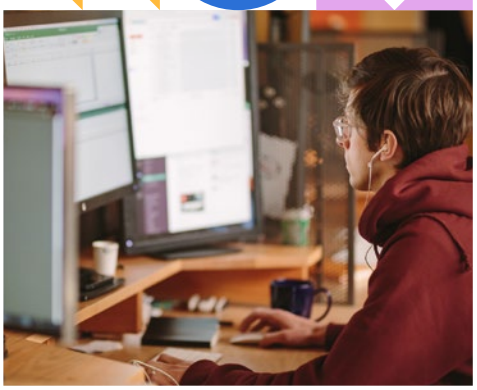
Coalition



THE CYBER SAVVY BROKER'S GUIDE

Cyber Insurance for the Technology Industry

Businesses in the technology industry face unique cyber exposures due to the data they possess and the technologies they use to support operations. They often store and process sensitive information on behalf of clients and may have direct access to customer applications and systems — all of which makes them prime targets for cybercriminals. These businesses may also rely on third-party software and services to build their products, which can expose them to additional risks if the components have vulnerabilities.

Technology companies typically have a broad attack surface due to their complex and interconnected IT infrastructures, creating a greater opportunity for adversaries to exploit vulnerabilities, gain unauthorized access, and disrupt services. Plus, many organizations have a significant online presence, exposing them to a wide range of threats that can target employees, customers, or infrastructure.

For technology companies that provide services via written contract, a cyber incident can trigger an Errors and Omissions (E&O) claim. These companies may need to maintain specific insurance coverages due to contractual agreements, requiring them to perform specific services, secure data, and control system access. A cyber incident can impact a company's ability to deliver those services, triggering a breach of contract and exposing clients or other third parties to attacks. This liability underscores the need for combined Cyber and Tech E&O coverages to help protect businesses in a coordinated manner.

Claims Insights

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

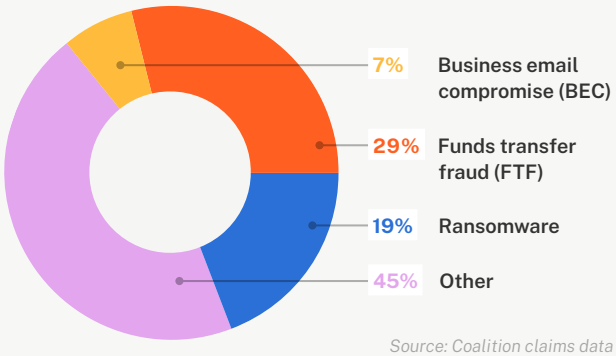
$343,000

Average cost of a cyber insurance claim for technology organizations

Claim Examples

ORGANIZATION	INCIDENT	LOSS
Home Energy Management	Funds Transfer Fraud	$279,000
Capital Markets Platform Solution	Ransomware	$442,000
Mobile Investing Application	Other (Service Fraud)	$39,000

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 technology industry is more than $417,000.

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

Coalition

Unique Exposures

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

Essential Technologies Can Create Cyber Risk

First-party software & services

Customer web applications and backend database security is a unique exposure for technology companies with customer-facing assets. Whether third parties use the tech-enabled solution for processing orders, tracking shipments, interfacing with suppliers, managing inventory, or managing customer relationships, data flow must be considered an asset with pertinent business risk, similar to financial or tangible assets.

Third-party software & services

Technology companies often rely on third-party software, libraries, or APIs. If these external components have existing vulnerabilities, or vulnerabilities are discovered in them later, it can create security risks for the technology companies that depend on them.

Code repositories

Code repositories are used to store and manage source code. A repository breach can expose sensitive code, API keys, or authentication credentials that can be exploited for unauthorized access or further attacks.

Cloud infrastructure

Technology companies typically rely on cloud services for storage, computation, or data processing. Breaches in cloud infrastructure may expose customer data, proprietary information, or sensitive configurations, making the companies vulnerable to various cyber threats.

CRM systems

Client relationship management (CRM) systems are used to support business development activities. Containing client data and confidential corporate information, these systems could be compromised and leveraged for malicious purposes, resulting in a data breach.

Email

Business email compromise (BEC) is a frequent cause of cyber insurance claims for technology organizations, which can trigger data breaches, business interruption and even reputational damage.

Artificial intelligence (AI) & machine learning (ML)

AI and ML systems have become more prevalent in organizations as a way to automate manual tasks, improve efficiency, and maximize productivity. However, these can be exploited to manipulate decision-making processes or trick algorithms into making incorrect predictions, impacting business operations.

Intellectual property

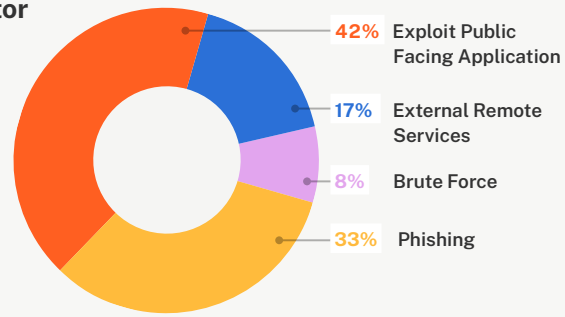
Many technology companies are involved in research, development, and innovation. They may have valuable intellectual property, proprietary algorithms, or patents that can make them attractive targets for industrial espionage or cyber theft.

Internet of Things (IoT) devices

IoT devices are programmable pieces of hardware used to transmit data over the internet or other networks. They can be embedded into other mobile devices and are vulnerable to intrusions, making them prime targets for attackers to gain access to a business' network.

Cyber Claims in the Technology Industry by Attack Vector

KEY INSIGHT —— Technology companies frequently see adversaries scan the internet for vulnerabilities in their public-facing applications to gain access, underscoring the need to secure these applications using multi-factor authentication (MFA) or putting them behind a virtual private network (VPN).



Source: Coalition forensics survey data

Coalition

Sensitive Data Can Increase Business Liability

Corporate confidential data

Technology companies may have access to internal operations data, trade secrets, or intellectual property — both their own and that of their clients. Unauthorized access of corporate confidential data could cause significant damage to the data owner, damage client relationships, and even trigger a breach of contract.

User credentials & personal data

Technology companies maintain customer databases containing users' personal information, including sensitive information like usernames and passwords. These databases are attractive to cybercriminals for identity theft, financial fraud, or selling the information on the dark web.

Protected health information (PHI)

Technology companies can have access to, or process, PHI for their clients. Often as a "Business Associate," some may even be bound by the Health Insurance Portability and Accountability Act Privacy Rule (HIPAA), which carries additional data protection and reporting requirements if an actual or suspected data breach occurs.

Communication & messaging data

Technology firms that provide communication platforms, email services, messaging apps, or social networks gather significant amounts of user-generated content and communications. Breaching these systems can result in blackmail, compromised privacy, or dissemination of sensitive information.

Financial data

Many technology businesses handle financial transactions and have access to bank details, credit card information, income and assets, loan information, and credit history. Threat actors may attempt to access this data to compromise financial security.

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.

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.

Sensitive employee information

Every organization collects and stores information about its employees. Unauthorized access or disclosure of this data — whether PII, PHI, financial, or otherwise — can cause direct harm to employees.

Examples of Legal & Regulatory Compliance

- Data privacy & security contractual obligations
- Fair Credit Reporting Act (FCRA)
- Financial Industry Regulatory Authority (FINRA)
- HIPAA
- International data privacy and consumer protection regulations
- State data privacy & consumer protection laws
- State notification requirements
- Payment Card Industry Data Security Standard (PCI DSS)

$4.66 million

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

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

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

Coalition

Business Impacts

What can technology businesses expect after a cyber incident?

Breach of contract or failure to provide services

A cyber incident can impact a company's ability to provide services, especially those providing technology or consulting services. If a company is unable to fulfill its obligations, it can result in a breach of contract that may expose a company to legal action and expenses beyond the direct costs to respond to an incident that would otherwise be covered by cyber insurance. By adding an endorsement to a cyber insurance policy, technology companies can maintain professional liability coverage that is aligned to the services that they provide. Relevant endorsements may include:

Technology Errors & Omissions (Tech E&O):
When providing technology services to clients

Miscellaneous Professional Liability (MPL):
When providing business and consulting services to clients

Direct costs to respond

Responding to a cyber event can require numerous direct costs, also known as first-party expenses. If a technology company experiences BEC and sensitive data is involved, it can trigger a need for additional legal counsel, forensic investigation, victim remediation, and notification. Simple investigations can cost tens of thousands of dollars, while complex matters can increase costs exponentially. Relevant insuring agreements may include:

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

Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on an organization's ability to operate and can be highly visible to clients, customers, and other stakeholders. Even short periods of disruption can lead to direct loss of revenue and inhibit a company's ability to support clients, negatively impacting client retention and acquisition. Relevant insuring agreements may include:

- Business Interruption & Extra Expenses
- Reputation Repair

Liability to others

The evolving cyber landscape can be difficult to navigate, particularly as it relates to legal, compliance, and contractual issues. Many technology companies face new and unexpected exposures after a cyber event. Even with strong contracts, policies, and best practices in place, a data breach, security failure, or even a simple mistake can trigger liability to third parties and expose an organization to regulatory investigations and legal action from victims. 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

Cybercrime

Beyond ransomware and data breaches, technology companies and their clients are vulnerable to the theft of money by electronic means. 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 donors, beneficiaries, 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 equipment, an organization may need to bring in external support or purchase new equipment. Full remediation, restoration, and recovery can take a significant amount of time, when possible, and may require new software, systems, and consultants to rebuild the network. Relevant insuring agreements may include:

- Computer Replacement
- Digital Asset Restoration

Coalition

Cyber Insurance Reimagined

How does Coalition perform?

1.87%
Coalition 2022 overall claims frequency

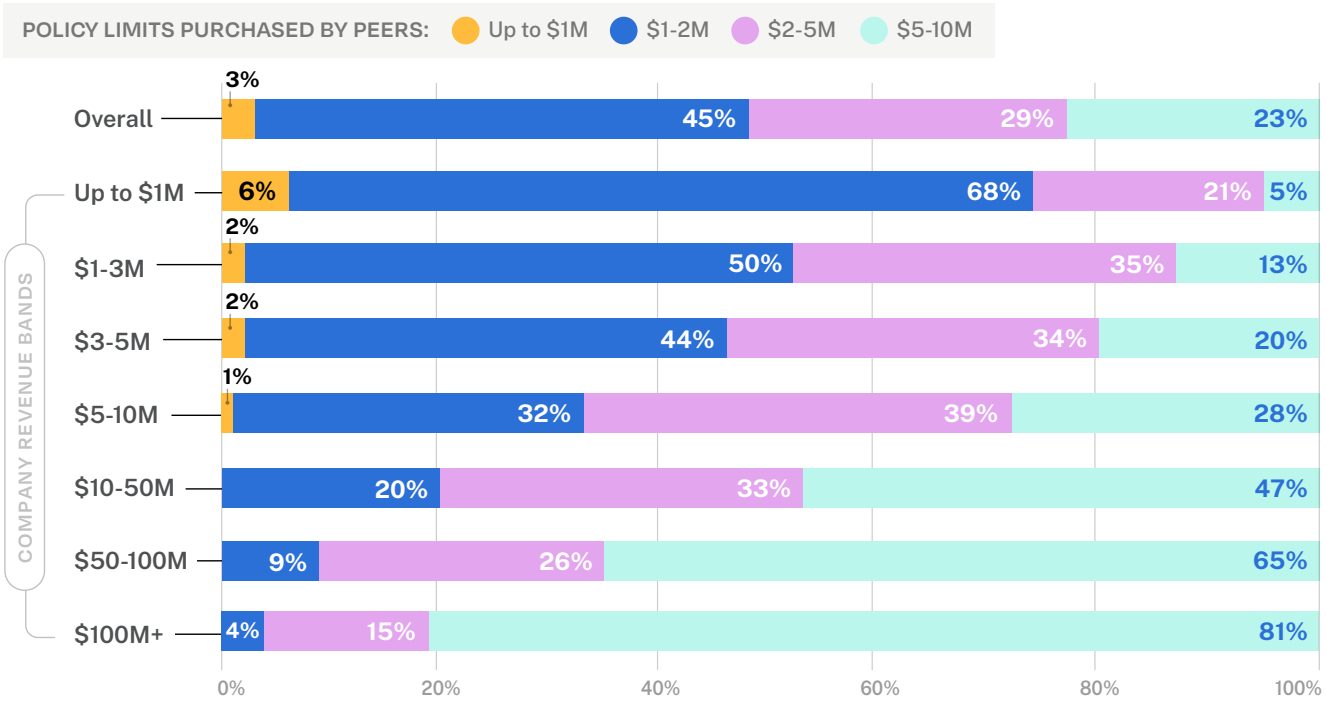
↓ 22%
Year-over-year decrease in claims frequency

64% fewer
Coalition claims vs. cyber industry average

Peer Purchasing Insights

Primary limit amounts purchased by others in the technology industry

PEER PURCHASING HABITS BY REVENUE



Source: Coalition policyholder data

KEY INSIGHT —— Most small and medium-sized businesses in the technology industry purchase $1M-2M in limits, while many mid-market organizations purchase between $2M and $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

Coalition

The Power of Active Insurance

Why do technology businesses choose Coalition?

47%

Reported cyber events handled with no cost to policyholder

43%

Reduction in critical vulnerabilities among policyholders in 2022

5 minutes

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

Technology businesses

Get a free risk assessment at control.coalitioninc.com

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