Crowe

Cybersecurity risk and regulation in financial services

The 2023 Crowe report

Financial services organizations rely heavily on technology to deliver products and services. That reliance is only increasing, and when money and technology intersect, cyber criminals will be there to attack.

Statistics from Crowe clientele reporting show that most financial services organizations experienced cybersecurity attacks last year. To guard against rising and evolving threats, financial services organizations must establish powerful, adaptable cybersecurity measures.

While implementing technical safeguards is vital, organizations can't afford to overlook the human element of cybersecurity.

Every financial services organization should foster a culture of security awareness and compliance.

This report is designed to provide a comprehensive review of the most pressing cybersecurity risk areas within the financial services sector and offer our vantage point of the current environment and regulatory climate. The reporting is derived from anonymized data from Crowe clients and their regulatory advisories.

Key statistics*

50%

The approximate percentage of financial services organizations that don't have a formal cybersecurity risk management program

70%

The approximate percentage of financial services organizations that experienced a cybersecurity incident in the past year

$5.85M

The average cost of a data breach in the financial services sector

*Based on data from risk assessments and final audit reports prepared for Crowe clients, September 2022-June 2023

The top 5 high-risk cybersecurity areas

Based on our findings in a variety of cybersecurity areas, Crowe cybersecurity specialists have compiled this list of the most high-risk areas as well as critical questions organizations should ask. A “no” answer to any question might indicate a possible source of risk and a potential problem in this area.

This list can serve as a road map for financial services organizations to understand and prioritize their risk management initiatives. Organizations should continually evaluate and enhance their security postures to address and mitigate these risks.

1 Cybersecurity governance

What Crowe cybersecurity specialists do:

Scrutinize the strategies, protocols, and safeguards employed to counter cybersecurity threats.

Questions to ask:

- → Do our strategies and protocols effectively counter cybersecurity threats?
- → Does our organization have a formalized cybersecurity risk management program?

2 Access management

What Crowe cybersecurity specialists do:

Evaluate the measures taken to control access to systems and data, with a particular focus on privileged access.

Questions to ask:

- → Do our organizational password standards align with industry best practices, and do we enforce those standards?
- → Do we conduct periodic and thorough reviews of access rights?

3 Network security

What Crowe cybersecurity specialists do:

Inspect the defenses in place to protect the integrity and usability of network and network-accessible resources.

Questions to ask:

- → Does our organization have a detailed knowledge of our network infrastructure, including potential attack pathways?
- → Do we have adequate controls in place to govern network access and data transfer?

4 Logging and monitoring

What Crowe cybersecurity specialists do:

Assess the procedures for tracking and reviewing operations on a system to detect security incidents.

Questions to ask:

- → Do we adequately log security events and incidents?
- → Do we have sufficient monitoring and alerting mechanisms for potential security threats?

5 Vulnerability and patch management

What Crowe cybersecurity specialists do:

Investigate how organizations identify, classify, prioritize, and address vulnerabilities as well as how they apply patches and updates.

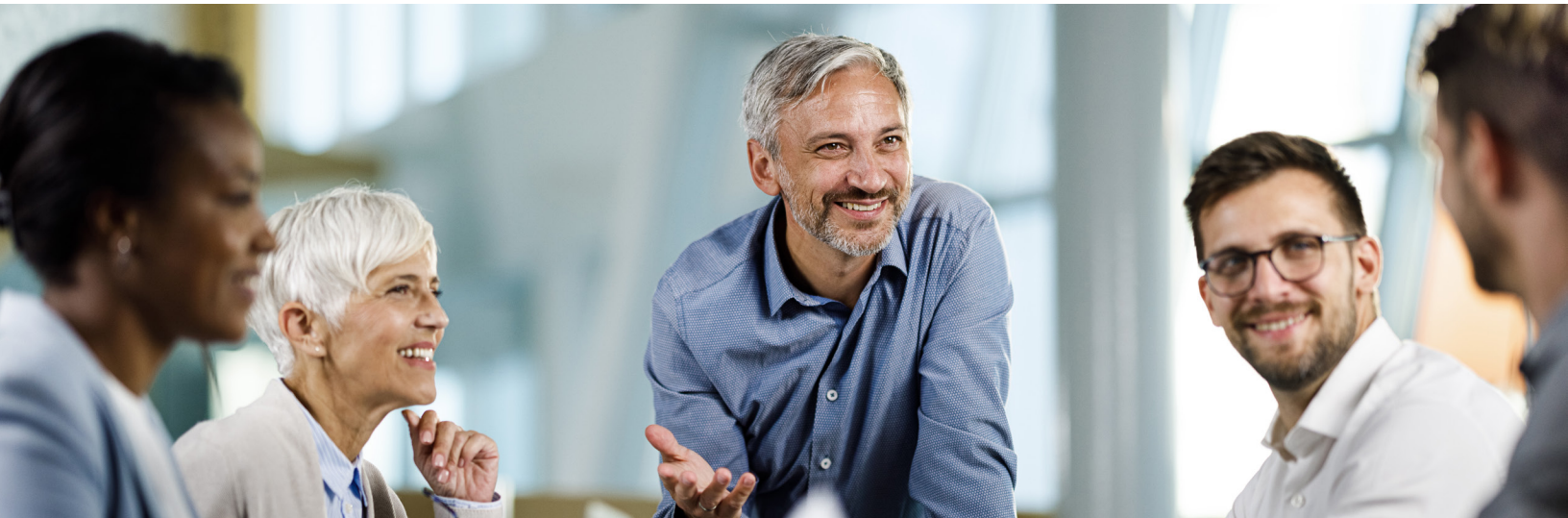
Questions to ask:

- → Do we consistently apply patches and updates?
- → Do we have adequate vulnerability management processes?

Other noteworthy areas

(listed by level of risk):

6. Networking device technical configuration review
7. Endpoint security
8. Active directory technical configuration review
9. Operating system security review
10. Cloud security
11. Threat management
12. Security engineering and architecture
13. Wireless security
14. Mobile device management
15. Data classification handling
16. Web security
17. Asset management



Let’s talk about how to make your financial services organization safer, more secure, and more prepared.

Crowe cybersecurity specialists help organizations like yours solve cybersecurity challenges and evolve to match the latest threats. We don’t just understand cybersecurity – we understand the business of banking.

David R. McKnight
Principal
Financial Services Consulting
+1 630 575 4399
dave.mcknight@crowe.com

Timothy Tipton
Financial Services Consulting
+1 202 552 8093
timothy.tipton@crowe.com

Stay up to date on the latest threats with Cybersecurity Watch

In this publication, our cybersecurity specialists offer insights on how organizations can take proactive steps to mitigate risk, shore up their network security, and quickly identify and respond to threats. **Explore Cybersecurity Watch and subscribe today for timely insights.**

Explore at crowe.com/cybersecurity-watch

CFS2409-002C