NEWS RELEASE

Cyber Security Regulations Are Breaking the Bank for UK Financial Service Organisations

2025-01-16

- Nearly Half (47%) of UK Businesses Reported Spending Over a Million Euros in the last two years.
- Ransomware remains the greatest cyber threat to the UK's finance and banking sector.
- Costs also deteriorated employee wellness; regulations put enhanced pressure on over half (58%) of UK CISOs.

LONDON--(BUSINESS WIRE)-- Although the European Digital Operational Resilience Act (DORA) and other Prudential Regulation Authority (PRA) measures offer increased resilience to organisations, new research from Rubrik today finds that compliance also comes with significant costs to businesses and their employees.

The report by Rubrik Zero Labs—commissioned by Rubrik (NYSE: RBRK) and conducted by Wakefield Research—finds that nearly half (47%) of financial and banking organisations in the UK reportedly have spent more than one million euros over the last two years on the implementation of regulations such as DORA and PRA, with over a quarter (28%) reporting spending between €501,000-€1,000,000. Despite implementation efforts, threats still loom, with ransomware remaining the greatest threat (46%) to financial organisations. One in five (20%) CISOs cited third-party compromise and 19% citing software supply chains as posing significant threats to security.

Equally concerning is the fact that 79% of these professionals report that it has had an impact on their mental health, highlighting the need for a more empathetic approach to these challenges.

Taking effect from January 17th 2025, DORA will **introduce** an enforced universal framework, including a focus on Information and Communication Technology (ICT) risk management. This framework could transform the financial

services and banking sector, given it typically holds some of the most sensitive data across all markets, and data.

“Given the increasing threat of ransomware and third-party compromise, the implementation of regulations is required and expensive. Understanding what data is the most critical, where that data lives, who has access to it, is essential to identifying, assessing, and mitigating ICT risks. If good hygiene practices like these are not followed, organisations can now receive fines from the Financial Conduct Authority (FCA),” said James Hughes, VP of Solutions Engineering and Enterprise CTO at Rubrik.

There also appears to be a major disconnect with the rest of the C-suite when it comes to prioritising cyber resilience, as over three-quarters (77%) of UK CISOs feel that their IT budget is not completely reflected by their board’s objectives to meet regulatory requirements.

“There is a critical gap between board-level understanding and reality. While regulators are increasingly stringent, many CISOs feel their budgets don't adequately reflect the board's commitment to compliance. This disconnect jeopardises not only organisations' security posture but also their ability to meet evolving regulatory demands,” added Hughes.

DORA mandates key provisions such as contractual safeguards and contingency plans to minimise dependencies and are in place to mitigate risks from partners. To ensure best practices regarding operational resilience, regular testing of digital resilience and attack simulations, as directed by DORA, will feed into cyber resilience plans and reassure CISOs.

Despite this, UK CISOs have more confidence in the cloud than their European counterparts with nearly three-quarters (73%) of UK CISOs feeling that their client, customer, partner and employee PII is secure in cloud environments.

CISOs, boards, and other stakeholders must work together to ensure that cyber resilience priorities are clearly defined, adequately funded, and effectively implemented to meet the evolving regulatory landscape and safeguard the industry’s future.

To find out more on EU data regulations, tune in to **CISO conversations** hosted on Rubrik’s YouTube channel.

Report Methodology

This research report was commissioned by Rubrik and conducted by Wakefield Research among 350 CISOs working at companies with a minimum of 500 employees, in the finance and banking sectors, excluding holding companies. Respondents comprised five markets: UK, Germany, France, Italy, The Netherlands, between November 21 and

December 3, 2024.

About Rubrik

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit **www.rubrik.com** and follow @ **rubrikInc** on X (formerly Twitter) and **Rubrik** on LinkedIn.

Media Contact:

Graham Day
Graham.Day@rubrik.com

Source: Rubrik