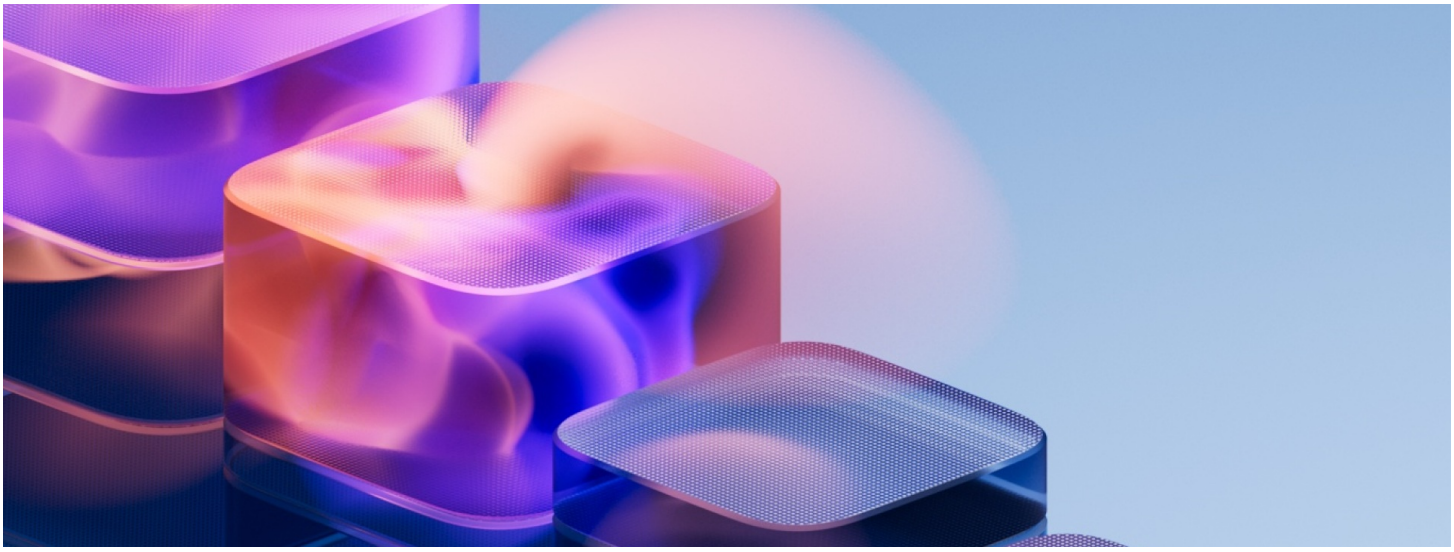
IBM NCEE News Room

Cost of a Data Breach in the Benelux Rises to an Average of 6.35 Million Euros

One in Four Malicious Data Breaches Now Enabled by AI



Amsterdam, July 30, 2026 — The average cost of a data breach in the Benelux**reached** 6.35 million euros, according to the 2026 IBM Cost of a Data Breach Report. This is an increase compared to the 6 million euros recorded in 2025 and 5.45 million euros in 2024. For comparison, this is significantly higher than the global average for data breaches, which stands at 4.99 million dollars.

One in four malicious data breaches in the Benelux (26%) was enabled by AI. These attacks, consisting primarily of deepfake impersonation and AI-assisted malware, are shifting the economic impact of data breaches. Cyberattacks are becoming faster and cheaper to execute, while detecting and containing breaches is becoming increasingly expensive.

Organizations in the Benelux that extensively deploy AI and automation within their security operations reduce data breach costs by an average of 1.64 million euros (costs of 5.45 million euros with extensive use versus 7.09 million euros for organizations not using AI/automation). Yet, more than one in four Benelux organizations (26%) has still not integrated these technologies into their security operations.

Advanced AI Threats Prompt Organizations to Act Sooner

Organizations are starting to take action based on future risks, rather than reacting only after an incident occurs. Additional global follow-up research by the Ponemon Institute shows that 85% of organizations worldwide plan to increase security spending after gaining insight into the advanced cyber capabilities of frontier AI. By comparison, in the standard Benelux study, only 68% of organizations indicated they wanted to increase security spending after actually experiencing a data breach.

At the same time, a gap remains in the areas where cybercriminals are evolving fastest. Although more than half of Benelux organizations (52%) deploy AI agents in their Security Operations Center (SOC), globally only 18% use these agents for vulnerability management. As a result, known vulnerabilities persist, while AI shortens the time cybercriminals need to exploit weak spots. Nearly three-quarters of organizations worldwide state that threats from frontier AI are prompting them to rethink how agents are deployed within their security operations.

“The report findings show that cybersecurity has become a business resilience issue, not just a technology issue. With the

average cost of a data breach in the Benelux now reaching €6.35 million, organizations need to move from reactive security to proactive risk management," said Marcell Schmidt, Country General Manager and Technology leader IBM Netherlands.*"The priority now is to shorten* the *delay between finding and fixing a breach by integrating remediation into development processes, securing identities during runtime, and resolving risks at the same speed at which attackers evolve."*

Critical Infrastructure at Greater Risk from AI-Driven Attacks

Most AI-driven attacks globally targeted critical infrastructure sectors (62%). Organizations in financial services and the energy sector were particularly hard hit worldwide, increasing the risk of broader disruption to essential systems.

Data breaches in the Benelux financial sector now cost an average of 7.90 million euros, while the Benelux communications sector (7.03 million euros) and the Benelux industrial sector (7.02 million euros) also sit well above the average. The concentration of attacks on these sectors increases the likelihood of cascading effects that could impact economies, supply chains, and essential services.

Other Key Findings

- **The weakest link of AI:** More than 20% of organizations worldwide experienced a data breach targeting AI models or AI applications. The most common global causes stemmed from vulnerabilities surrounding these systems, such as compromised APIs, applications, or plug-ins (27%) and misconfigured cloud environments affecting AI workloads (27%).
- **Encryption shortcomings persist as quantum risks grow:** Fundamental weaknesses in encryption and cryptographic management continue to expose organizations to risk, despite growing investments in quantum-safe security. Only 36% of Benelux organizations that experienced a data breach report encrypting sensitive data both at rest and in transit. However, 61% of Benelux organizations have formal controls in place to monitor secure cryptography and cryptographic objects.
- **Cybercriminals increasingly leverage reputation as leverage:** The number of ransomware incidents globally has risen compared to last year (39% versus 34%), with cybercriminals increasingly using AI to automate and scale attacks. While operational disruption still plays a role, cybercriminals worldwide are focusing more on high-impact extortion methods. The most common lever used globally is damaging brand reputation (41%), followed by exfiltrating employee data (35%) and intellectual property (31%).

The 2026 Cost of a Data Breach Report features a specific sample of 34 organizations for the Benelux. The overarching global study was conducted by the Ponemon Institute and is based on data breaches that occurred at 602 organizations worldwide between March 2025 and February 2026.

To supplement this research, the Ponemon Institute conducted a follow-up survey of these organizations in May 2026. A total of 456 organizations from the original study responded. Of these, 78% (or 356 organizations) were familiar with recent developments surrounding highly advanced frontier AI models, such as Mythos.

Download the full report here.

Additional Resources

- Register for the webinar.
- Schedule a briefing with IBM experts.

- Understand your AI Cyber Resilience.

Media Contact
Jasmina Premrl
jasmina.premrl@si.ibm.com
