.

Understanding Business Goals

The best candidates for cyber security roles are able to resonate effectively with your company brand and your defined cyber security objectives.

If you can successfully tell your story to a potential hire, you are in a strong position as you can challenge them to demonstrate they have the relevant skills, attributes and mindset to be successful in that role.

Developing, or Outsourcing Technical Knowledge

Although HR staff usually have a basic understanding of the need for cyber security, they often lack comprehension of the more technical aspects. These need to be handled by external recruitment specialists that have the breadth of knowledge required to ensure the right candidate is identified.

The Way Forward for HR?

Historically cyber security was not viewed as a concern for HR teams.

WITH THE CHANGE IN APPROACH, HR HAS BEGUN TO VIEW CYBER SECURITY RECRUITMENT FROM A LEGAL AND OPERATIONAL PERSPECTIVE.

The hard-nosed approach to fill the position as quickly as possible proves detrimental as far as cyber security is concerned – with younger candidates often overlooked due to a perceived lack of experience. This means companies miss out on their fresh, innovative ideas, not to mention their passion and drive to learn new skills and techniques to help the business grow.

If you're in need of cyber security professionals and need the right candidate the first time, Via Resource are cyber security recruitment specialists. Since 2008 we've been doing just one thing: placing cyber security candidates.

Contact us today and see why our cyber security recruitment services are trusted by FTSE 100 companies and UK Government Departments.

If you are a CISO and you want to find out how to best project the needs of your cyber security team in the boardroom, download our specialist whitepaper here.

If you want to read more, discover what problems the retail industry are encountering with cyber security due to digital transformation here, or explore how the Internet of Things (IoT) is changing cyber security forever.