THE STATE OF DATA SECURITY

The New Rules

BREAKING THE BANKS

Rubrik Zero Labs

CONTENTS

THE STATE OF DATA SECURITY: THE NEW RULES BREAKING THE BANKS

This year, 2025, marks the much-anticipated implementation of The Digital Operational Resilience Act (DORA) in the European Union. While businesses ready themselves for implementation, what are the true costs to those in the financial sector? What stress has that put on the workforce? What are the biggest threats to financial services security?

Rubrik Zero Labs looked at the financial services sector, uncovering that not only is the monetary cost of implementation staggering, the cost to employee welfare is a significant consideration for financial organisations. Rubrik Zero Labs also delved into data security threats and those technologies that are keeping data safe.

We partnered with Wakefield Research to survey hundreds of CISOs working at companies with a minimum of 500 employees in the financial sector at the end of 2024. The individuals surveyed spanned five markets—the United Kingdom, Germany, France, Italy, and the Netherlands—and gave insight into the effects of DORA implementation on the financial sector.

The Costs of

IMPLEMENTING DORA

DORA which came into effect January 17th, 2025, introduced a new framework, including a focus on Information and Communication Technology (ICT) risk management in an industry that holds some of the most valuable data.

But what does the implementation of DORA really cost financial institutions, and how does that differ by country?

While more than one in four organisations (29%) report spending 501,000 to 1,000,000 Euros...

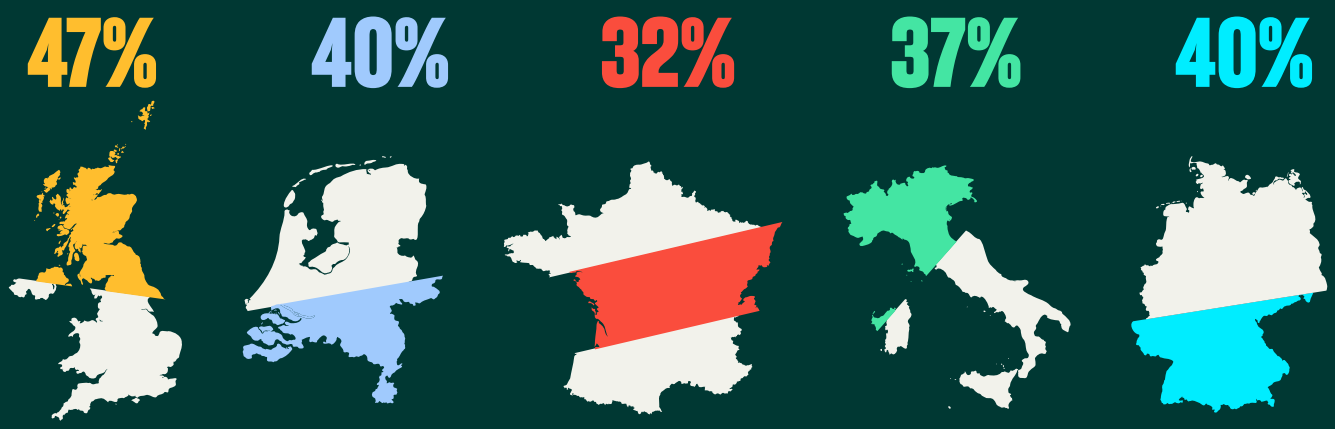
43%

reported spending more than

€1M

on implementation for DORA over the last two years.

How does that break down by country?



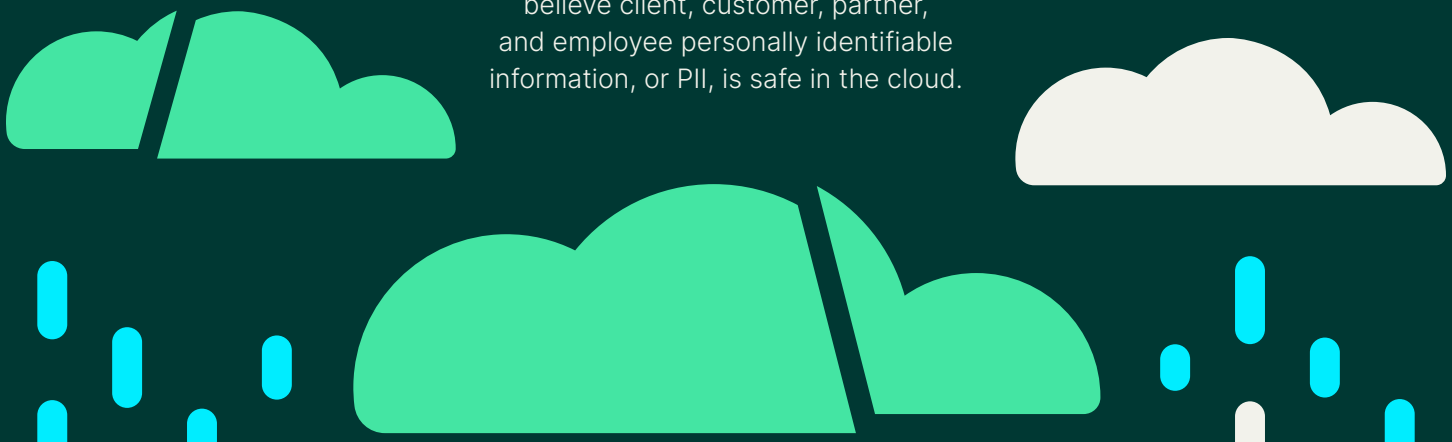
HIGH CONFIDENCE

in Data Security & Cloud

There is positive news for the financial sector: confidence remains high that our data is secure, despite wide data sprawl.

66%

believe client, customer, partner, and employee personally identifiable information, or PII, is safe in the cloud.



92%

of CISOs surveyed said their data sprawl environments were an issue.

Rubrik Zero Labs

The Unexpected Cost:

EMPLOYEE WELFARE

The monetary cost doesn't just apply to the balance sheet, but also to the welfare of those responsible for implementation.

80%

of all those surveyed confirmed that the implementation of DORA has had an adverse effect on their mental health.

23%

of financial sector employees working on DORA implementation have considered moving to a less-regulated industry.

The Biggest Concern for CISOs: RANSOMWARE

Threats loom and become more diverse every year, but ransomware rules for 2025 say financial sector CISOs.

CISOs reported the following as the biggest threats to their organisation:

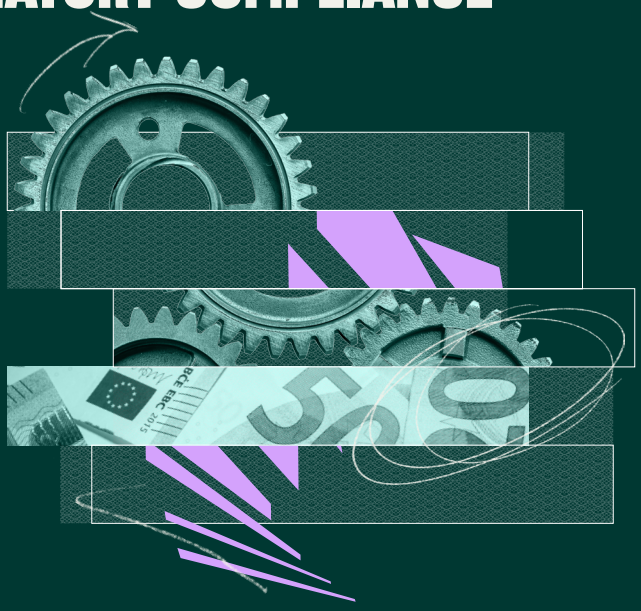
39%	23%	22%	9%	6%
Ransomware	Software Supply Chain	Third Party Compromise	Insider Threats, Including Human Error	Regulation

OUR RECOMMENDATIONS

Three steps to approaching regulation in financial services and securing your data:

USE AUTOMATED TOOLS & WORKFLOWS TO REDUCE THE MANUAL BURDEN OF REGULATORY COMPLIANCE

These technologies help streamline processes and alleviate the mundane heavy lifting forced on employees. Examples include governance, risk, and compliance (GRC) platforms, cloud-based auditing systems, and AI-driven monitoring tools. Though automation is key for efficient implementation, it is equally important to understand the entire pipeline. As a quality assurance measure, identify key failure points or points of interest that may require human intervention or review and build that into your process so employees know when to intervene.

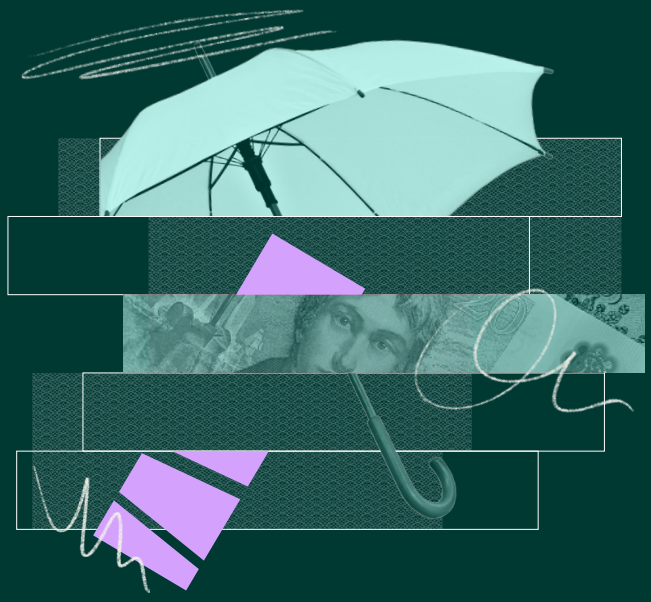


THIRD PARTY RISK MANAGEMENT

Develop and implement comprehensive third-party risk assessment frameworks, conduct regular audits, and require vendors to adhere to appropriate cybersecurity supply chain standards to minimise vulnerabilities introduced by third-party organisations and relationships.

PREPAREDNESS & READINESS ARE IMPERATIVE TO STRENGTHEN CYBERSECURITY DEFENSES

Prioritise endpoint protection tools like extended detection and response (XDR) platforms with containment features or capabilities to counter ransomware threats and robust backup and recovery solutions with immutable storage for rapid recovery. Invest in advanced threat intelligence platforms that provide real-time insights into emerging threats. This will further enable your proactive defense measures and improve response time by providing better-informed decision-making. Train staff using phishing simulations, incident response exercises, and tabletop exercises to level up key decision makers and security practitioners.



For more valuable insights, subscribe to Rubrik Zero Labs for actionable, vendor-agnostic insights to help bolster your organisation's cyber resilience strategy.

Sign up here to learn more.

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 were made up of five markets: the United Kingdom, Germany, France, Italy, and The Netherlands, between November 21 and December 3, 2024.