

Demand for Cybersecurity Talent soars amid attacks on high street retailers

11 months ago



In the wake of recent cyberattacks targeting popular high-street retailers, [Robert Walters Market Intelligence](#) team releases data on the current state of the cybersecurity hiring market. Including key skills, top employers and sectors with the highest vacancies.

Cybersecurity Vacancies on the Rise

Cybersecurity skills have consistently ranked in the top five in-demand skills across professional services for several years now. In the UK alone, there are around 17,000 live cybersecurity vacancies at any one time - with estimates projecting vacancies to grow by around +10-12% each year.

Most In-Demand Cybersecurity Skillsets:

As cybersecurity threats become increasingly sophisticated and substantial in scale, the need for cybersecurity specialists has intensified across all sectors. This rapid evolution means that professionals often struggle to keep pace with necessary skill advancements. Key skills in current high demand include:

- Cloud Security Engineers
- Security Operations (SOC) Analysts
- Penetration Testers & Ethical Hackers
- Cyber Risk & Compliance Specialists
- AI & Threat Intelligence Analysts

Top 5 sectors with the highest levels of cybersecurity vacancies (% of all vacancies):

1. Finance & Banking - 20%
2. Public Sector & Defence - 18%
3. Technology & Digital Services - 16%
4. Healthcare & Life Sciences - 12%
5. Retail & E-commerce - 10%

Top 10 Employers

Large, multinational banks and financial institutions, as well as government departments make up cybersecurity's top employers.

Joined in the ranks by retail and e-commerce companies, who currently command 10% of all vacancies. However, this is expected to grow over the coming months as the retail sector responds to the recent cyberattacks by strengthening their preventative cybersecurity capacities.

Phill Brown, Global Head of Market Intelligence at Robert Walters comments: "Retailers have heavily invested in recent years to hire professionals who can assess their system security and identify vulnerabilities. Penetration testing and ethical hacking are among the most sought-after skills today.

"The recent cyberattack, on some of our most well-known high street retailers, carries with it short-term disruption, but also the very real risk of long-term damage to trusted brand image and reputation. The scale and impact of these attacks is often extensive and takes considerable time and cost to rectify. This underscores the urgent need for businesses to prioritise cybersecurity hiring.

"Many retailers rank among the top employers of cybersecurity talent and consistently allocate substantial resources towards enhancing their security systems. However, following these high-profile attacks, we anticipate that budgets will be stretched even further this year.

"Indeed, regardless of this investment, efforts must be ongoing and companies who neglect the hiring and upskilling of cybersecurity staff, risk lost profits, damaged reputations, diminished consumer trust, and vulnerability to future security breaches.

"Companies will not only need to hire or contract cybersecurity experts to address the current issue, but they will also require additional specialists to rebuild their IT systems and advise on stronger security measures. This process will be both costly and time-consuming.

"This latest situation serves as a cautionary tale for all businesses. By hiring the right professionals and consistently investing in their upskilling from the beginning, companies can better protect themselves against ever-evolving cyber threats."