



Broking Manager Cyber Risk Analysis Report

v4

About CyberCube

CyberCube delivers world-leading cyber risk analytics for the insurance industry to empower data-driven decision making.

Broking Manager: Cyber Risk

Broking Manager is a cyber risk analytics solution that helps brokers and their clients make risk transfer decisions based on their unique cyber risk exposures. This report will specifically help you:

- Quantify your financial exposure
- Evaluate risk transfer strategies
- Make informed insurance coverage & limit decisions
- Identify key areas of exposure across multiple cyber scenarios in comparison to your peer group

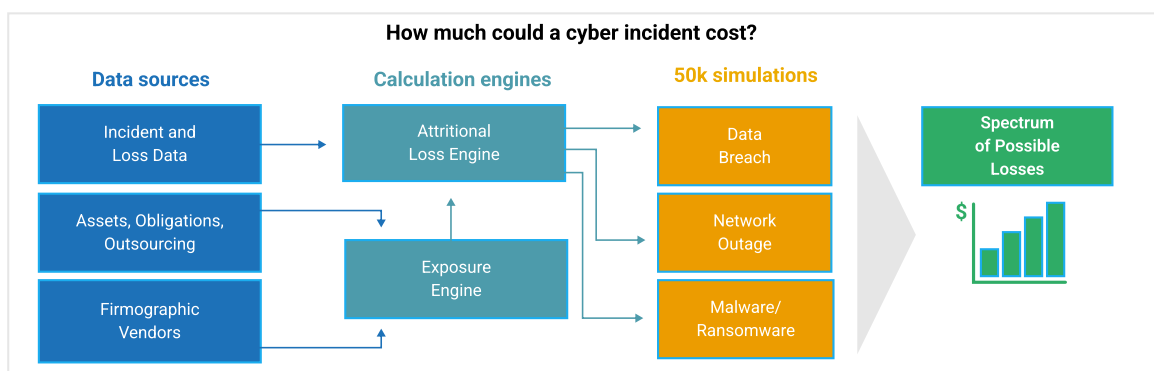
Quantify Financial Exposure

If you experience a cyber incident, how much could it cost your organization?

Broking Manager's Financial Loss model draws upon:

- A variety of cyber incident and loss data sources
- Firmographic data
- Cybersecurity assessment responses

The cyber losses shown assumes a company has experienced a cyber incident. The Attritional Loss Engine then runs 50,000 simulations each for Data Breach, Network Outage, and Malware/Ransomware events and sees what the losses could be. It's like seeing 50,000 different loss possibilities. The overall possible losses of these 3 main event types can be used to assess a company's potential financial exposure, and thereby select cyber insurance limits.



Evaluate risk transfer strategies

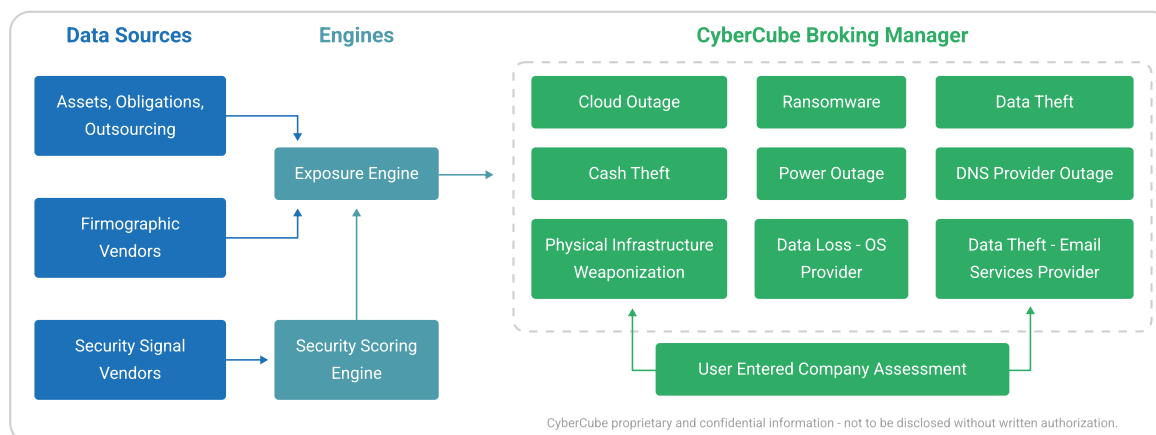
Broking Manager's Risk Transfer Benchmarking feature enables you to compare your risk transfer strategy relative to your peer group:

- Traditional limits comparison does not take into account an individual company's operations, budgets, risk tolerance, or other unique risk factors.
- Using the Financial Model, you can see how much risk you've transferred by seeing what your limits map to on the Aggregate Severity Distribution chart.
- Averaging what peers purchase in limits and calculating the level of risk transferred allows for an apples to apples comparison of risk strategies.

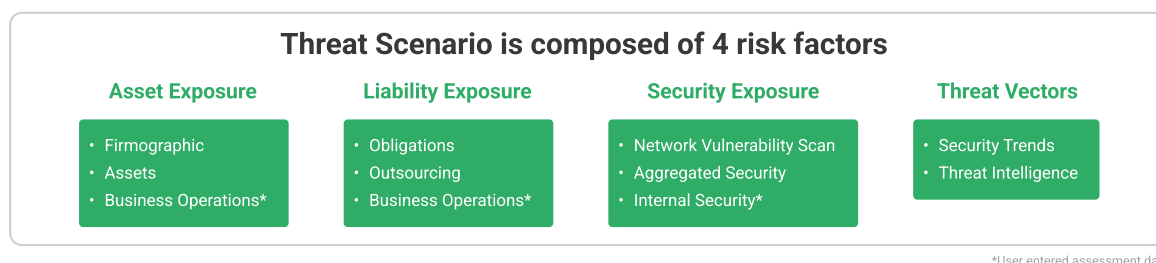
The feature is built off tens of thousands of companies' total limits information from CyberCube's proprietary data partners. Each peer group will typically have tens of companies at least.

Identify your exposure to various cyber scenarios

Where does your organization have exposure and how does that exposure compare to others?



- The Threat Model displays exposure for each threat based on percentile rankings. The percentiles show how exposed the company is relative to others to a specific threat scenario.
 - For example, if a company is in the 14th percentile compared to their peers, 14% of companies within the same peer group are less exposed than the company to a given threat.
 - The peer group comparison is the company vs industry in the pre-assessment view and the company vs industry and size in the post-assessment view.
- Exposure based on both your inherent and controllable exposure.
- Drawing upon firmographic information, external scan telemetry, aggregated internal security data and user entered assessment responses
- Compare your exposure to your peers and those in your broader industry.
- Understand which factors contribute to your overall exposure to a given threat.



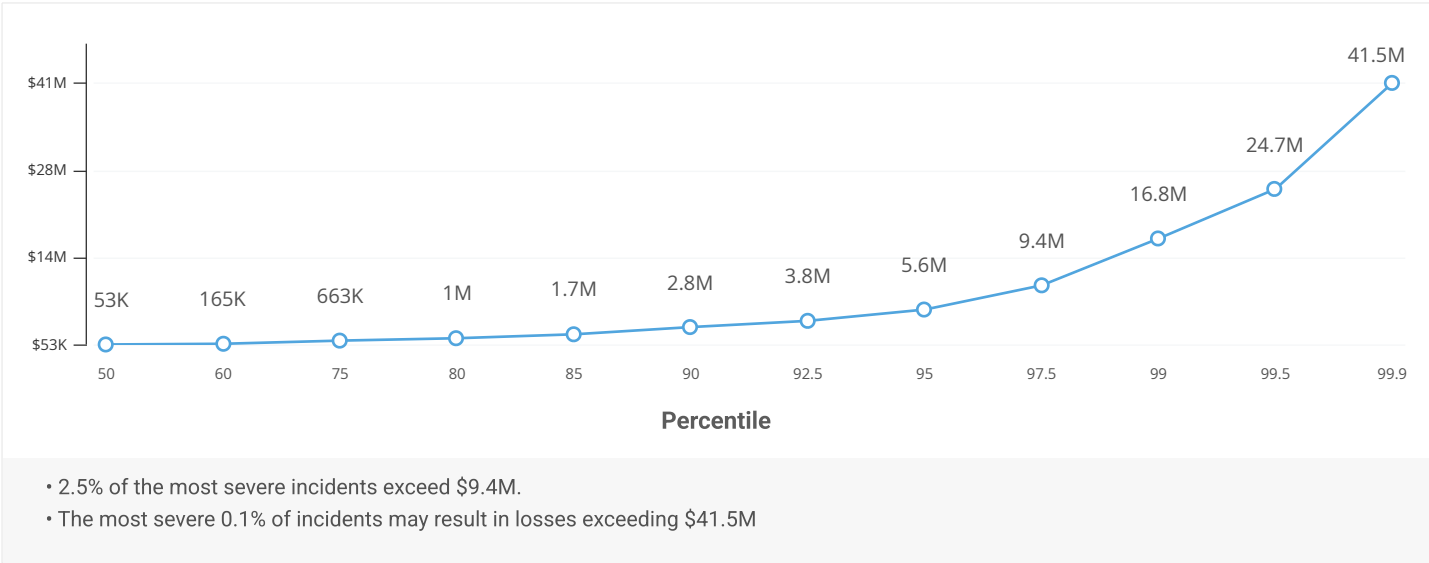
- Four (4) risk factors contribute to each threat scenario, which are dynamic and change for each threat scenario. To comprise and calculate each of these 4 contributing risk factors, our analytics model relies upon data gathered from a multitude of security signal vendors, firmographic information, and company assessment responses.
 - Security Exposures
 - Assets Exposures and Liabilities Exposures
 - Threat Vectors

ASSESSMENT STATUS	SECURITY ASSESSMENT	BUSINESS ASSESSMENT	INDUSTRY
Updated	13 of 15 answered	9 of 9 answered	Retail
REGION	SIZE	REVENUE	
US	Small	\$170M	

Aggregate Financial Exposure

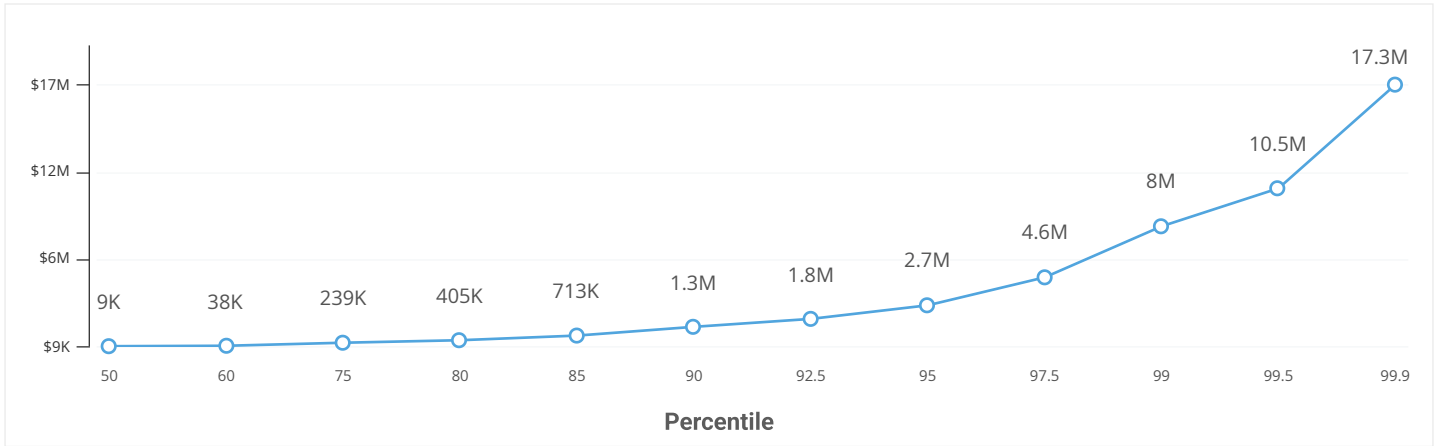
Aggregate Severity Distribution

The Aggregate Severity Distribution represents the potential losses a company may experience given a cyber incident. It is based on modeling and running 50K simulations about this company and ranking the incidents by estimated loss.



Data Breach

Data Breach - Severity Distribution



Potential Triggered Losses

- Investigation & Response Costs

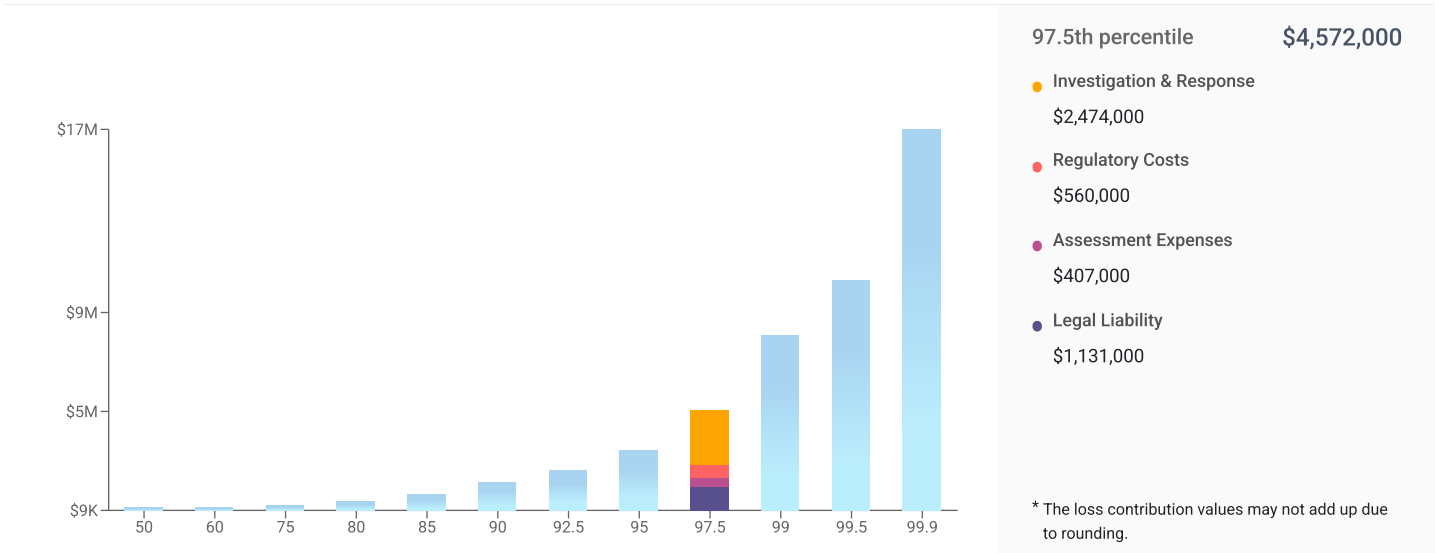
 - Forensic IT Investigation
 - Notification Costs
 - Breach Coach / Legal
 - PR Firm Costs
 - Call Center Costs
 - Reputational Loss
- Legal Liability

 - Defense Costs
 - Legal Damages
 - Legal Settlements
- Assessment Expenses

 - Credit Monitoring Costs
 - Payment Card Assessments
- Regulatory Costs

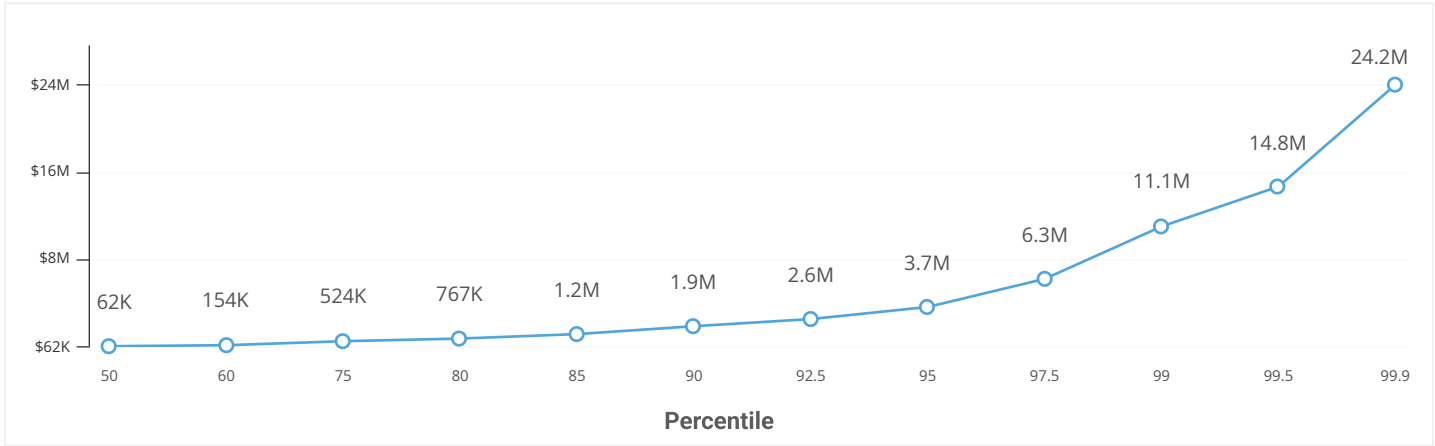
 - Payment Card Industry
 - Regulatory Proceeding

Data Breach - Loss Contributions



Network Outage

Network Outage - Severity Distribution



Potential Triggered Losses

Investigation & Response Costs

- Forensic IT Investigation
- Notification Costs
- Breach Coach / Legal
- PR Firm Costs
- Call Center Costs
- Reputational Loss

Business Interruption

- Business Income Loss
- Contingent Business Income Loss
- System Failure Income Loss
- Contingent System Failure Income Loss
- Extra Expense
- Reputational Loss

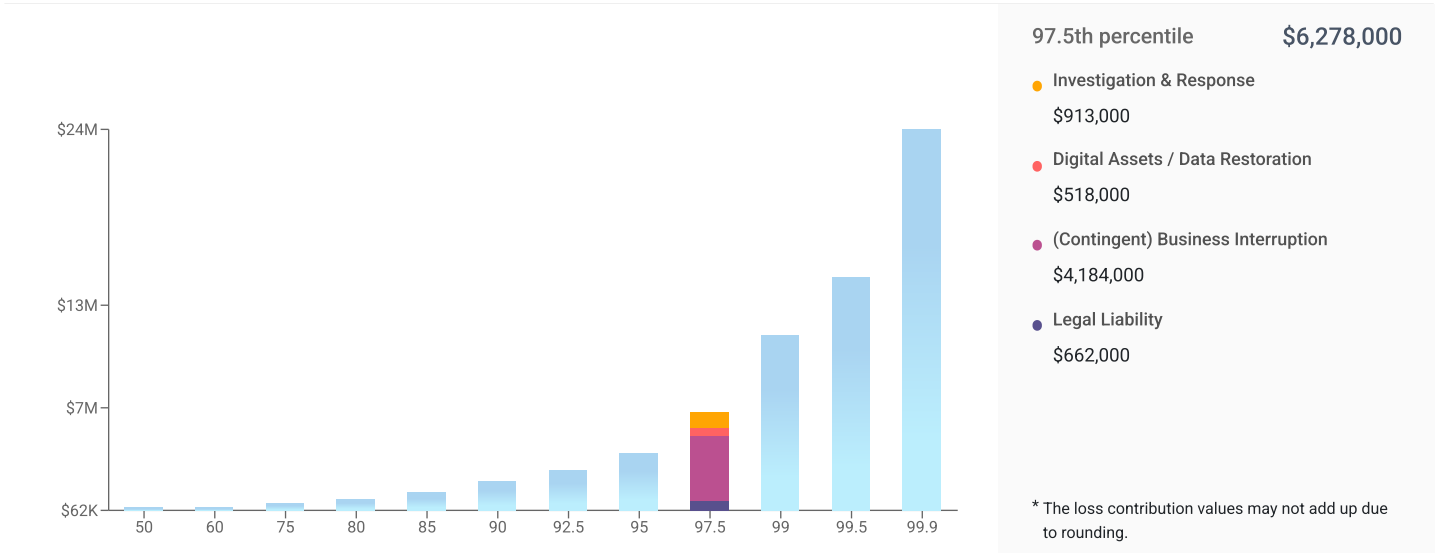
Legal Liability

- Defense Costs
- Legal Damages
- Legal Settlements

Digital Assets and Data Restoration

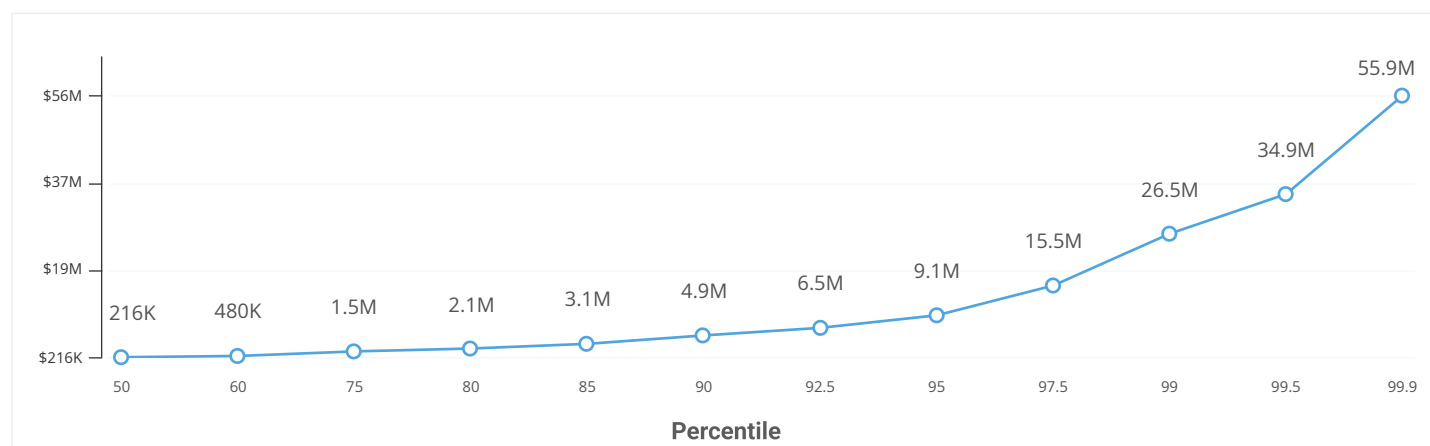
- Data Restoration and Re-creation
- System Replacement Costs/Bricking

Network Outage - Loss Contributions



Malware/Ransomware

Malware/Ransomware - Severity Distribution



Potential Triggered Losses

Investigation & Response Costs

- Forensic IT Investigation
- Notification Costs
- Breach Coach / Legal
- PR Firm Costs
- Call Center Costs
- Extortion Payments
- Reputational Loss

Assessment Expenses

- Credit Monitoring Costs
- Payment Card Assessments

Business Interruption

- Business Income Loss
- Contingent Business Income Loss
- System Failure Income Loss
- Contingent System Failure Income Loss
- Extra Expense
- Reputational Loss

Digital Assets and Data Restoration

- Data Restoration and Re-creation
- System Replacement Costs/Bricking

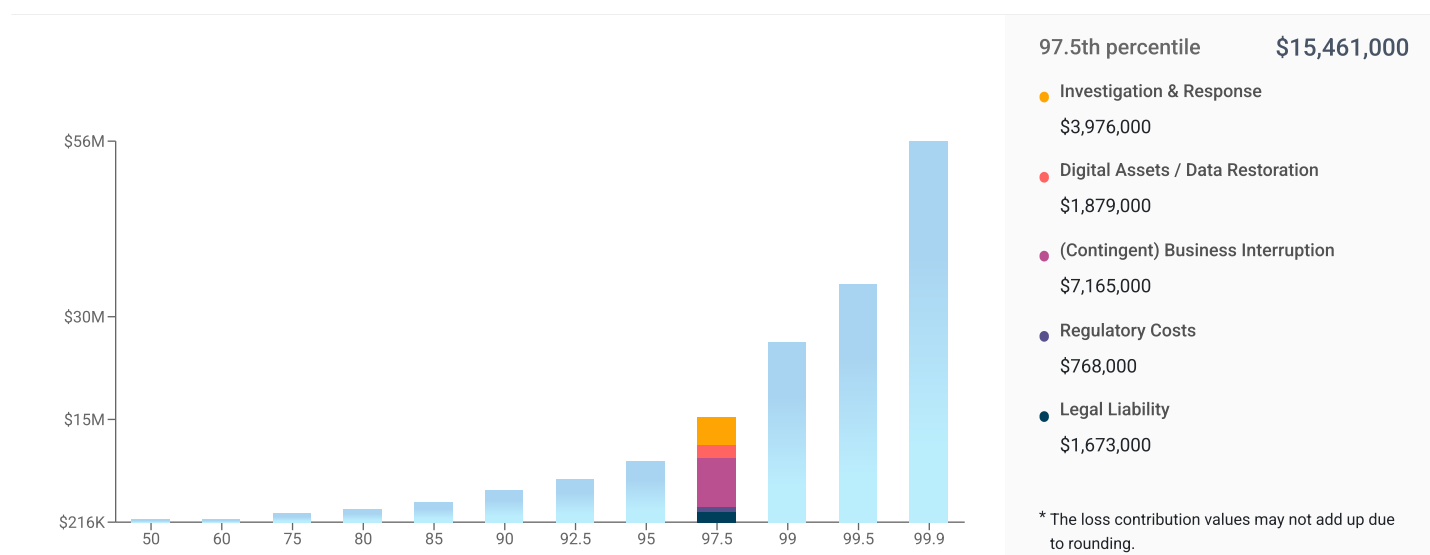
Legal Liability

- Defense Costs
- Legal Damages
- Legal Settlements

Regulatory Costs

- Payment Card Industry
- Regulatory Proceeding

Malware/Ransomware - Loss Contributions



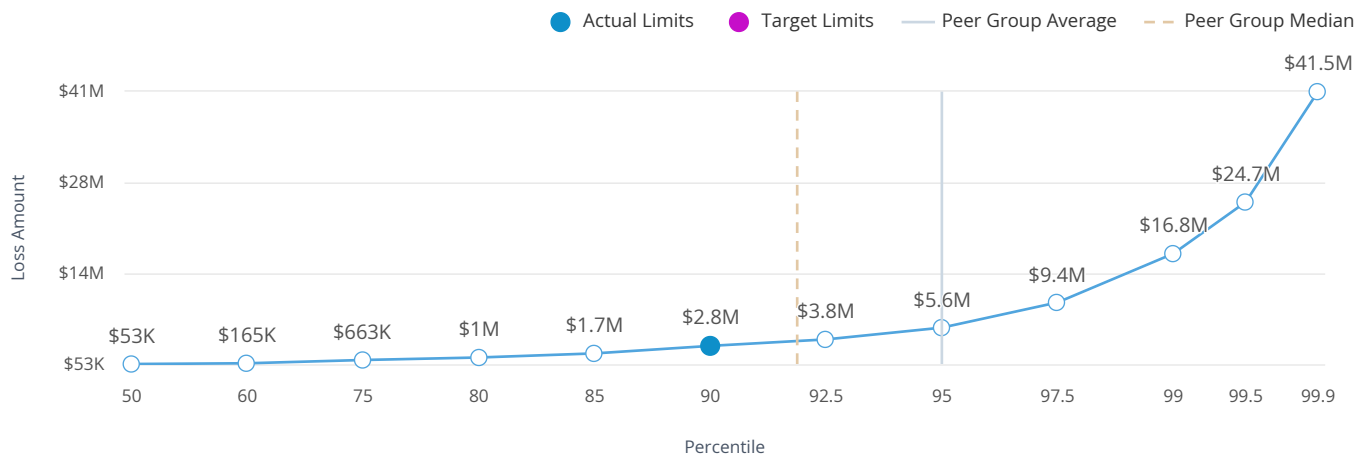
Risk Transfer Benchmarking

Your Actual Limits
\$3,000,000

Your Target Limits
N/A

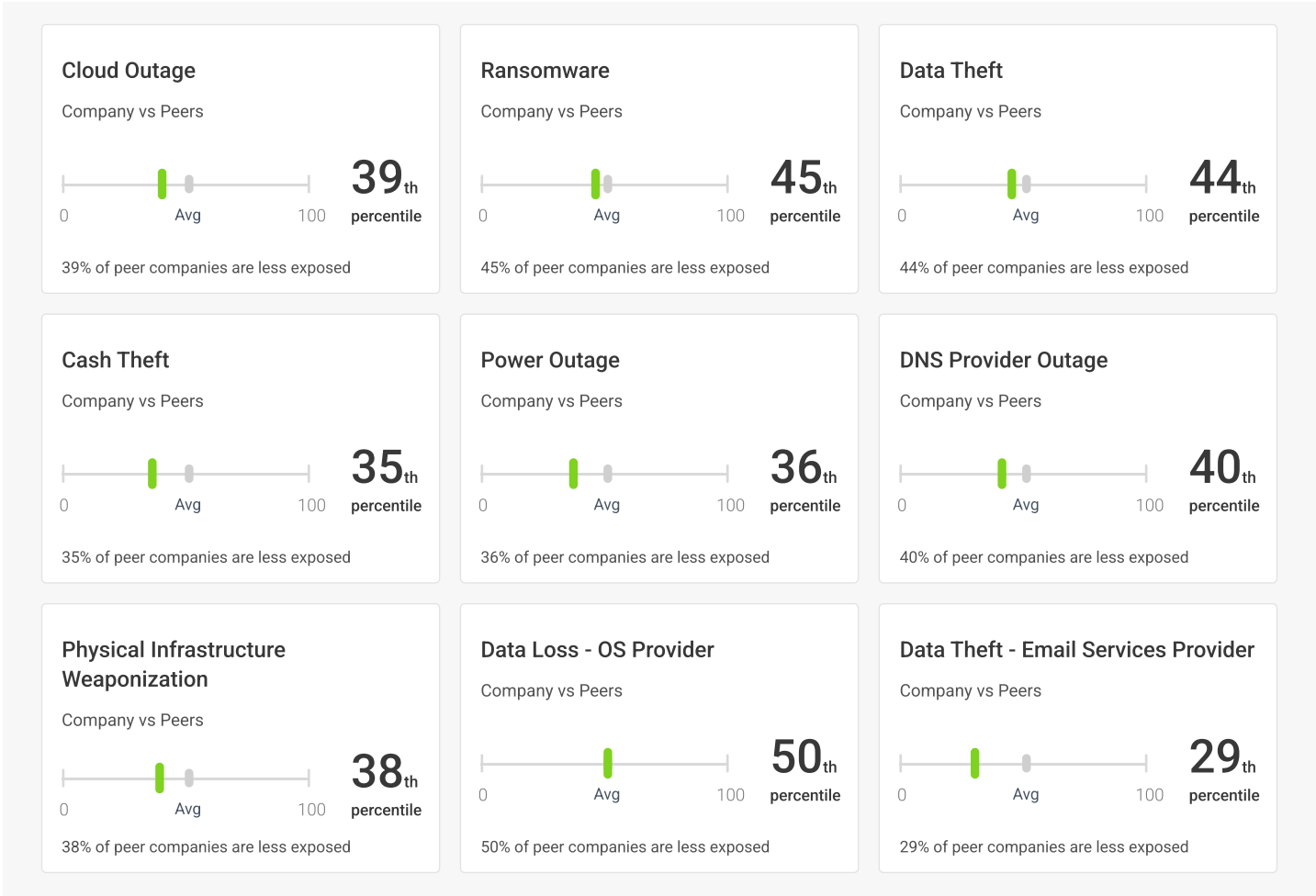
Peer Group Average Comparison (for Aggregate Severity Distribution)

PEER GROUP INFO
Retail | Small : (10M–250M) | more, than 100 Peers



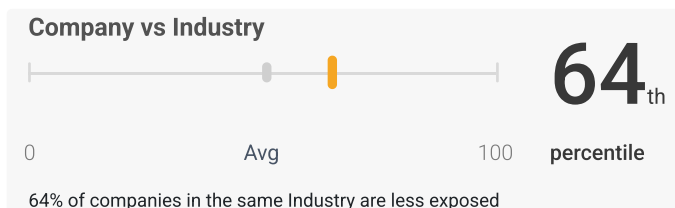
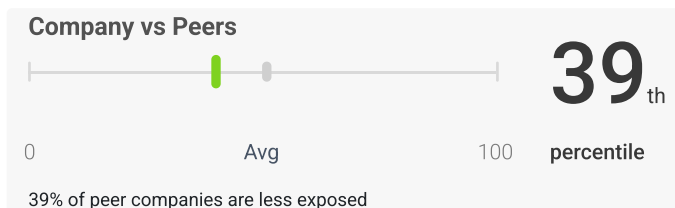
	Risk Transfer Percentile	Meaning
Your Actual Limits	90 th \$3M	Your Company's limits are transferring financial risk for 90% of simulated cyber losses.
Your Target Limits	N/A	Missing
Peer Group Average	95 th \$5.6M	Your peer group (mean) average limits is transferring financial risk for 95% of simulated cyber losses. Your equivalent limits at this peer percentile
Peer Group Median	92 nd \$3.6M	The peer median company is transferring financial risk for 92% of simulated cyber losses. Your equivalent limits at this peer percentile

Peers: Small (\$10M–\$250M), Retail
Industry: Retail



Cloud Outage Threat Factor

Cloud Outage occurs when a Cloud service provider used becomes unavailable for variety of possible reasons, including user error, actor attacks, or an indeterminate caused outage



Asset Exposure ⓘ above average

- Trade Secrets Risk
- Outsourcing Risk
- Dependencies Risk
- Revenues Risk

Liability Exposure ⓘ average

- Contractual liability
- Fiduciary liability
- Legal liability

Security Exposure ⓘ below average

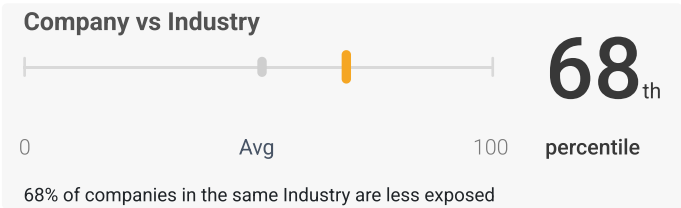
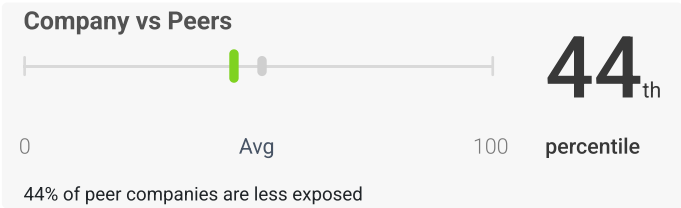
- Vendor Security
- Employee Training
- Resiliency
- Risk Assessment

Threat Vectors ⓘ high

- Threat actors risk
- Trending methods risk
- Resources of Active Actors

Data Theft Threat Factor

Data Theft occurs when a threat actor steals confidential data from an enterprise. This data may contain but is not limited to trade secrets, intellectual property, PII, PCI, or PHI



Asset Exposure ⓘ above average

- Records stored risk
- Trade Secrets Risk
- Employee Exposure Risk
- Revenues Risk

Liability Exposure ⓘ average

- Contractual liability
- Fiduciary liability
- Legal liability

Security Exposure ⓘ average

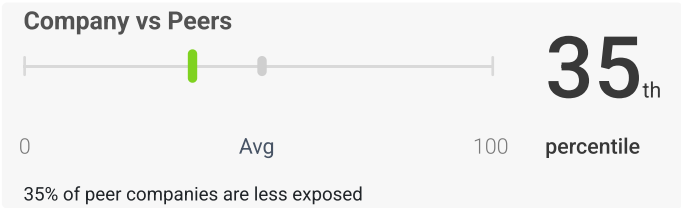
- Network security
- Vulnerability management
- Logging & Monitoring

Threat Vectors ⓘ below average

- Threat actors risk
- Trending methods risk
- Resources of Active Actors

Cash Theft Threat Factor

Cash Theft typically occurs when a threat actor steals an enterprise's funds following an exploitation of enterprise security or social engineering



Asset Exposure ⓘ

above average

- Employee exposure risk
- Outsourcing Risk
- Revenues Risk

Liability Exposure ⓘ

average

- Contractual liability
- Fiduciary liability
- Legal liability

Security Exposure ⓘ

below average

- Network security
- Vendor Security
- Logging and Monitoring
- Risk Assessment

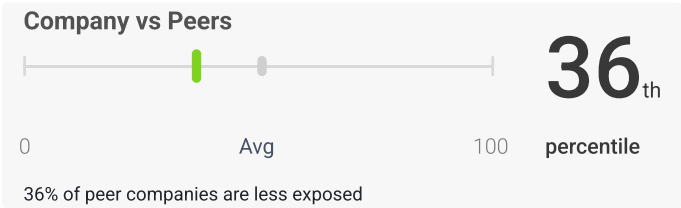
Threat Vectors ⓘ

above average

- Threat actors risk
- Trending methods risk
- Resources of Active Actors

Power Outage Threat Factor

Power Outage may occur when a threat actor causes long-lasting power outage that impacts an enterprise capabilities or services



Asset Exposure ⓘ

above average

- Employee exposure risk
- Physical Sites Risk
- Dependencies Risk
- Revenues Risk

Liability Exposure ⓘ

average

- Contractual liability
- Fiduciary liability
- Legal liability

Security Exposure ⓘ

average

- Logging and Monitoring
- Resiliency
- Risk Assessment

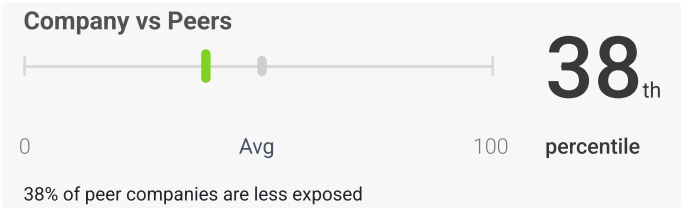
Threat Vectors ⓘ

average

- Threat actors risk
- Trending methods risk
- Resources of Active Actors

Physical Infrastructure Weaponization Threat Factor

Physical Infrastructure Weaponization a threat actor may execute digital takeover of physical infrastructure to cause physical damage or harm



Asset Exposure ⓘ

above average

- Employee Exposure Risk
- Physical Sites Risk
- Outsourcing Risk
- Dependencies Risk

Liability Exposure ⓘ

average

- Contractual liability
- Fiduciary liability
- Legal liability

Security Exposure ⓘ

average

- Network security
- Configuration Management
- Vulnerability Management
- Logging and Monitoring

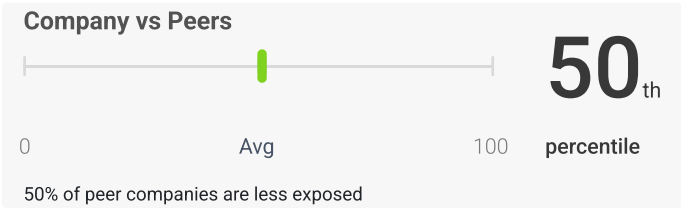
Threat Vectors ⓘ

below average

- Threat actors risk
- Trending methods risk
- Resources of Active Actors

Data Loss - OS Provider Threat Factor

Data Loss - OS Provider - Widespread exploit of vulnerability in a leading operating system which causes data loss/destruction and system outages at enterprise customers



Asset Exposure ⓘ above average

- Records stored risk
- Employee Exposure Risk
- Outsourcing Risk
- Dependencies Risk

Liability Exposure ⓘ average

- Contractual liability
- Fiduciary liability
- Legal liability

Security Exposure ⓘ average

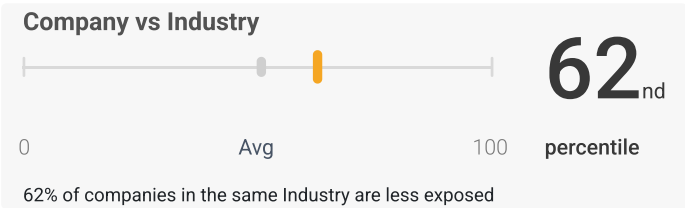
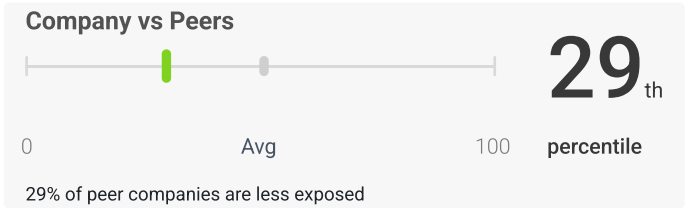
- Network security
- Configuration Management
- Vulnerability Management
- Resiliency

Threat Vectors ⓘ low

- Threat actors risk
- Trending methods risk
- Resources of Active Actors

Data Theft - Email Services Provider Threat Factor

Data Theft - Email Services Provider - Large scale phishing campaign impacting an enterprise email service provider, which ultimate results in enterprise email compromise



Asset Exposure ⓘ

above average

- Records Stored Risk
- Trade Secrets Risk
- Employee Exposure Risk
- Outsourcing Risk

Security Exposure ⓘ

below average

- Network Security
- Employee Training
- Logging and Monitoring
- Risk Assessment

Liability Exposure ⓘ

average

- Contractual liability
- Fiduciary liability
- Legal liability

Threat Vectors ⓘ

below average

- Threat actors risk
- Trending methods risk
- Resources of Active Actors

Disclaimer

This report is provided for general information purposes only and does not constitute legal or professional advice. This report is generated using CyberCube's proprietary cyber analytics technology and at times, data input from the Client and Recipient. As the analyses in the report are dependent on variable factors such as data quality, emerging threats and other factors that are outside CyberCube's control, this report may not represent a whole of the Recipient's cyber risk assessment and is provided on an "as is basis" without any representation or warranties. The Recipient shall be solely responsible and liable for all decisions made pertaining to the use of the report and the information contained within. No Recipient should act on the basis of any material contained herein without obtaining proper legal or other professional advice specific to their situation. No liability is accepted by CyberCube or Client for any loss or damages suffered arising from or in connection with the report, or for any error or omission, or deficiency contained in the report. This report is proprietary to CyberCube. "CyberCube" means CyberCube Analytics Inc. and its affiliates. "Client" means a licensee of Broking Manager which is CyberCube's proprietary analytics technology. "Recipient" means the subject company of the report.
