

# CYBER

10 ways cyber risks threaten businesses



## Property Damage & Pollution Liability

Remote-controlled equipment gives cyber saboteurs a way to destroy property from afar, potentially creating pollution hazards that affect the environment and human health.



## Reputational Harm

A highly publicized cyberattack can damage a company's reputation in several ways — such as eroding customer trust and even lowering its stock market price. Responding thoughtfully and immediately to cyber events can help mitigate these negative impacts.

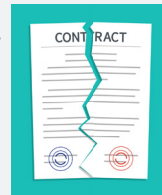


## Business Interruption

Whether caused by phishing, malware, denial of service, or another form of attack, business interruption due to a cyber event can result in significant downtime and losses of productivity, sales, and income.

## Lost Customer Relationships

Some sectors, including the financial industry, are especially vulnerable to customer dissatisfaction following a breach. Besides lost revenue, a cyber incident can cost a company long-standing relationships that have taken years to build.



## Legal Costs & Fines

Class action lawsuits related to data breaches rose 46% last year to over \$700M. Cyberattack-related lawsuits, regulatory action defense and fines now cost large companies more than \$3 million on average.



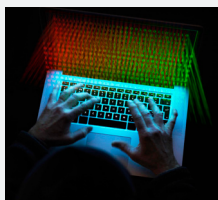
## Stolen Intellectual Property

For some industries, such as life sciences, technology, and defense, losing corporate secrets can compromise a firm's competitive advantage, and illegally unlocked products can significantly impact a company's bottom line.



## Hardware & Digital Asset Losses

Cyberattacks can result in lost or damaged digital files as well as hardware failure, which can lead to disruptions and financial losses.



## Business Email Compromise and Payment Fraud

In 2022, the FBI's Internet Crime Complaint Center (IC3) received 21,832 business email compromise (BEC) complaints with adjusted losses totaling over \$2.7 billion.

## Ransom Payments

Ransomware payments fell by over 40% to \$457M in 2022 as businesses increasingly refuse to pay ransom demands.



## Incident Response Costs

According to a 2022 report, companies spent an average of \$110k on services associated with responding to breach incidents; for large companies, the average is \$4.1M. Having an incident response team and regularly tested plan can reduce total data breach costs by as much as 50%.



Impact

Frequency

