Mind the Gap… But Also Your CoV – The Hidden Costs of (Cybersecurity) Vacancies

Written by Joshua Bucheli, Talent Community & Business Development Manager at cyberunity AG

With a shortage of 4.8 million security specialists as of 2024, the cybersecurity workforce gap represents a persistent and growing challenge that threatens to undermine even the most robust security strategies. This gap, characterised by long-standing vacancies in critical security positions, poses a significant risk to businesses and institutions worldwide. While these security-related risks are beginning to gain recognition in corporate circles, the underlying financial costs of long-term vacancies are still, all too often, overlooked or underestimated.

This situation raises critical questions about organisational awareness and priorities. Are businesses truly cognizant of the comprehensive costs associated with their vacancies in general and in cybersecurity in particular? Are they even aware of Cost of Vacancy (CoV) as a relevant metric? And, perhaps more importantly, is there a genuine willingness to confront this uncomfortable reality, or is the illusion of short-term savings providing a false sense of comfort that is just too good to pass up on?

Cost of Vacancy (CoV) – The Underappreciated Metric

HR costs (employer branding, job advertisements, conducting interviews, active sourcing and potential third-party recruiting fees) are not the only expenses that must be considered when undertaking the search for a new employee. Indeed, they represent only a fraction of the true underlying costs of deciding to look for a new team member.

Cost of Vacancy (CoV) is a vital yet often underappreciated corporate metric that quantifies the financial impact of leaving a position unfilled. It encompasses both direct costs, such as lost productivity and recruitment expenses, and indirect costs, like diminished team morale, employee burnout, missed business opportunities, and, in the case of cybersecurity, exacerbated vulnerabilities.

CoV can be calculated using the following formula: (**Annual Salary ÷ Workdays per Year**) × a **Factor Multiplier** depending on the qualitative impact of a missing worker on business outcomes × the number of (work)days it takes to fill the vacancy (aka the **TTF**). By providing a tangible estimation of the financial loss incurred for each day a role remains empty, businesses can better understand the urgency of optimising hiring strategies, refining resource allocation, and filling roles efficiently.

The False Economy of Empty Chairs
Thanks to the cybersecurity workforce gap, the process of filling roles has become increasingly protracted and complex. Entry-level security positions typically require three to six months to fill, professional roles often remain vacant for over half a year, and leadership positions can take up to a year to staff.

When faced with difficult to fill positions, organisations may be tempted to look for a silver lining – to perceive long-term vacancies as a temporary reprieve for corporate budgets. After all, for every month that a position remains unfilled, there is a salary that does not need to be paid out. While intuitively plausible, the reality is that significant revenue losses and operational inefficiencies can ensue from a vacancy.

Companies don't create positions frivolously and they definitely don't hire for the fun of it. When a new role is established, it is with the expectation that the employee's contributions will significantly outweigh their compensation as well as any associated social contributions and overheads (insurance, pension etc.). Otherwise, it would make no fiscal sense to establish the vacancy in the first place. When a position remains unfilled, organisations miss out on this anticipated value at a cost that exceeds any unspent salary payments – hence why the annual salary is a factor when calculating CoV.

The concept is most easily demonstrated in the context of sales: Assuming a salary of CHF 100'000 and overheads of CHF 30'000, one could theoretically save CHF 130'000 in salary expenses per year if the position remains unfilled. However, if said sales manager was expected to reach a sales target of CHF 250'000 a year, then it would actually be more accurate to say that the employer has lost out on CHF 120'000 (250'000-130'000) in expected revenue – CHF 10'000 for every month that the vacancy remains unfilled!

The same principle applies (albeit less intuitively) for non-revenue-generating positions: Businesses are ultimately concerned with their bottom line – as they should be – and they cannot afford to hire employees for more money than they seek to gain in expected value, however tangible or intangible. In sales this value comes directly in the form of revenue, in legal roles it comes in the form of ensured compliance and prevented legal fines, in IT it may manifest as operational continuity, and in HR it is the very ability to attract, hire, and retain the talent that keeps the business running.

Hidden Costs – Productivity and Opportunity
While central to CoV calculations, the true costs of a vacancy extend well beyond the visible line items of HR costs, salary, and anticipated value. They also include various hidden costs that contribute to a cumulative financial and security burden which many organisations fail to fully appreciate.

First of all, productivity suffers as tasks go unattended or as existing team members struggle to cover the responsibilities of unfilled positions (a leading cause of burnout). This causes overall efficiency to suffer, and can even give rise to further vacancies, worsening the problem.

Then there are opportunity costs to consider – opportunities for innovation, growth, and new business that may be missed without the specialised skills and insights that new hires would bring. Crucial market trends can go unnoticed, warm leads can turn cold, emerging technologies may not be capitalised on, and ground may be lost to more agile competitors. Moreover, the absence of fresh perspectives and diverse skillsets can stifle creativity and problem-solving within teams, further hampering an organisation's ability to adapt and thrive.

Vulnerabilities and Risk
All of what has been said so far is true for any vacancy. In the cybersecurity sector, however, the costs don't end there. In addition to untapped anticipated value, HR costs, opportunity- and productivity costs, vacancies in the security sector also introduce additional layers of risk. Each day without an appropriate complement of security specialists is a day when an organisation's defences may be compromised.

As the potential for cyber incidents increases, so too does the likelihood that such incidents will have more severe, far-reaching consequences. With data breaches costing companies an average of $4.88 million and ransomware demands averaging $115'000 the stakes of an extended vacancy in cybersecurity speak for themselves.

Honesty is the Best Policy – The Factor Multiplier
While salary is used as a proxy for expected value in CoV calculations, costs associated with potential incidents, opportunity-, and productivity-costs are less easily quantified.

This is where the factor multiplier mentioned in the CoV formula comes into play: where expected impacts of a missing employee are low, the factor can be set to 1 or 2; where they are high, a factor of 3, 4 or more may be more appropriate (most CoV calculators recommend a factor multiplier of 3).

Strictly speaking, a factor multiplier of 1 is only appropriate in CoV calculations where an organisation is expecting only to recoup its investment when hiring a new employee and nothing more – a scenario that makes little economic sense and that should present only rarely.

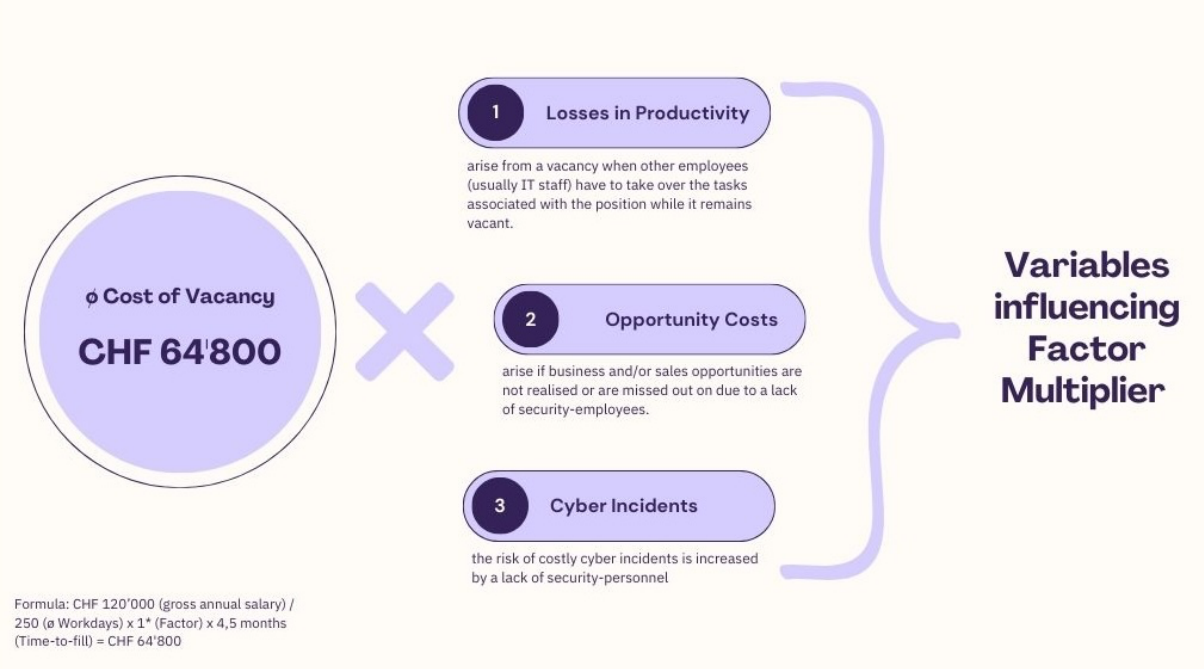

Figure 1: CoV for a Mid-Career Security Engineer assuming a factor multiplier of 1

As seen in Figure 1, the CoV for a mid-career security engineer position is already considerable when taking just a factor of 1. Factor in security's role in business continuity… the financial impacts of potential incidents... the opportunity- and productivity-costs of a security vacancy and 'considerable' quickly becomes an understatement:

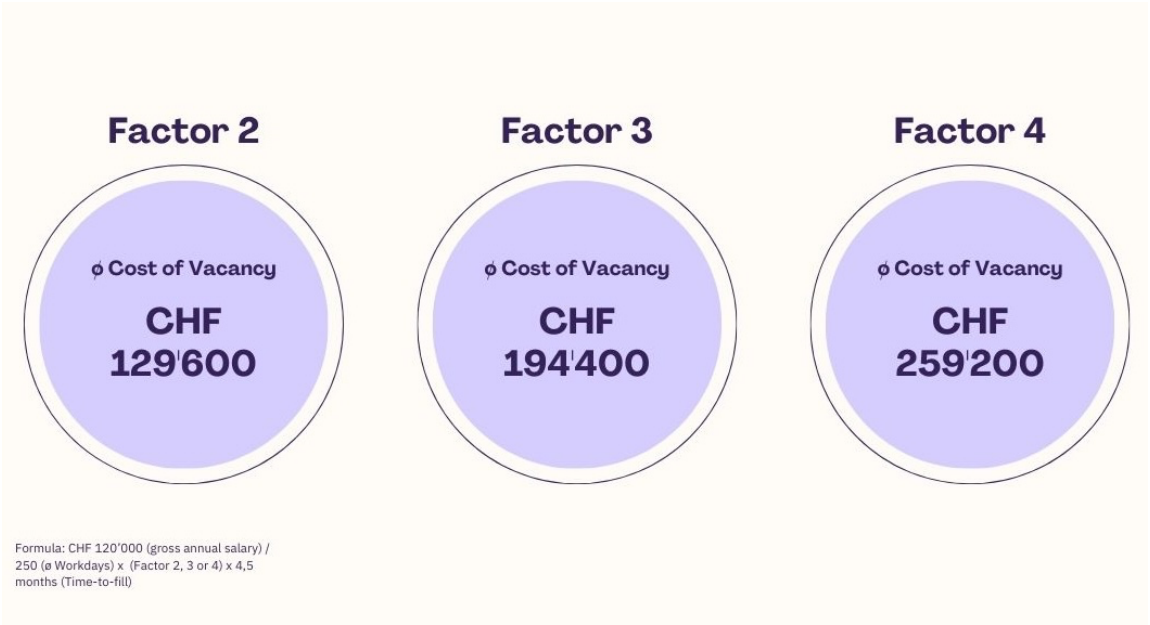

Figure 2: CoV for a Mid-Career Security Engineer assuming factor multipliers of 2, 3, and 4

Adopting an honest and comprehensive approach to the factor multiplier allows companies to better visualise the urgency of filling their positions and to better justify the resources needed for effective recruitment. At the end of the day, it's up to each company to consider its individual priorities and circumstances when determining how prominently a cybersecurity vacancy should figure into their calculations – but considering the potential impacts, it seems safe to say that a factor of 1 is missing the mark.

Shifting the Mindset – from Complacence to Cognizance

As summed up by Dr. Annabella Bassler, CFO at Ringier, "[cybersecurity] vacancies don't just leave gaps in teams—they create cracks in an organisation's entire foundation. The hidden costs of unfilled roles extend far beyond salaries, impacting security resilience, productivity, and even business growth. Recognising the true Cost of Vacancy isn't just an HR concern; it's a strategic imperative."

Ultimately, every vacancy demands urgent attention and action, and the time has come for businesses to shift their mindset and recognise that an empty chair represents more than just unspent salary (regardless of how intuitive or reassuring this perspective may be).

Organisations must become cognizant of the true cost of inaction, the substantial drain on resources, and the compounding risks associated with prolonged vacancies (especially in critical cybersecurity roles). Understanding and applying the concept of CoV facilitates this mindset shift, allowing businesses to gain a more comprehensive view of the true impact of vacancies on their operations, security posture, and bottom lines. As average time-to-hire balloons in the cybersecurity field, organisations can simply no longer afford to adopt a complacent attitude towards vacancies, whether they realise it or not.

This mindset-shift is not just about filling chairs - it's a call to action for leadership to prioritise cybersecurity staffing as a critical business imperative and to transition from viewing cybersecurity as a cost centre and a mere operational concern to seeing it as a profit center – but this is a matter for another day (see our article on cybersecurity as a corporate USP or the NTNU's publication on business focused cybersecurity for more info).

Calculate your CoV today!