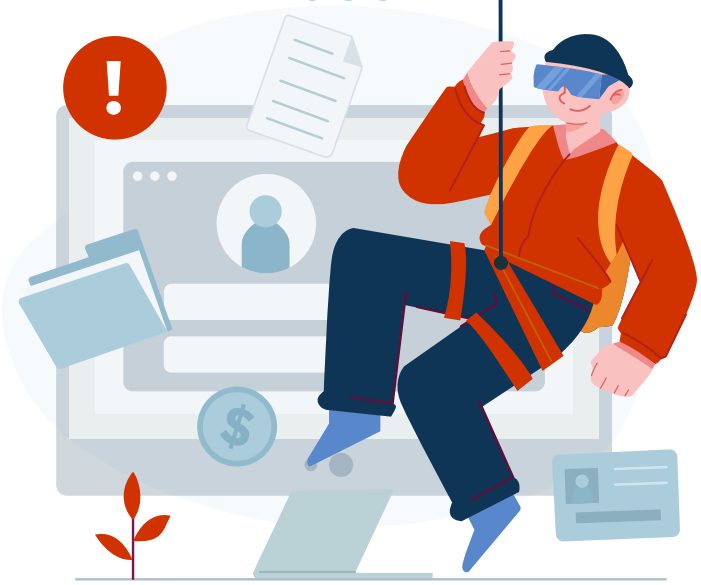
DATASTREAM
CYBER INSURANCE

# CLAIM EXAMPLE

## DATA EXPOSURE



## SITUATION

An employee at Allan's company was uploading hundreds of customer records to the corporate cloud, but the cloud file storage was mistakenly set to be publicly readable. A few days later, the employee noticed the error and contacted his supervisor.

## OUTCOME

Thankfully, Allan had **Breach Response** coverage. After notifying his insurer, a breach advisor was assigned to the case, who involved a forensics firm. They were able to quickly identify the exposed customer records and comply with all requirements to notify customers. Thanks to quick action, no customers reported any damages. Identifying and notifying all the customers cost $25,000, and the forensic cleanup cost $35,000.

SAVINGS:
95%

Total cost of the claim:
**$60,000**

Paid by Allan's company:
**$2,500 (retention)**

Covered by the insurer:
**$57,500**





Limit

DATASTREAM
CYBER INSURANCE

# CLAIM EXAMPLE

## RANSOMWARE


## SITUATION

It was a normal workday at Susan's company, until suddenly every employee's computer froze and displayed a message: "You have been hacked. Pay us $500,000 by tomorow or we'll delete all your data." This effectively shut down the company's operations, losing them thousands of dollars in revenue every hour.

## OUTCOME

Thankfully, Susan had **Cyber Extortion** coverage. She contacted her insurer and they immediately assigned a security response team. They began negotiating with the criminals, while working in the background to restore business operations. Ultimately, the response team broke through the ransom software and successfully restored the manufacturer's systems.

SAVINGS:

99.5%

Potential Loss:

**$500,000**

Paid by Susan's company:

**$2,500 (retention)**

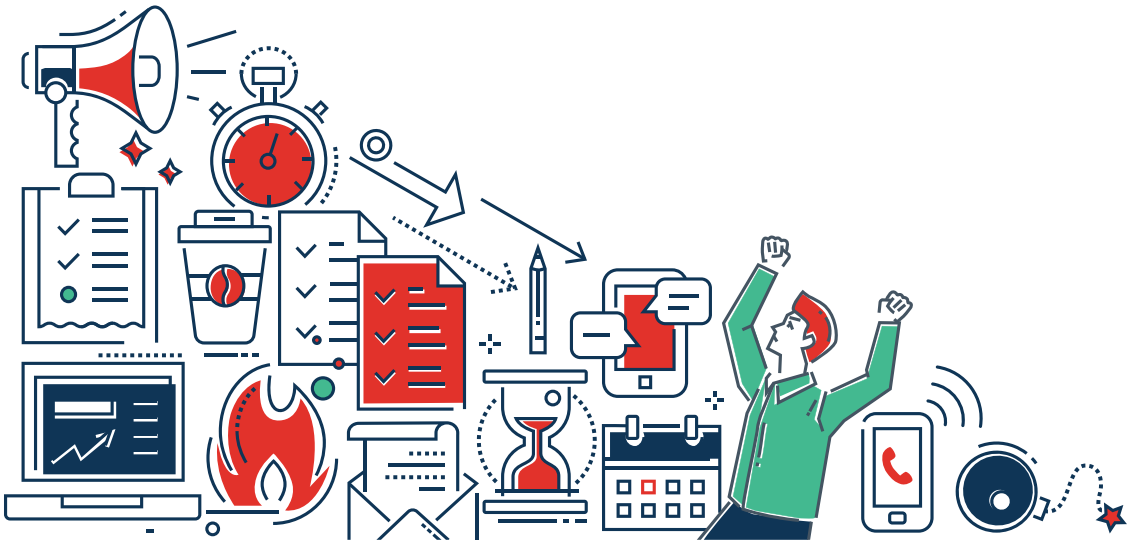
Loss avoided:

**$497,500**

DATASTREAM
CYBER INSURANCE

# CLAIM EXAMPLE

## CONTINGENT BUSINESS INTERRUPTION



## SITUATION

Daniel's online shop has an IT provider, who suffered a major breach. Hackers shut down the IT provider for a week, demanding a ransom. This affected all clients of the IT provider, including Daniel he was unable to do business that week. After a week of negotiations, the IT provider's systems were restored, allowing Daniel to do business again.

## OUTCOME

Thankfully Daniel had **Contingent Business Interruption** coverage. As soon as his website was down for more than an hour, he contacted his insurance carrier. The insurance carrier activated the policy and indemnified Daniel's shop for every day it was offline. Daniel's shop normally grosses $8,000 a day in revenue, so he was paid out $56,000 for seven days.

SAVINGS:

91%

Lost revenues:

**$56,000**

Paid by Daniel's company:

**$5,000 (retention)**

Paid by the insurer:

**$51,000**



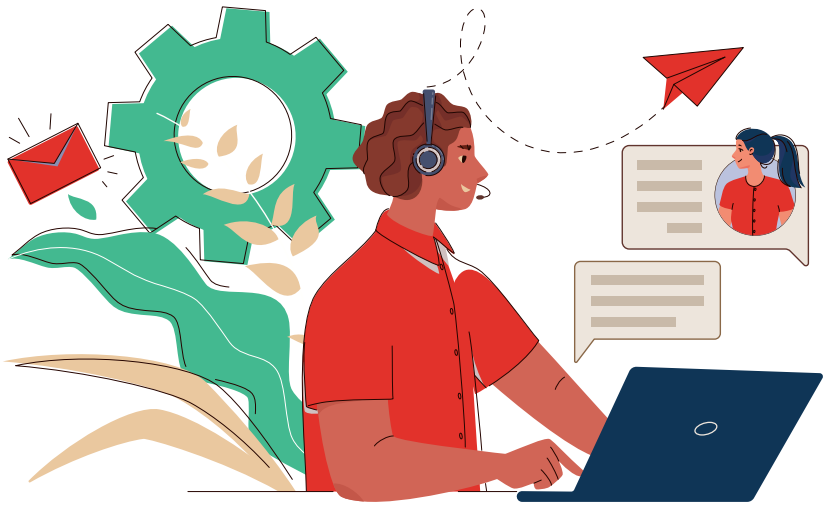


Limit

DATASTREAM
CYBER INSURANCE

# CLAIM EXAMPLE

## SOCIAL ENGINEERING



## SITUATION

An executive assistant received an email from the CEO claiming they had forgotten to pay one of their vendors, and urgently needed to pay the $80,000 bill. The assistant wired the money immediately. A few hours later, the assistant spoke to the CEO in the office, and they realized they had been tricked.

## OUTCOME

Thankfully, the company had **Social Engineering** coverage. They filed a claim with the insurance carrier straight away. After a review of the incident, the insurance carrier activated the policy and indemnified the company for its loss.

SAVINGS:
97%

Loss:
**$80,000**

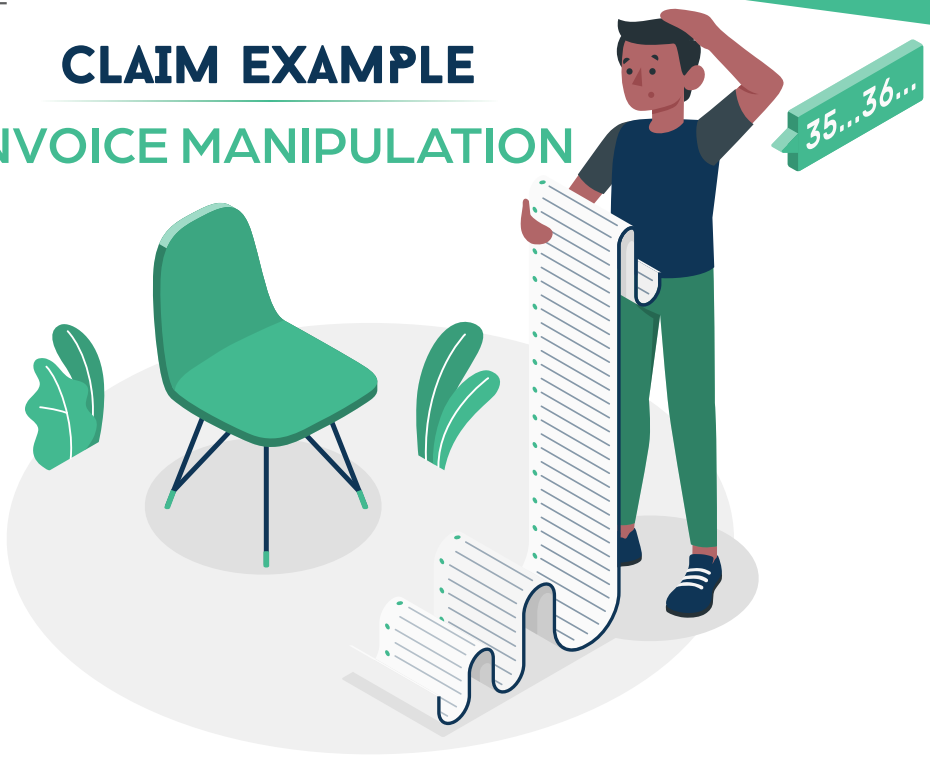
Paid by the company:
**$2,500 (retention)**

Paid by the insurer:
**$77,500**

DATASTREAM
CYBER INSURANCE

# CLAIM EXAMPLE

## INVOICE MANIPULATION




## SITUATION

Hackers broke into a law firm's invoice management system. They updated payment instructions such that the hackers would start receiving customer wires intended for the lawyers. A week later, the lawyers noticed they were missing $140,000 in client payments.

## OUTCOME

Thankfully, the lawyers had **invoice manipulation** coverage. Their insurance carrier immediately assigned a security response team to the case. After carefully tracking the funds transfers and contacting the relevant financial institutions, the team was able to recover $45,000 and the carrier stepped in to cover the rest.

SAVINGS:

96%

Loss:

**$140,000**

Paid by the company:

**$5,000 (retention)**

Recovered by the insurer:

**$45,000**

Paid by the insurer:

**$90,000**

DATASTREAM
CYBER INSURANCE

# GLOSSARY

## Aggregate Limit

The maximum total amount a carrier will pay for all claims during the policy period.

**Example:** if you have a one-year policy with an aggregate limit of $1M, and you have a claim for $500K and a claim for $750K in the same year, then the insurer will cover $1M in losses. You will have to cover the remaining $250K in losses.

## Breach Response

Coverage for notification costs, forensic costs, legal expenses, and crisis management in the event of a data security or privacy breach.

**Example:** your database containing customer payment information gets breached. The insurer will pay for security forensics of the breach, and for notifying affected customers about the breach.

## Breach Costs Inside or Outside the Limit

**Inside:** covered costs associated with recovering a breach count against the policy's aggregate limit.

**Outside:** covered costs associated with recovering a breach do not count against the policy's aggregate limit.

**Example:** you have a policy with an aggregate limit of $1M. One day, you suffer a data breach, and your insurer spends $50,000 on notifying customers about their breached data, as required by law. If your policy's breach costs are inside the limit, then you have $950K of coverage remaining. If your breach costs are outside the limit, then you still have $1M of coverage remaining.

## Bricking

Coverage for costs to replace hardware if it becomes unusable due to a cyber event. (Useless hardware may be colloquially referred to a "brick".)

**Example:** a virus breaks your computer. The insurer will pay to replace it.

# GLOSSARY

## Business Interruption

Coverage for lost revenues or expenses incurred due to an interruption or outage of an insured's systems caused by a cyber security breach. This coverage usually has a **waiting period** of downtime that you must endure before you are allowed to file a claim, and an **indemnity period** that is the longest amount of downtime that will be covered.

**Example:** you have business interruption coverage with a four-hour waiting period. A cyber attack leaves important servers offline, so you cannot do sales during that time. The insurer will cover both the revenues lost due to downtime after four hours, and the costs to put the servers back online

## Carrier

Also known as the **insurer**, this is a company that issues an insurance policy.

## Claim

A request from an insured to a carrier for indemnification of losses due to an  event covered by an insurance policy.

## Contingency

Also known as a **subjectivity**, this is a requirement that must be fulfilled by the insured to be crvered by the policy.

## Contingent Business Interruption

Coverage for lost revenues or costs due to Business Interruption as a consequence of third parties suffering outages that prevent the insured from generating revenue or operating normally.

**Example:** the vendor managing your IT system has downtime due to a cyber attack. Consequently, you cannot process new sales. Your insurer will reimburse you for those lost revenues.

# GLOSSARY

## Endorsement

An amendment added to an insurance policy that changes some of its terms.

## Insured

The party that is insured by an insurance policy. A policy may have many insureds.

## Indemnification

The act of restoring an insured to their original financial position prior to a loss covered by a policy. It makes the insured whole for damages incurred.

## Invoice Manipulation

Coverage for losses due to customer invoices being fraudulently sent or modified.

**Example:** a criminal gains access to an employee's email account, and sends a legitimate-seeming invoice to one of your customers. The customer pays the invoice to the criminal, while your company does not get paid. The insurer will cover the net financial loss to you.

## Network Security and Privacy Liability

Coverage for expenses incurred in an alleged privacy or data breach, such as remediation and defense/damages in the event of litigation due to the breach.

**Example:** your customer database is breached and your customers' passwords are leaked. A customer consequently suffers damage and sues you. The insurer would cover the costs of your litigation defense.

## Media Liability

Coverage for damages due to the publication of media material (text, sounds, images, etc.) that results in allegations of defamation, slander, trademark or copyright infringement, etc.

**Example:** your company changes its logo. Another company alleges that your new logo infringes on their trademarked logo. The insurer would cover any legal costs in defending your new logo.

# GLOSSARY

## Payment Card Industry ("PCI") Liability

Also known as **Data Security Standard ("DSS")**, this is coverage for losses (defense costs and corresponding fines and penalties) due to any alleged or actual noncompliance with PCI security standards.

**Example:** your company accidentally stores some customer credit card numbers in an insecure way. Those numbers become leaked to the public, and some customers suffer damages. The insurer would cover those damages, as well as any additional fines that are assessed.

## Policy Period

Also known as the **term**, this is the time period for which the policy is active. Losses incurred while the policy is active may be submitted as claims. The term begins on the "effective date" and ends on the "expiration date."

## Policyholder

The owner of the insurance policy. Usually, the policyholder is also the insured under the policy.

## Premium

The amount an insured must pay an insurer to be covered by a policy.

## Regulatory Liability

Coverage for legal defense and civil fines or monetary penalties that an insured may be required to pay if investigated by a regulatory authority following a cyber event.

**Example:** your customers' sensitive data is leaked to the public. A government agency investigates you to assess if you have complied with all applicable privacy/data storage requirements. They find that you have not, and you are fined. The insurer would cover any legal defense costs, as well as the fine.

DATASTREAM
CYBER INSURANCE

# GLOSSARY

## Reputational Harm

Coverage for lost revenues or expenses incurred due to an adverse media event following a cyber attack.

**Example:** your corporate LinkedIn is taken over by a hacker and defaced with offensive messages. The insurer would pay for a public relations firm to remedy the situation, and for any lost revenues if sales decrease because of the defacement.

## Retention

The amount an insured must pay toward any loss before the insurer begins providing coverage under a policy. (This is like a deductible, except that retentions do not decrease the limit of coverage available.)

**Example:** if you have a one-year policy with a $1M aggregate limit and a $5K retention, and you have a claim for $700K, then you are paying $5K out of pocket, and the insurer is providing $695K of coverage. There remains $305K of aggregate limit that the insurer would have to pay toward any other claims that year.

## Social Engineering

Coverage for losses due to criminals deceiving the insureds' employees into taking damaging actions, such as initiating payments to fraudulent actors.

**Example:** an employee wires a vendor after receiving an urgent email from the CEO about payment being overdue. It turns out that the email was not from the CEO but from an impersonator. The insurer will cover the loss.

# GLOSSARY

## Sublimit

The maximum total amount a carrier will pay for a specific type of loss under the terms of the policy. Sublimits for some individual coverages may be lower than the aggregate limit.

**Example:** if you have a one-year policy with a $1M aggregate limit and a $250K sublimit on the bodily injury coverage, and you have a claim for $100K in a bodily injury event and a claim for $400K in another bodily injury event, then the insurer would only provide $250K of coverage.

## Surplus Line

An insurance product that is not "admitted" with the department of insurance in the state in which it is being sold. A surplus lines product may only be sold by a licensed surplus lines broker.

Any insurance quotes on GetCyber are provided by an insurance broker licensed for surplus lines in all 50 states and the District of Columbia.

## System Failure

Coverage for lost revenues or expenses incurred due to an outage of an insured's systems for any reason (not limited to cyber security breaches).

**Example:** a software update for employee workstations malfunctions, and those workstations are rendered unusable for a day. The insurer may cover costs of restoring the workstations, and any losses due to these employees being unable to perform work for that day.