FIFTHWALL
SOLUTIONS

CYBER LIABILTY REVIEW

to Optimize Risk Management

1 Heat Map

Identify where your sector is most susceptible to the three most common exposures.

2 Loss Estimate

Quantify the true cost of ransomware between 5 and 60 days in the dark for a business of your size and sector.

3 Industry Specific Education

Learn about specific claims scenarios within your sector.

Identify Exposures

4 Policy Review

Learn how your current policy stacks up with your industry exposures according to the Heat Map and Loss Quantification.

5 Gap Analysis

Review your deployed security controls and roadmap a path to deploy needed security controls.

Roadmap & Deploy Risk Management

6 Price Benchmarking

Compare your current and potential coverage options with current pricing in the market to ensure best rates.

7 Carrier Market Access

Leverage our 40+ carriers to get best-in-class quotes based on your unique risk profile

Secure Top Cyber Coverage

Start a conversation today at www.fifthwallsolutions.com

Powered by
FIFTHWALL
SOLUTIONS
CYBER INSURANCE SIMPLIFIED

© FifthWall Solutions, 2023, All Rights Reserved.

Disclaimer: Listed services are in beta testing. Consulting and/or brokerage fees may apply.

FIFTHWALL SOLUTIONS

HEAT MAP

Let's explore your organization's exposures unique to your industry. No matter how unique your industry may be, you'll find several examples that will hit close to home In at least one of the three most common cyber exposure categories: Ransomware/Business Interruption, Third-Party Liability, and Funds Transfer Fraud.

	Funds Transfer Fraud	Third-Party Liability	Ransomware/ Business Interruption
Schools	A cybercriminal gains access to your finance department's email accounts and manipulates tuition payment instructions, causing legitimate payments to be redirected to fraudulent accounts.	A security vulnerability in your faculty email system allows cybercriminals to access confidential student data, including academic records and test scores. You must inform parents, manage inquiries, and deal with potential legal and privacy-related actions.	
Technology		A security breach in your cloud storage services results in the theft of sensitive client data, such as proprietary code and intellectual property. You are held responsible for the breach, facing potential legal actions and regulatory penalties.	
Retail		A data breach exposes personal info of your online customers, including names, email addresses, and credit card numbers. You not only incur costs to notify affected individuals, but also face regulatory fines and penalties.	A ransomware attack encrypts your point-of-sale (POS) system, making it impossible to process sales or accept payments in-store, resulting in revenue losses and a decline in customer trust.
Professional Services	Your business falls victim to Business Email Compromise where an attacker poses as one of your top executives, instructing a finance team member to make a significant payment to a fraudulent account under the pretense of a confidential transaction.		
Construction	An attacker impersonates a trusted supplier and manipulates payment instructions, leading to fraudulent payments that result In significant financial losses.	A cyberattack on your project management software compromises critical project data and schedules. As a result, you face delays and additional costs due to the need to recover and rebuild project plans.	
Manufacturers	A cybercriminal infiltrates your email system and manipulates the wire transfer instructions between you and your overseas supplier, resulting in a fraudulent payment to the wrong account.	Your supplier's systems fall victim to a ransomware attack, disrupting the delivery of critical raw materials needed for production. This leads to production delays, increased costs, and potential reputational damage due to unfulfilled customer orders.	
Healthcare	A cybercriminal targets your scheduling software, accessing patient records, appointment histories, and contact information. This raises concerns about patient data security, leading to legal repercussions and damaged patient trust.	A ransomware attack locks down your electronic health records system. This forces you to suspend appointments, extend staff hours for manual record-keeping, and reroute patients to other facilities, affecting revenue and patient care.	
Municipalities	A cyber incident compromises your voter registration database, exposing voter details such as political affiliations and personal info. This raises concerns about election integrity, leading to legal challenges and investigations.	A cyber incident compromises the utility management systems, leading to power outages and water supply disruptions for the community. Emergency responses are enlisted, leading to interruptions and increased operational costs.	

FIFTHWALL SOLUTIONS

LOSS ESTIMATE

through Ransomware or Business Interruption

Cost over time

Based on:

- **$100M revenue**
- **Healthcare Industry**
- **> 500K records**
- **~ 200 employees**

5 DAYS
~ $3,500,000

15 DAYS
~ $6,000,000

30 DAYS
~ $9,500,000

45 DAYS
~ 12,000,000

60 DAYS
~ $16,000,000

Calculations are an approximation of a ransomware event that shuts down organization operations. The above estimate is based on historical claims data according to client revenue and sector history.

When it comes to ransomware, threat actors target businesses of every size. Ensure your business is covered with a comprehensive cyber liability policy to endure the true cost of a cyber attack and its effects.

Powered by
FIFTHWALL SOLUTIONS
CYBER INSURANCE SIMPLIFIED

FIFTHWALL SOLUTIONS

PRICE BENCHMARKING

Cyber Insurance for Healthcare

Dec 2023

Lower Range:

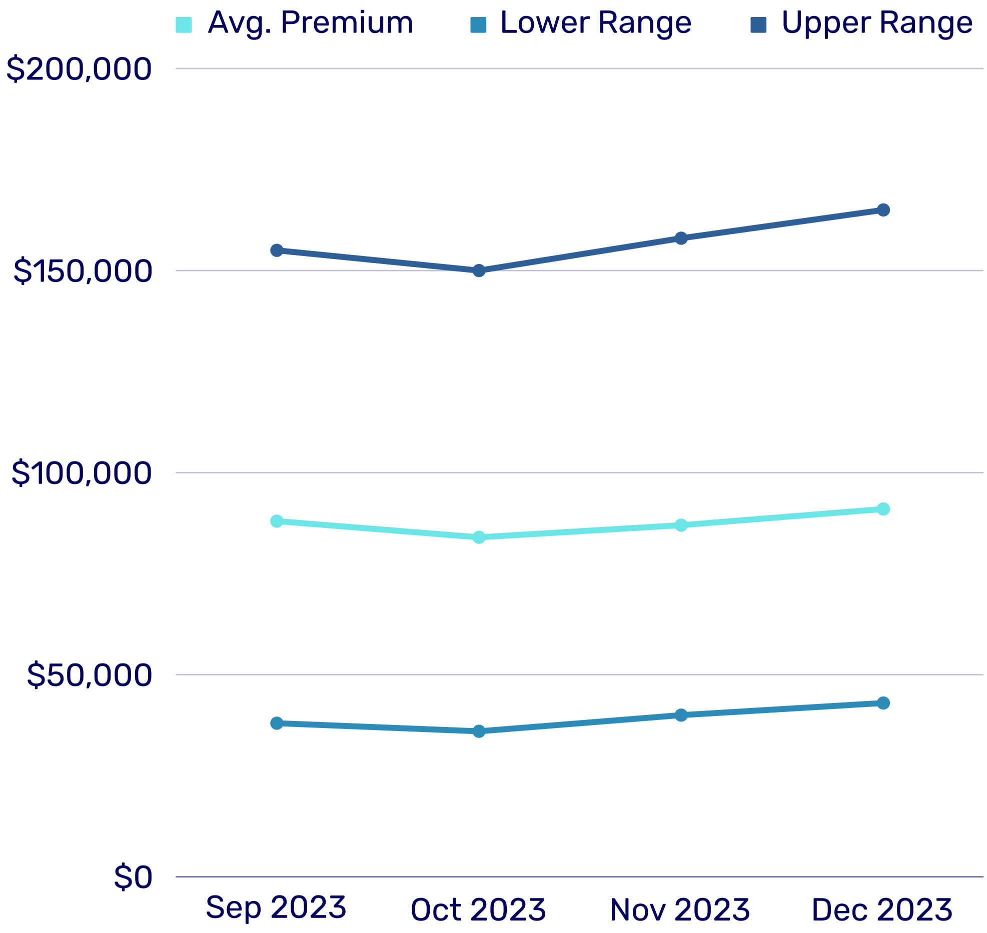
$43,000

Avg. **$91,000**

Upper Range:

$165,000

40-45% of the breaches handled at Experian, a major credit monitoring firm, are linked to healthcare.**



When purchasing insurance, actual policies should be reviewed for specific terms, conditions, limitations, and exclusions that will govern in the event of loss.

Find cyber rates today at www.fifthwallsolutions.com

**Based on $5M limits with provided revenue*

***NetDiligence*