maxwellbond

CYBER SECURITY IN 2020

WITH STEVEN JAGGER

Steven Jagger, founder of Maxwell Bond, explores the current cyber-security talent and recruitment landscape, and how businesses can still source, hire, and retain the top cyber talent despite the current skill-shortage.

www.maxwellbond.co.uk

THE CYBER TALENT & RECRUITMENT LANDSCAPE

maxwellbond

Supply vs. Demand

UK businesses faced one attack every 50 seconds between April and June 2019 alone.

Businesses are investing heavily in cyber, but the talent pool is limited as it is still maturing, and the demand for these skills far outweigh the supply for the next few years.

More than half of businesses...
have a "basic technical cyber-security skills gap"

51% of businesses...
are not confident in carrying out a cyber-security risk assessment

47 % of businesse
lacked confidence in developi rity policies

3 in 5 businesse
are not confident in their re
complex cyber-security on testing
or performing forensic

Statistics from: Gov.UK, Forbes, pwc, Centre for Greater Manchester

MAXWELL BOND IS LOCATED IN THE HEART OF MANCHESTER, WHICH IS QUICKLY BECOMING THE LARGEST AND MOST INNOVATIVE TECH HUB OUTSIDE OF LONDON.

Greater Manchester is home to a fast-paced, fast-growing £5bn digital ecosystem, which includes more than 10,000 digital and creative businesses and employs over 85,000 staff.

Businesses recently joining Manchester include Amazon, GCHQ, Microsoft, Google, Autotrader, MoneySupermarket & Freshfields. With so much to offer, it is likely that big, tech-driven companies will continue to migrate to Manchester for many years to come!

SUPPLY VS. DEMAND

THE DEMAND FOR CYBER SKILLS WILL LIKELY OUTWEIGH THE SUPPLY UNTIL AT LEAST 2021.

UK businesses faced one attack every 50 seconds between April and June 2019 alone.

Businesses are investing heavily in cyber, but the talent pool is limited as it is still maturing, and the demand for these skills will far outweigh the supply for the next few years, making it difficult for businesses to effectively implement cyber-security solutions.

This limited talent pool has led to over 50% of businesses confessing a basic cyber-skill gap within their company. 51% of businesses are not even confident in carrying out a cyber security risk assessment, and 47% of businesses would be unsure as to how to implement policies in response to a risk assessment. This is leaving businesses exposed and vulnerable to cyber-threats.

With 3 in 5 businesses incapable of conducting more complex cyber-security tasks such as penetration testing or performing forensic analysis of their own data, there is a serious need for cyber talent within businesses.

Without effective cyber-security personnel, businesses are unable to implement and maintain technology and processes that counter cyber-threats. This leaves financial and other sensitive information vulnerable to theft, extortion, or manipulation, which could lead to significant financial or reputational damage.

Businesses must find a way to circumvent the lack of supply, and find alternative methods to recruiting and hiring the top cyber talent available.

THE RECRUITMENT PROBLEM

THE LIMITED TALENT POOL ISN'T THE ONLY REASON BUSINESSES ARE STRUGGLING TO HIRE TOP CYBER TALENT. FROM THE GRASSROOTS LEVEL, UNDERFUNDED 'ALTERNATIVE EDUCATION' PATHS, AND STUBBORN PROCESSES FOR CYBER-SECURITY SOLUTIONS CUT THE FLOW OF CYBER-SECURITY TALENT FROM THE GET-GO. THIS, ALONGSIDE COUNTER-PRODUCTIVE RECRUITMENT PROCESS ADOPTED BY MANY COMPANIES IS CONTRIBUTING TO THE SKILLS GAP IN BUSINESSES.

Recruitment problems include:

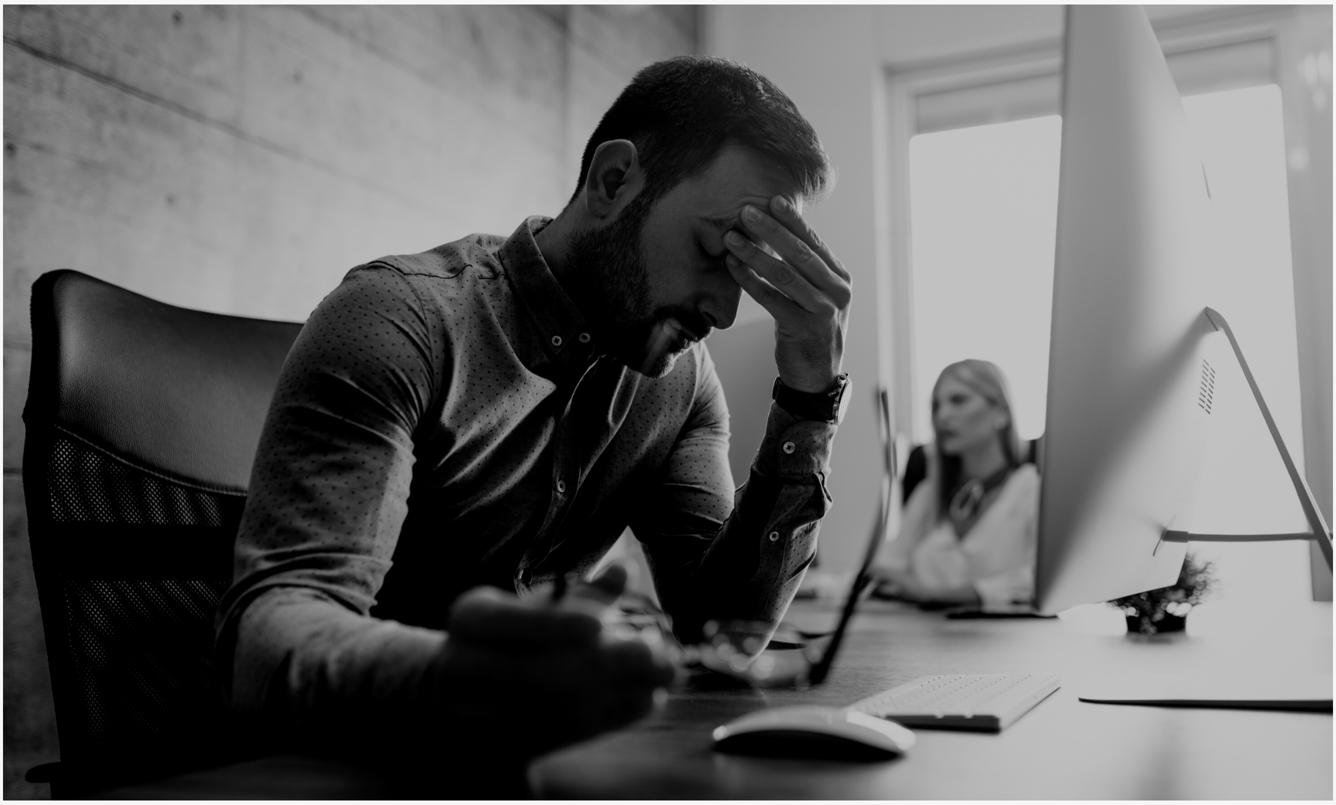
1. Over-generalisation of job specifications and simply adding cyber-security as part of general IT roles is problematic. Companies should be hiring cyber-specific talent for these roles.

2. Lack of specialist knowledge of cyber-security, and the associated threats and terminology, in HR teams means they cannot fully understand cyber-security requirements, which can often lead to poor and inadequate hires.

3. Poor communication throughout the supply chain. Typically what happens is, a cyber-security specialist role comes live and is then passed on to talent/HR teams but not fed properly through to the recruitment channels, meaning that traction, engagement, and simple solutions are often missed.

IMPACTS OF POOR RECRUITMENT

POOR RECRUITMENT IS COSTLY IN TIME AND MONEY, AND LEAVES YOUR BUSINESS BACK AT SQUARE ONE.



Poor recruitment processes lead to lengthy hiring times which is costly in time, money, and resources. They also lead to inadequate hires resulting in a high staff turnover and a loss of productivity. A high staff turnover can also be damaging to reputation and have a negative impact on company culture and staff morale. This whole process becomes drawn out and costly, when you account for recruitment costs, training costs, lost operational productivity, re-hiring, and retraining. Whilst all this is happening, your company remains at risk from cyber-threats.

DID YOU KNOW A POOR HIRE, ON AN AVERAGE ANNUAL SALARY OF £52.5K WILL COST YOUR BUSINESS APPROXIMATELY £163,018, WHICH IS 3X AS MUCH AS THE INITIAL HIRE!

HIRING RIGHT THE FIRST TIME, EVERYTIME

It is fundamental to get your hiring right the first time, every time, so that you can stay ahead of emerging cyber threats. Your ability to source and retain the top industry talent is also key to maintaining effective cyber-security processes, protocols, and technologies. As a business hiring for cyber-security there are three main areas you should be focusing on.

3 KEY AREAS YOU SHOULD FOCUS ON

- **Define your objectives and gain feedback** from experts who will be able to help you recruit right the first time.
- **Get your story and candidate journey right.** The days of 'the candidate should want to join us' are over, or never began in cyber security. You need to sell your company to the candidate.
- **Ensure your process works** and is communicated effectively throughout the supply chain, to avoid missing great opportunities!