Rocket® software

Enhancing Mainframe Security and Building a Scalable Risk Management Program

Contents

Introduction

Cyber threats are escalating while regulatory requirements become more stringent, making the security of your mainframe more crucial than ever. According to recent studies, 91% of mainframe organizations have experienced data breaches or security compromises in the past five years. This alarming statistic underscores the need for a comprehensive and scalable risk management strategy. In this whitepaper, we will explore the key components of mainframe security, the importance of adhering to regulations like DORA, PCI DSS 4.0, and NIST, and how to build an effective risk management program.

91%

of mainframe organizations have experienced data breaches or security compromises in the past five years.

← Back to contents

The imperative of mainframe security

The State of mainframe vulnerabilities

The mainframe is often misconceived as an impregnable fortress. But its vulnerabilities range from configuration-based and code-based attacks to insider threats, unauthorized open source, and inadequate authentication measures. Many organizations fall short in compliance by only addressing configuration-based vulnerabilities and failing to address the ones that are code-based. Regulations require both, and not taking action leads to significant financial liabilities and non-compliance with regulatory standards.

28%

of IT leaders are extremely confident in their response to mainframe vulnerabilities.

Why prioritizing mainframe security is essential

Neglecting mainframe security is simply not an option. Regulations like DORA and PCI DSS 4.0 require stringent security measures to protect sensitive data and ensure operational continuity. The stakes are high: non-compliance or a breach could cost your organization millions. Today's cybercriminals have financial backing, sophisticated tools, and even AI assistance to exploit vulnerabilities. A proactive approach to mainframe security not only shields your organization from breaches but also reduces financial risks and ensures compliance with essential regulations.

4.45 million:

average revenue lost from a single non-compliance event.

← Back to contents

Key regulations guiding mainframe security

Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) mandates financial services companies to upgrade, evaluate, and implement innovative systems and protocols to safeguard their data. Key requirements include routine risk assessments, regular vulnerability management on the mainframe, and ensuring rapid data recovery within a two-hour window.

PCI DSS 4.0

PCI DSS 4.0 emphasizes the need for comprehensive security measures to protect payment card data. This includes regular vulnerability assessments, robust authentication mechanisms, and stringent data privacy policies.

NIST Guidelines

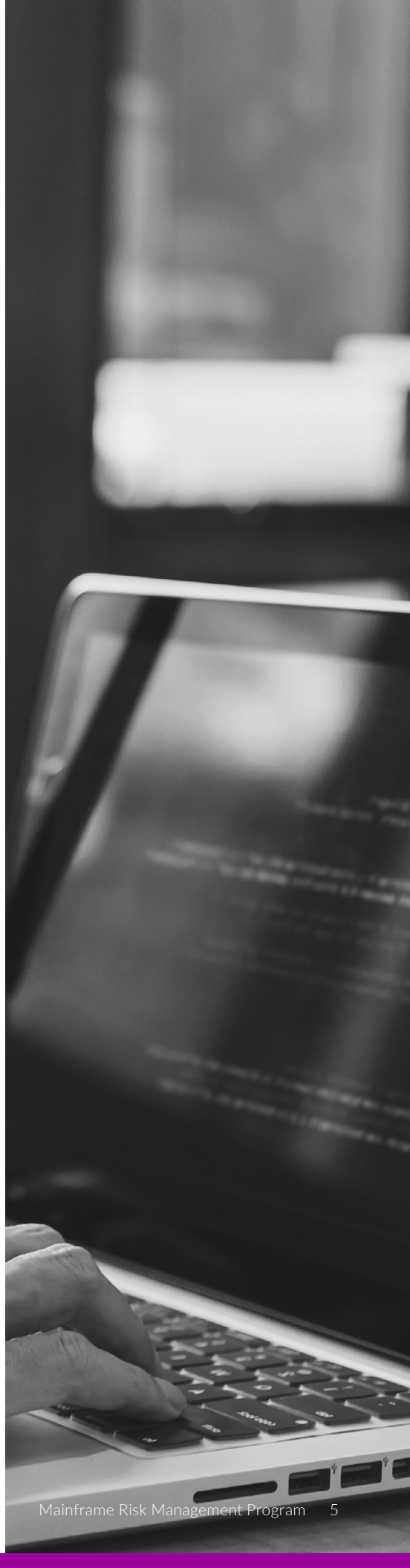
The NIST guidelines provide a framework for improving the security and resilience of critical infrastructure. They emphasize the importance of continuous monitoring, vulnerability management, and incident response planning.

NIS2

The NIS2 directive mandates organizations in Europe to prioritize resilience and incident response in both public and private sectors. It specifically targets combating cybercrime and enhancing cybersecurity management at both European and national levels.

GDPR

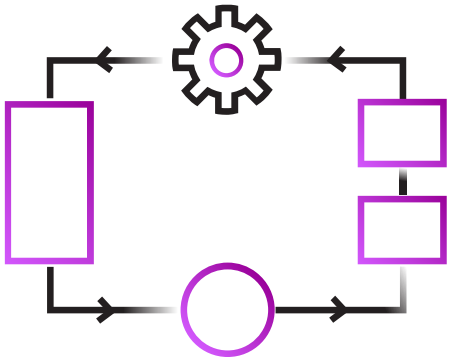
GDPR empowers consumers by giving them greater control over how companies use their personal data. By standardizing data protection rules across the EU, it creates a clearer and simpler legal framework for businesses.



← Back to contents

Building a scalable mainframe risk management strategy

To create a scalable risk management strategy for your mainframe, it's crucial not just to follow these regulations but to use them as a roadmap for evolving security practices. Focus on these key components to stay ahead:



01

Encryption and Data Privacy

Document data that shares use cases that are currently restricted, engaging in scenario planning to demonstrate the value to the organization if restrictions were lifted. By outlining specific objectives and evaluating the impact of more flexible yet secure data sharing, leaders can illustrate how such changes would benefit the business. Additionally, assessing pervasive encryption across all systems, including the mainframe, is crucial for maintaining robust security while accommodating more dynamic data sharing practices.

02

Authentication

Strong authentication mechanisms are essential to prevent unauthorized access. Implement multi-factor authentication (MFA) to add an additional layer of security. Regularly review and update access controls to ensure only authorized personnel have access to sensitive data.

← Back to contents

03

Response and Recovery

Despite the best preventive measures, breaches can still occur. A robust incident response plan is essential to mitigate damage and speed up recovery. Regularly conduct drills to ensure everyone knows their role during a crisis. Implement a surgical data recovery solution to recover data at a dataset level from a single point in time.

04

Vulnerability Management

Regular vulnerability assessments and timely patch management are essential for identifying and addressing security flaws. Focusing solely on configuration-based vulnerabilities leaves gaps in your mainframe cyber defenses and falls short of regulatory compliance. To meet standards like DORA and PCI DSS 4.0, you must implement regular code-based vulnerability management on your mainframe.

05

Resiliency

Business resilience involves the ability to adapt and continue operations despite disruptions. Develop a comprehensive disaster recovery plan and conduct regular testing to ensure your organization can quickly recover from incidents. Focus on building resilient systems that can withstand and adapt to evolving threats.

← Back to contents

Starting your mainframe security journey

For organizations just beginning their mainframe security strategy, we recommend focusing on the following key areas:

01

Implement Code-Based and Configuration-Based Vulnerability Management

Start by implementing both code-based and configuration-based vulnerability management on your mainframe. Regulations like DORA and PCI DSS 4.0 require regular vulnerability scanning and assessments to identify and mitigate vulnerabilities. Just one line of bad code or gap in integrity standards can lead to millions in liabilities.

02

Run Mainframe Penetration Testing Frequently

While vulnerability scanning identifies vulnerabilities based on where your z/OS® standards drift from policy, regulations also require penetration testing multiple times per year. Penetration testing uses tools and tactics wielded by cyber threat actors to replicate the conditions of a genuine hack on your mainframe infrastructure. This enables you to take an informed, aggressive approach to data and system security.

← Back to contents

03

Ensure Support for Unauthorized Open-Source Software

Unauthorized open-source software can pose significant security risks. Ensure that any unauthorized open-source software is supported and updated to the latest versions, including fixes for CVEs, and regularly patching vulnerabilities. This proactive approach can help mitigate risks and ensure compliance with regulatory standards.

04

Implement Surgical Data Recovery Solutions

Data recovery is a critical component of business resilience. Implement a surgical data recovery solution that can recover data at a dataset level from a single point in time. This is particularly important for financial organizations, as DORA requires data recovery within a maximum of two hours.

Conclusion

Securing your mainframe's data is not just about compliance; it's about safeguarding your organization's future. By prioritizing encryption and data privacy, robust authentication, effective response and recovery, comprehensive vulnerability management, and building resilient systems, you can create a scalable risk management strategy that adapts to evolving threats and regulations.

Are you ready to enhance your mainframe security and build a scalable risk management program? **Connect with our experts at Rocket Software** to learn more about how we can help you achieve your security goals.

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X (formerly Twitter).

Rocket® software

Modernization. Without Disruption.™

Visit RocketSoftware.com ›

Learn more

MAR-10531_WP_MainframeRiskMgmtPg_V2