Coalition

THE CYBER SAVVY BROKER'S GUIDE

Cyber Insurance for the Financial Services Industry

Financial services organizations are attractive targets for cybercriminals due to the vast amount of data they handle and the types of transactions they facilitate. Direct access to financial records, social security numbers, and other types of sensitive data puts the financial services industry at increased risk of experiencing a cyber attack.

Cyber risk for financial institutions can originate both internally and externally — from disgruntled employees and contractors who have access to sensitive information to threat actors executing sophisticated cyber attacks. These attacks can exploit vulnerabilities in software systems or use social engineering techniques to access and steal sensitive data, manipulate financial transactions, and even disrupt their clients' business systems — all of which can result in significant financial loss, reputational damage, and legal consequences,

Claims Insights

It's just a little security incident. How bad could it be?

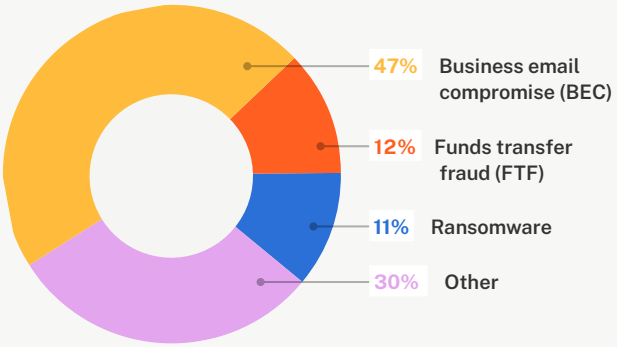
$150,000

Average cost of a cyber insurance claim for financial services organizations

Claim Examples

ORGANIZATION	INCIDENT	LOSS
Investment Advisory Firm	Funds Transfer Fraud	$107,000
Real Estate Lending	Business Email Compromise	$116,000
Health Insurance	Ransomware	$502,000

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT — Although it's not the leading event type, the average ransomware loss for organizations in the financial services industry is more than $206,000.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

*Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. ("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers. Copyright © 2023. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.

Coalition

Unique Exposures

Most financial services businesses use data and technology. Why is that risky?

Essential Technologies Can Create Cyber Risk

Mobile banking platforms

Mobile banking enables users to access their accounts remotely and perform various transactions. While convenient, the technology can be vulnerable to phishing, malware, and data interception, potentially leading to unauthorized access, data theft, or financial fraud.

Cloud computing

Cloud computing allows financial institutions to store and process large amounts of data off-site, improving scalability, profitability, and efficiency. However, risks include unauthorized access to sensitive data, data breaches due to misconfigurations, and lack of control over security measures implemented by cloud service providers.

Customer relationship management (CRM) systems

CRM systems store extensive customer data, including personally identifiable information. If breached, cyber attackers can gain access to sensitive customer information, leading to identity theft, financial fraud, litigation and regulatory proceedings, and reputation damage for the financial institution.

Biometric authentication

Biometric authentication technologies, such as fingerprint or facial recognition, are often used for secure access to financial services. These technologies carry cyber risks related to spoofing attacks, where biometric data can be replicated or manipulated, bypassing authentication measures and gaining unauthorized access to accounts or transactions.

Data analytics and machine learning

Financial institutions use data analytics and machine learning algorithms to gain insights, detect patterns, and make automated decisions. Robotic Process Automation (RPA) technology, in particular, can automate repetitive financial tasks to improve speed and efficiency. However, the technology that makes this possible can be susceptible to data manipulation, model poisoning, and adversarial attacks, leading to inaccurate predictions, fraudulent activities, or biased decision-making.

Email

Business email compromise (BEC) is the leading cause of cyber insurance claims in the financial services industry, triggering data breaches, business interruption and even reputational damage.

End-of-life software & hardware

Organizations may use outdated technologies with the belief that upgrading would be expensive, time-consuming, and disruptive. However, technologies no longer supported by the manufacturer often have known security vulnerabilities and may lack important security features to protect against modern threats.

High-frequency trading (HFT) systems

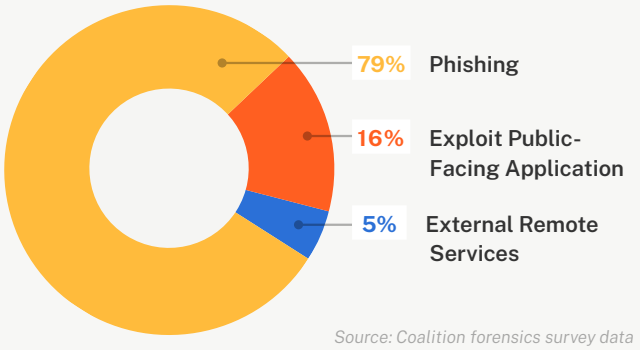
HFT systems enable financial firms to execute trades at high speeds using advanced algorithms. Cyber risks associated with HFT systems include distributed denial-of-service (DDoS) attacks on trading infrastructure, market manipulation, and algorithmic vulnerabilities leading to unintended or harmful trades.

Payment gateways

This technology is used to securely transmit cardholder information between merchant websites and financial institutions. Online payment processing poses significant cyber risk, including payment card fraud, data breaches, and skimming attacks targeting card information during the payment process.

Cyber Claims in the Financial Services Industry by Attack Vector

KEY INSIGHT —— Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue all sorts of malicious activities, which is why **phishing is the leading attack vector for all cyber claims.**



Source: Coalition forensics survey data

*Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. ("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers. Copyright © 2023. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.

Coalition

Sensitive Data Can Increase Business Liability

Protected health information (PHI)

Many financial organizations have access to employee or client healthcare information. This may require these organizations to sign Business Associate Agreements that dictate compliance with the Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule. Access to PHI data exposes financial institutions to additional cyber risks and possible fines and penalties if an actual or suspected data breach occurs.

Personally identifiable information (PII)

PII is any data that can potentially identify a specific person. PII can be used to launch cyber attacks or gain access to networks to initiate attacks. Organizations that mishandle PII or fail to respond to a data breach appropriately can be subject to fines, penalties, and other financial damages.

Know your customer (KYC) data

Financial institutions collect and store customer information for the purposes of establishing customer identity and determining their risk. Attackers may target this data through insider threats, third-party breaches, or social engineering attacks to perform identity theft, open fraudulent accounts, or enable other criminal activities.

Sensitive employee information

Every organization collects and stores information about its employees. Unauthorized access or disclosure of this data can cause direct harm to employees.

Financial data

Collecting and processing financial information — bank accounts, credit cards, balances, transaction history, loan and credit application data, and even wire transfer details — requires adherence to industry standards. Mishandling or unauthorized disclosure of this data can cause direct harm to clients and trigger industry and regulatory investigations.

Biometric data

Fingerprints, facial scans, and other biometric data technologies are frequently used for authentication purposes. Much like passwords, this data can be stolen and used to impersonate individuals, access accounts, and perpetuate cybercrime.

Geolocation data

Some financial institutions may use geolocation data to provide enhanced services and security to clients. Enhanced user experience and protections help attract and retain clients, but this data can be used to track individuals, commit identity theft, and other types of fraud if it falls into the wrong hands

Non-sensitive personal information

Some data may be publicly available and not considered protected, but a breach can still impact trust and public image if it appears the organization did not handle the situation appropriately.

Examples of Legal & Regulatory Compliance

- Data privacy & security contractual obligations
- Gramm-Leach-Bliley Act
- International data privacy and consumer protection regulations (e.g. GDPR)
- Sarbanes-Oxley Act
- State data privacy & consumer protection laws (e.g. CCPA)
- State notification requirements
- Payment Card Industry Data Security Standard (PCI DSS)

$5.04 million

Average total cost of a **data breach** for financial services organizations[1]

1. IBM Security, Cost of a Data Breach Report 2023

*Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. ("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers. Copyright © 2023. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.

Coalition

Business Impacts

What can financial services organizations expect after a cyber incident?

Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on a financial institution's ability to operate and can be highly visible to clients and other stakeholders. Even short periods of disruption can lead to direct loss of revenue and inhibit an organization's ability to support customers, negatively impacting not only client retention but also the delivery of essential services. Relevant insuring agreements may include:

- Business Interruption & Extra Expenses
- Reputation Repair

Cybercrime

Beyond ransomware and data breaches, cyber events can result in financial theft for a financial institution or its customers — often without an actual breach. If an attacker dupes someone in the billing department to alter payment instructions, an organization can lose tens or hundreds of thousands of dollars almost instantly. Attackers can also gain access to email accounts and send fraudulent invoices or payment instructions to clients, vendors, and other third parties. Relevant insuring agreements may include:

- Funds Transfer Fraud
- Invoice Manipulation
- Phishing (Impersonation) and Proof of Loss Preparation Expense Endorsement
- Service Fraud

Recovery and restoration

After a cyber event, resuming operation is no easy task. If an attacker damages or destroys essential technology, data, or physical equipment, an organization may need to bring in external support or purchase new equipment to re-secure systems. Full remediation, restoration, and recovery can take a significant amount of time, when possible, and may require purchasing new software, systems, and consultants to rebuild the network. Relevant insuring agreements may include:

- Computer Replacement
- Digital Asset Restoration

Direct costs to respond

Responding to a cyber event typically requires numerous direct costs, also known as first-party expenses. If a financial services organization experiences a data breach involving PII, it will require a prompt response and the need for additional legal counsel, forensic investigation, victim remediation, and notification to comply with regulatory requirements. Simple investigations can cost tens of thousands of dollars, while more complex matters can increase costs exponentially. In extreme cases, organizations may consider negotiating with cybercriminals or paying ransom demands to recover encrypted or compromised data. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 1st Party
- Breach Response
- Crisis Management
- Cyber Extortion

Liability to others

Navigating the patchwork of laws and regulations after a security incident or data breach is especially difficult for organizations that operate in a highly regulated industry across multiple legal jurisdictions. A data breach or security failure can trigger liability to third parties and cause bodily harm or injury, even if the management of financial records is outsourced and the organization is otherwise in compliance with applicable regulations. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 3rd Party
- Multimedia Content Liability
- Network and Information Security Liability
- PCI Fines and Assessments
- Pollution
- Regulatory Defense and Penalties

*Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. ("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers. Copyright © 2023. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.

Coalition

Cyber Insurance Reimagined

How does Coalition perform?

1.87%
Coalition 2022 overall claims frequency

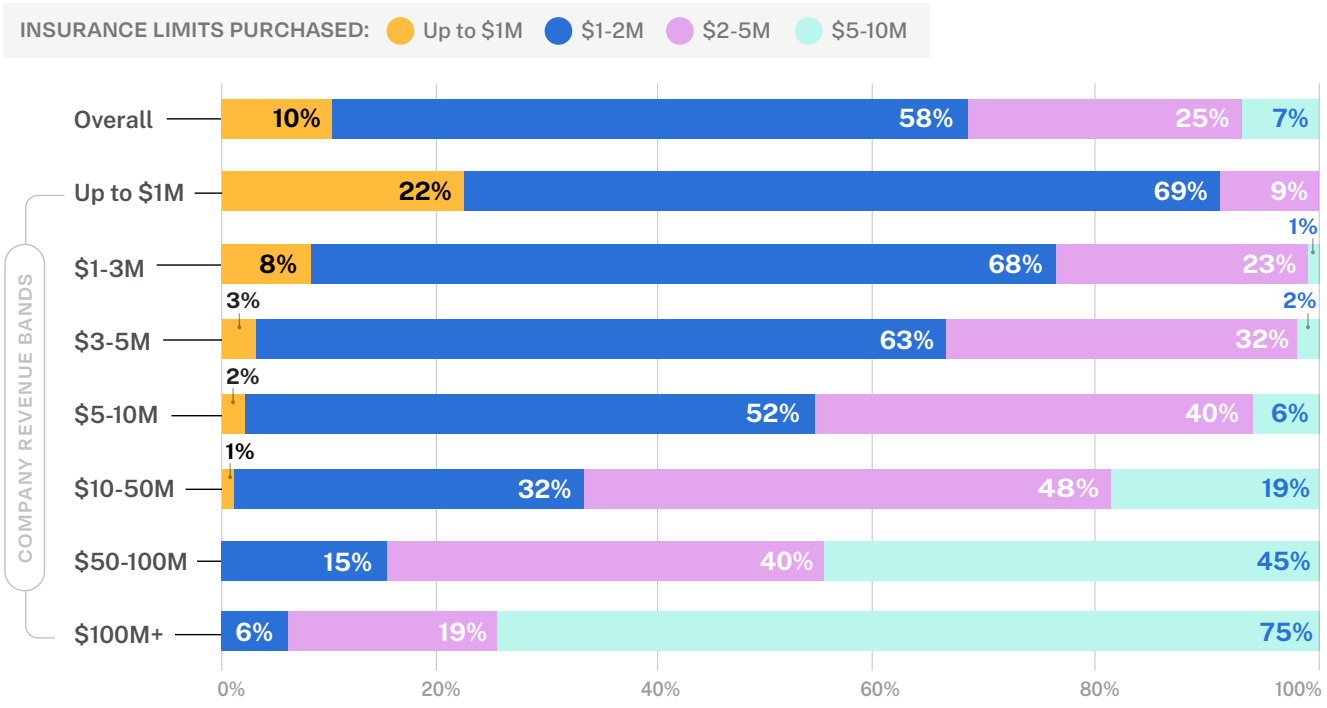
↓ 22%
Year-over-year decrease in claims frequency

64% fewer
Coalition claims vs. cyber industry average

Peer Purchasing Insights

Primary limit amounts purchased by others in the financial services industry

PEER PURCHASING HABITS BY REVENUE



Source: Coalition policyholder data

KEY INSIGHT — Most small and medium-sized businesses in the financial services industry purchase $1M-2M in limits, while many mid-market organizations purchase $5-10M in limits. For those needing more than $10M in limits, Coalition offers primary and excess terms for businesses up to $5B in revenue.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

*Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. ("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers. Copyright © 2023. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.

Coalition

The Power of Active Insurance

Why do financial services organizations choose Coalition?

47%	43%	5 minutes
Reported cyber events handled with no cost to policyholder	Reduction in critical vulnerabilities among policyholders in 2022	Average response time to a cyber incident

Active Insurance* is designed to help mitigate digital risk before it strikes.
Our new approach to managing digital risk provides **three layers of support**:

Active Protection

Monitoring and alerting to identify and prevent risk before it strikes

Active Response

Access to in-house resources that accelerate response and coverage if an incident occurs

Active Risk Assessment

Underwriting, quoting, renewals, and digital risk scores powered by real-time data

Insurance as active as digital risk

In the digital economy, Coalition wants to ensure that all organizations can thrive by helping to protect them from the threat of emerging risks. We've built an expert team across incident response, claims, and our panel vendors. In the event of a claim, Coalition helps organizations respond and recover so they can get back to business.

Brokers

Get appointed today at signup.coalitioninc.com

FInancial services organizations

Get a free risk assessment at control.coalitioninc.com

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **coalitioninc.com**

*Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. ("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers. Copyright © 2023. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.