Beyond Defense: Know Your Business Value

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

Traditionally, industry leaders and boards have approached security primarily as a technical safeguard – a necessary cost to assure business continuity i.e., a pain. Slowly but surely, a more constructive paradigm is taking shape: cybersecurity as a strategic business enabler – an investment with a legitimate ROI, not merely a defensive expense.

For the time being, this mindset shift has yet to reach critical mass, and mostly occurs top-down in board rooms and management circles. But the greatest potential remains untapped and presents myriad benefits that would serve all parties involved: a grassroots approach by which cybersecurity specialists themselves understand the business-value of their field (and their skills).

Why the Mindset Shift Matters

Traditionally, cybersecurity teams found themselves first in line for budget cuts and last in line for strategic recognition, with security initiatives seen as impediments to speed and innovation. This has resulted in a security landscape that is reactive in posture and measured by incidents prevented rather than proactive and measured by business outcomes.

Today, CEOs and decision-makers are waking up to the competitive advantage that security can bring: it drives customer trust, improves regulatory compliance, and can even directly influence revenue (most obviously in the case of security service providers). According to a survey by Gartner as many as 85% of CEOs now consider cybersecurity a critical strategic growth driver, integrating it into core business objectives. The more this perspective takes hold, the better the chances of proper investment in what is a notoriously underfunded field with equally notorious stakes.

Empowering Early-Career Specialists

While executive buy-in is important, a grassroots movement advocating for cybersecurity as a worthwhile investment rather than a cost center may hold the greatest transformative potential. When security specialists en masse understand not only how to do their work, but also how it influences a business's bottom line, recognising that their contributions enable growth and support innovation, they become powerful agents of this shift.

Early-career security specialists especially face a paradoxical and frustrating position: cybersecurity talent is in high demand, yet genuine entry points into the field remain scarce and fiercely competitive. This makes it even more important for juniors to stand out by understanding and clearly communicating the business value of their work. Instead of relying solely on degrees, labs, or certifications, they can answer the implicit question "Why should we hire you?" with a concrete value proposition: "Because I can help you protect and generate revenue, reduce risk, and ultimately save or earn measurable amounts of money through smarter security decisions."

Security professionals across the board have a vested interest in making this value visible, as it directly influences their salary, career progression, and bargaining power over time. By actively tracking, documenting, and communicating the business outcomes of their work (accelerated product launches, measurable reductions in fraud, optimised business continuity, or streamlined compliance and fines avoided) they help shift the industry narrative, raise overall cyber resilience, and continuously differentiate themselves in the job market. Communicating the value of your work in clear, business-focused terms is a career-long asset that will never work against you.

This bottom-up approach creates a sustainable culture shift, embedding business-focused thinking into everyday practice and is far more effective than relying solely on top-down pressure from leadership.

Communicating Business Impact in Your CV

One of the most actionable ways to drive this paradigm shift is in the way security specialists present themselves. Rather than just listing technical achievements, candidates can gain an edge by framing their skills in a way that highlights direct or indirect business value.

Quantify where you can (small wins count too!) but do not exaggerate or invent numbers – even qualitative impact, like describing how your work helped a business unit achieve its goals, is far better than purely technical descriptions. It is easy to forget that, even for technical roles, not everyone involved in hiring or decision making is technically oriented, so clear business language becomes a differentiator.

In short, do not assume that because you are a security specialist applying for a security role, "security" is the only thing that matters. For many hiring managers, your technical skills are a means to an end: enabling more revenue, reducing risk, and supporting sustainable growth.

- Instead of "Implemented multi-factor authentication across enterprise systems," try: "Enabled CHF 1.2M in new business by meeting client security requirements while maintaining 99.8% user productivity."

- Replace “Performed vulnerability scanning and remediation” with something like: “Accelerated product launch by 3 weeks by streamlining the vulnerability management process.”
- Rather than “Led security awareness training for 500 employees,” consider: “Reduced phishing susceptibility by 62% through the development of innovative security awareness programs, preventing CHF 85K in annual fraud losses.”

It is important to acknowledge that identifying clear business value in day-to-day security work is not always straightforward, especially early in a career. Many seasoned leaders still struggle to quantify cybersecurity’s impact beyond risk reduction, so it is entirely normal not to have a long list of polished examples from the start.

What matters most is becoming aware of this perspective as early as possible, deliberately thinking about how your activities support revenue, resilience, or efficiency, and gradually gathering evidence as you go. Treat it as an ongoing practice: keep notes on small wins, follow how others articulate security’s business impact, and periodically translate your technical contributions into business language. Over time, this mindset will compound, making it far easier to demonstrate your value convincingly when opportunities arise.

- Awareness: Recognise, document and track business impact in daily security work.
- Alignment: Directly connect technical achievements to business objectives and KPIs.
- Articulation: Use clear language to convey impact to non-technical stakeholders.
- Amplification: Share success stories and value creation examples within teams and across networks and organisations.

Take the Next Step

Revisit your CV and identify where you can reframe technical tasks as business contributions. Document a specific example of where your security work led or contributed to real business growth or operational efficiency. Have a conversation with a business stakeholder about how your efforts help them succeed. For further support, our community offers value-focused sample CVs, interview prep guides, and regular industry updates – all designed to help you stand out and support the ongoing redefinition of cybersecurity as a business enabler.

Reach out to info@cyberunity.io if you’re interested in any of the aforementioned resources ☺