SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

The Cyber Storm: Addressing Cyber Security Hiring Challenges in the Benelux

sgi
#DiscoverYourPotential

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

Contents

sgi
#DiscoverYourPotential

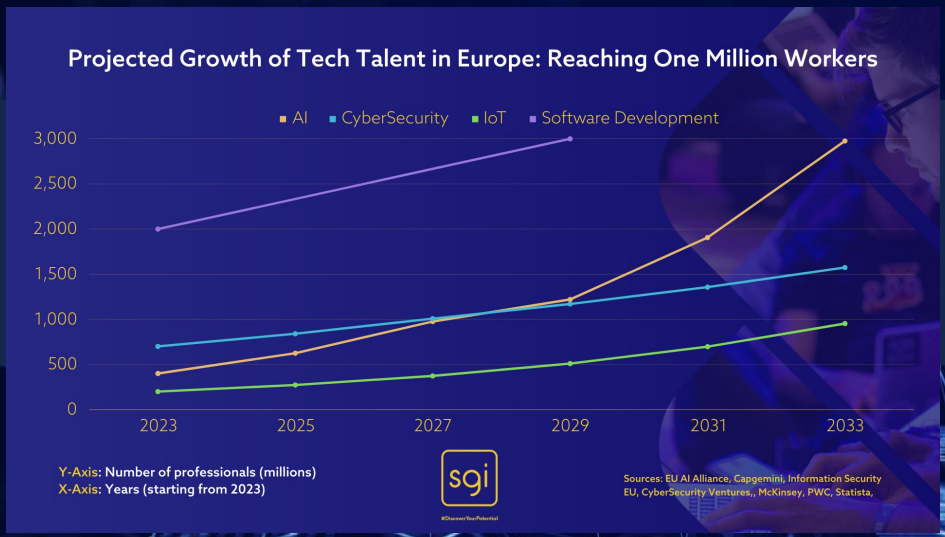
SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

Executive Summary

Following the global pandemic, many tech firms were forced to reduce their workforces as they looked to cut costs. This situation created a perfect storm for cyber criminals, as businesses streamlined their tech departments, often removing important IT security roles.

Cost cutting is not the only major challenge affecting tech companies, there is also a global talent shortage of Cyber Security professionals.

The pandemic accelerated the adoption of digital technologies, which presented more opportunities for cyberattacks on connected devices. While businesses with larger recruitment budgets have been able to invest in recruiting Cyber Security professionals, the shortage of workers with the relevant qualifications has posed a problem across all industries.



sgi
#DiscoverYourPotential

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

The Benelux Region: A Hub for Digital Innovation and Connectivity

The Benelux region, comprising Belgium, the Netherlands and Luxembourg is one of the world's most competitive economic regions. The area attracts a high volume of foreign investors and the strategic location as a gateway to Europe provides the Benelux region with an advantage for industries such as transport and logistics.

Across the Benelux region, digitalisation has been identified as one of its top priorities, with strong investment into the development of government systems and initiatives to drive digital transformation. Due to this investment, the Benelux region has a more advanced digital infrastructure than many other countries.

The Netherlands has a very strong internet economy, hosting many data centres, while Luxembourg is a hub for the insurance industry. With advanced digital infrastructure and a large volume of technologically-centric businesses, the Benelux region has emerged as a prime target for cyberattacks.

2 Million

SMEs

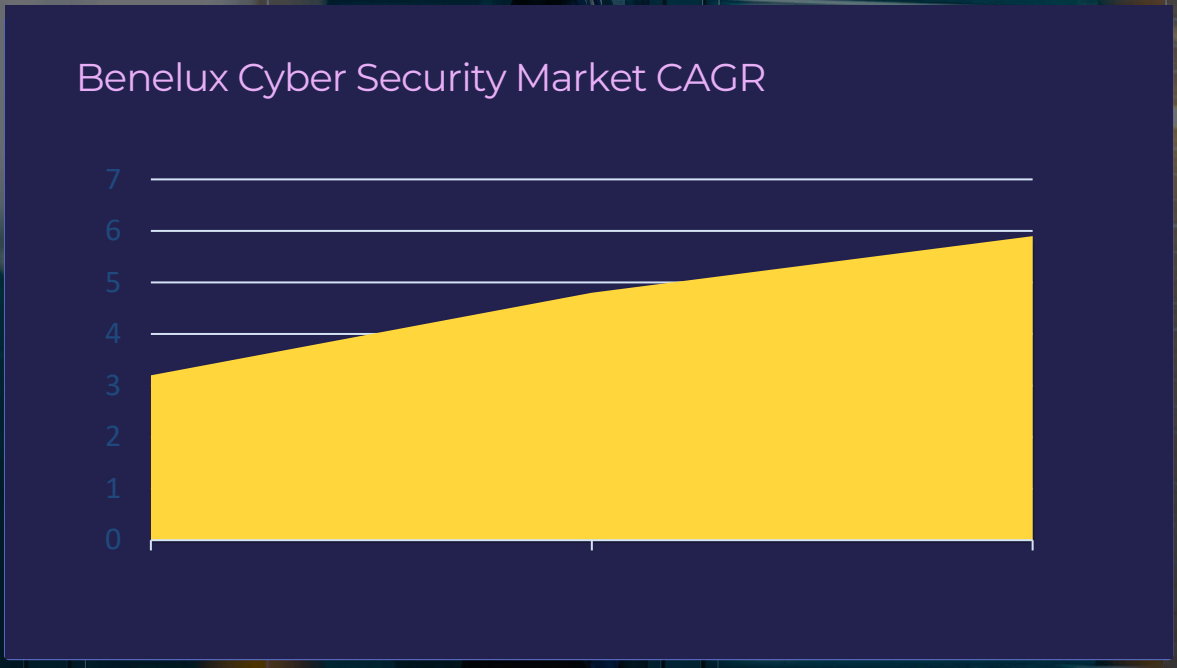
In **2022,** there were approximately **2 million SMEs** in Benelux[3], with the Netherlands **possessing around 1.28 million** of businesses operating in non-financial sectors.

In the Global Finance 2023 Ranking of the World's Most Technologically Advanced Countries and Territories report[4], the **Netherlands** was **ranked 8th**, **Belgium** was **ranked 13th** and **Luxembourg ranked 30th.**

sgi
#DiscoverYourPotential

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

The Unique Cyber Security Challenges of the Benelux Region



The Benelux Cyber Security market size is estimated at USD 4.04 billion[3] in 2024, with forecasted growth to USD 5.90 billion by 2029. The steep increase in the number of SMEs in the region is a key driver in the Cyber Security market for Benelux.

SMEs largely rely on cloud systems and generally focus their time on core skills rather than security infrastructure, which makes them an easier target for cyberattacks. Cloud adoption supports the modern working from home models, with IT provision now shifted from being on-premises to outside of a company's borders.

High levels of digital integration in these countries place them at a higher risk of cyber threats. The regulations and policies of the local governments are additional drivers of the Cyber Security market, with the Benelux Union collaborating to develop strategies to strengthen cyber resilience in the countries.

sgi
#DiscoverYourPotential

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

The Threat Landscape

One of the biggest problems that businesses are facing is the pace of evolution of cyber threats. Digital transformation happens at great speed and new cyber threats emerge on a regular basis, targeting weaknesses in new technology solutions. Digital innovations such as AI provide some solutions to improve Cyber Security, but AI can also be used by cyber criminals to identify security weaknesses.

These are some of the most prominent cyber threats businesses currently face:

Advanced persistent threats (APTs)

Advanced Persistent Threats (APTs) use sophisticated hacking techniques to access and persist within a system for an extended period. Typically targeting high-value businesses, these attacks involve stealing data over an extended timeframe. APTs pose a threat not only to large enterprises but also to SMEs in the supply chain. Smaller businesses, with less advanced cybersecurity, can serve as gateways for attackers to access larger organizations with more robust security frameworks.

Ransomware attacks

As of 2023, ransomware attacks have impacted over 72% of global businesses (Statista). These attacks involve locking a victim's data or device and demanding a ransom for its release. The attacker encrypts the data and requests payment in exchange for the encryption key. SMEs, local authorities, and public health organizations are particularly targeted in Europe. An example is the recent ransomware attack on Creos Luxembourg, a gas and energy provider within the Encevo Group.

Data Breaches

Data breaches involve unauthorized individuals exposing confidential information. This cyber threat affects businesses of all sizes, targeting employees through phishing attacks, which exploit unwittingly clicked links to gain access to company systems and data. Weak passwords and malware are additional contributors to data breaches.

Emerging threats from cloud computing, IoT and mobile devices

The widespread adoption of cloud computing, mobile devices, and remote work has increased vulnerabilities for cyber attackers. Weaknesses in device security, internet connections, cloud deployment, and the expansion of IoT devices have contributed to a surge in cyberattacks.

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

The Impact of Cyber Security Challenges

Cyber Security challenges have a profound impact on businesses, from financial losses to long-term reputational damage. According to Statista reports[8], the average cost of all cyberattacks to European and North America firms in 2023 were:

#	Company Size	Description	USD
1.	Small	10-49 Employees	9.500
2.	Medium	50-249 Employees	10,700
3.	Large	250-999 Employees	24,800
4.	Enterprise	1000+ Employees	53,500

*cost per attack

Some of the biggest ransomware attacks such as WannaCry and ExPetr have resulted in financial losses of billions of dollars, hitting multiple companies at a time.

In addition to the costs associated with being victims of cyberattacks, businesses also suffer significant reputational damage and loss of customer trust.

The Impact of Cyber Security Challenges

These are three of the top priorities for the Cyber Security industry:

Protecting essential services

Many sophisticated cyberattacks target essential services such as healthcare systems, government services and e-commerce. Protecting these essential services has become a top priority and government organizations and businesses are investing more into the cybersecurity strategies for essential services

Safeguarding sensitive data

The European GDPR regulations have helped to strengthen the protection of sensitive data, but the processes and systems required to implement changes have provided challenges to many businesses. The consequence of a data breach can be a fine of up to €20 million if a company is found to have not taken adequate measures to protect sensitive data.

Ensuring economic prosperity

In competitive markets, having a robust cybersecurity strategy can give businesses an edge over their competitors. Consumer trust is a significant factor in ensuring economic prosperity and growing brands. Businesses that are able to share a high quality cybersecurity framework can also win more work tenders and impress prospective clients/customers.

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

A Comprehensive Approach to Cyber Security

These are the key elements of an effective Cyber Security strategy:

Investing in Cyber Security infrastructure

Despite the financial challenges presented by the global health pandemic, one area that businesses cannot afford to cut back on is their Cyber Security infrastructure.

Promoting effective threat intelligence sharing

Collaboration across organizations is integral in fighting cybercrime. Gathering and sharing threat intelligence helps to prevent copycat cyberattacks targeting similar businesses. Organizations can join cybersecurity communities and networks for their industry, such as ENISA (European Union Agency for Cyber Security).

Enhancing cybersecurity regulation and compliance

Complying with Cyber Security regulations such as the EU Cyber Security Act is another key element of a robust and effective cybersecurity strategy. Compliance with all the required regulations is heavily reliant on having skilled and knowledgeable Cyber Security managers and additional senior Cyber Security focused roles.

Fostering international Cyber Security cooperation

ENISA has been formed to help foster international Cyber Security cooperation, including representatives from the European Parliament, the European Commission and election authorities as well as Cyber Security authorities. This collaboration enhances cyber resilience on an international landscape by preparing for cyberattack incidents and working together on developing best practices for cybercrime strategies.


SOURCE
TECHNOLOGY
DISCOVER TECH POTENTIAL
Cyber Security Hiring Challenges
sgi
#DiscoverYourPotential

While the case for investing in Cyber Security is clear to businesses, there is a major barrier in developing a robust Cyber Security strategy - the Cyber Security talent gap. The demand for Cyber Security professionals far outnumbers the available experts in the sector.

The Growing Demand for Cyber Security professionals

As the threat landscape of Cyber Security continues to evolve at pace, with high stakes for businesses who are targeted, the demand for Cyber Security professionals is higher than ever. The shortage of Cyber Security experts leaves businesses vulnerable to a huge range of cyber threats, so an advanced Cyber Security hiring strategy is required to ensure businesses are protecting their assets and data.

20%

Employers across the Benelux experience extreme difficulty finding good talent.

Talent shortages leave employers without key roles across the business, so a hiring solution must be identified to protect businesses.

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

The Key Skills and Competencies Required for Cyber Security Professionals

Competent Cyber Security professionals should be able to demonstrate a combination of technical and soft skills such as:

#	Key Skills
1.	Understanding of network architectures, protocols and security measures.
2.	Ability to secure applications against vulnerabilities.
3.	Ability to resolve complex problems under high pressure.
4.	Knowledge of laws and regulations including GDPR, HIPAA and PCI-DSS.
5.	Experience of identifying, responding to and investigating cybersecurity incidents.
6.	Ability to conduct security audits to identify and implement security improvements.
7.	Knowledge of current cybersecurity trends and threats.
8.	Proficiency in installing antivirus and security software.
9.	Ability to analyze network data and system logs.

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

Strategies to address the Cyber Security talent gap

Offer competitive compensation and benefits

Increasing salaries and benefits for roles which are difficult to fill helps to attract a higher calibre of candidates.

Enhance training and development opportunities

Providing training opportunities for new and existing employees supports employees in acquiring cybersecurity qualifications and other professional development options.

Expand the recruitment pool

Use specialized platforms and online communities to find cybersecurity experts, create partnerships with universities and colleges and engage in cybersecurity conferences to establish connections within the industry.

Improve workplace diversity

Creating a more diverse and inclusive culture helps to expand the recruitment pool of people who will be interested in working for your company.

Try a different approach to recruitment

Taking a different approach to recruitment may help to identify high quality candidates with an alternative background. For example, consider candidates who are self-taught or who have come through a non-traditional education route but can demonstrate the required skills and competencies.

sgi
#DiscoverYourPotential

Our Meetup Community

Join a growing network of Cyber Security professionals exploring the future of Talent Acquisition across Cyber Security. On Cyber host a combination of webinars, live podcasts, in person meetups.

Join here

Our Podcast

Stay informed, connected, and inspired as we navigate the latest trends, insights, and innovations in the ever-changing world of Cyber Security talent through our podcast series.

Listen here

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

About Source Technology

We're Source Technology, an International Recruitment business specializing in Technology Recruitment. We operate across Europe in the UK, Nordics, Benelux, DACH regions, and the USA. We are the technology experts of Source Group International (SGI).

Our core purpose is to source exceptionally talented technology people for ambitious businesses, from SMEs to major multinational organizations.

We recruit on a contract, permanent, and retained search basis in the following market areas:

Areas of Expertise

- Data
- Cloud
- Engineering
- Cyber Security
- BA/PM

sgi
#DiscoverYourPotential

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

References

1. https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive#:~:text=In%20Europe%20only%2C%20the%20shortage,will%20soon%20reach%204%20million.
2. https://www.mordorintelligence.com/industry-reports/benelux-cybersecurity-market
3. https://gfmag.com/data/non-economic-data/most-advanced-countries-in-the-world/
4. https://english.ncsc.nl/publications/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028
5. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/#:~:text=As%20of%202023%2C%20over%2072,far%20the%20highest%20figure%20reported.
6. https://cybernews.com/news/ransomware-gang-says-it-hit-luxembourgs-energy-supplier/
7. https://www.statista.com/statistics/1008112/european-north-american-firms-cyberattack-cost/
8. https://www.manpowergroup.be/2023/03/14/job-market-under-pressure-in-belgium-recruitment-intentions-down-and-talent-shortages-up/
9. https://ceoworld.biz/2023/10/05/report-best-countries-for-cyber-security-professionals-2023-average-salary/#:~:text=Switzerland%20offers%20the%20highest%20salaries,for%20professionals%20in%20the%20field.&text=Luxembourg%20is%20renowned%20for%20its,its%20unwavering%20commitment%20to%20cybersecurity

sgi
#DiscoverYourPotential

SOURCE TECHNOLOGY
DISCOVER TECH POTENTIAL

Connect With Us On LinkedIn

Check Out Our Website

Join Our Meetup Community

Listen To Our Podcast

Subscribe To Our Newsletter

sgi
#DiscoverYourPotential