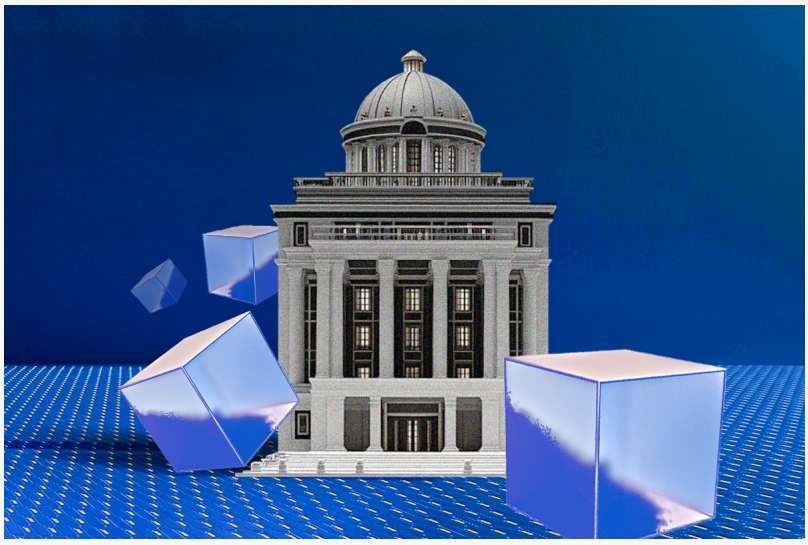
67% of EU governmental institutions score D or F for cybersecurity efforts

VILNIUS, VILNIUS, LITHUANIA, July 23, 2025 /EINPresswire.com/ -- As recently as 2025, the European Commission announced new initiatives to promote cyber resilience and introduced legislation aimed at strengthening cybersecurity across the European Union (EU). However, concerns about the overall readiness of EU institutions remain.



67% of EU governmental institutions score D or F for cybersecurity efforts

In 2022, the European Court of Auditors (ECA) issued a special report stating that the level of cybersecurity preparedness among European Union Institutions, Bodies, and Agencies (EUIBAs) was not proportionate to the threats they faced. The report urged the Commission to take action to improve cybersecurity across bodies and increase funding.

Despite these efforts, the latest data from the Business Digital Index, powered by Cybernews, shows that the European Union still struggles to secure its systems against cyberattacks. According to the analysis, 67% of the evaluated organizations scored a D or F — the lowest security grade assigned by the index. All institutions had experienced data breaches, and 85% of employees working for institutions with the lowest security grades reused passwords that had already been compromised.

Despite managing some of the most sensitive political, economic, and citizen-related data in Europe, nearly all institutions face major cybersecurity threats.

EU institutions struggle with basic cybersecurity hygiene

The Business Digital Index research team analyzed 75 EU governmental institutions' websites and evaluated their cybersecurity posture.

In the report of the index, which grades worldwide organizations based on their online security measures, 33% of the 75 governmental bodies were rated with a C score, which represents a below-average security level. Meanwhile, 32% of institutions were categorized as high-risk with a D score, and 35% received an F score, falling into the critical risk category. None of the institutions achieved an A or B score.

The average score among EUIBA stood at 71 out of 100. According to the index methodology, a score within the 70–79 range places an organization in the high-risk category, meaning that, despite some foundational security measures, the organization remains significantly vulnerable to cyberattacks.

The current cybersecurity posture of EU organizations is deeply concerning and shouldn't be taken lightly. Poor results should serve as a wake-up call for institutions to take immediate action and improve their systems. The longer vulnerabilities persist, the greater the risk of sensitive institutional and personal data being stolen, leaked, or misused.

46% of all F-rated entities had suffered a recent data breach

Institutions with the lowest cybersecurity scores are the ones getting hit hardest. 96% of F-rated and 92% of D-rated institutions had experienced at least one data breach, compared to just 36% of C-rated ones. Nearly half (46%) of all F-rated entities in the dataset had suffered a recent data breach. D-rated organizations weren’t far behind with 17%. Meanwhile, not a single breach was reported among C-rated institutions — a clear indicator that weak hygiene leads to real-world consequences.

A major behavioral red flag is password reuse. Among F-rated organizations, 85% of employees were found to reuse credentials that had already been leaked in previous breaches. At the D level, that figure was 71%. In C-rated organizations, only 8% of staff reused breached passwords. This suggests that repeated breaches in low-scoring organizations are not just possible — they’re predictable outcomes of ongoing negligence.

These findings align with high-profile real-world incidents. In 2024, the European Parliament disclosed a breach of its PEOPLE recruitment platform that exposed the personal data of more than 8,000 current and former employees. The breach went unnoticed for months and compromised documents such as ID cards, residence documents, and marriage certificates — all sensitive enough to enable identity theft or blackmail.

Reusing passwords after a data breach increases the risk to personal and organizational security. As this research revealed, the issue is persistent but also preventable. It signals an urgent need to educate employees about password hygiene and the implications of reusing the same credentials.

Low-scoring institutions face widespread technical vulnerabilities

The data shows a direct correlation between cybersecurity scores and critical system-level weaknesses. SSL/TLS configuration issues were identified in 100% of F-rated institutions, 92% of D-rated, and 100% of C-rated ones. These vulnerabilities leave systems exposed to man-in-the-middle attacks and weaken secure communication protocols.

System hosting vulnerabilities were similarly prevalent. 92% of D-rated and F-rated institutions had insecure hosting environments, while the issue persisted across all C-rated institutions as well. Domains vulnerable to email spoofing were found in every C-rated organization and in 96% of D-rated and F-rated ones, allowing for potentially dangerous impersonation attempts.

Exposed corporate credentials were discovered in 96% of F-rated and 83% of D-rated institutions. In contrast, only 12% of C-rated organizations had leaked credentials, underscoring the gap in basic security hygiene between lower- and mid-performing organizations. While the dataset included relatively few cases of flagged critical vulnerabilities, half of the F-rated institutions showed signs of high-risk web vulnerabilities.

Research Methodology

This analysis is based on data collected by the Business Digital Index (BDI) research team, which uses the BDI to evaluate publicly accessible information. The team uses custom scans, IoT search engines, IP, and domain name reputation databases to assess companies and institutions based on online security protocols. The index comprehensively assessed the cybersecurity hygiene of 75 European Union Institutions, Bodies, and Agencies (EUIBA).

The report evaluates cybersecurity risk across seven key dimensions: software patching, web application security, email protection, system reputation, hosting infrastructure, SSL/TLS configuration, and data breach history. The report's Methodology can be found here. It provides detailed information on how researchers conducted this analysis.

About Business Digital Index

The Business Digital Index (BDI) is a cybersecurity reputation platform initiative by Cybernews that provides organizations with a real-time security rating based on publicly available data. It continuously monitors external digital assets — such as exposed systems, outdated technologies, and other risk indicators commonly targeted by threat actors — and evaluates them using a weighted scoring model. This model considers technical vulnerabilities and real-world attack patterns to deliver a clear, standardized view of your organization's external cybersecurity posture.

Ruta Pauliukonyte
Cybernews
email us here