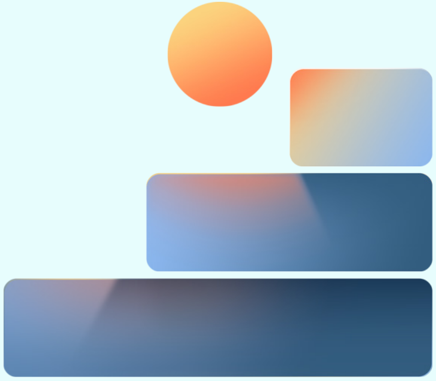
ThreatConnect Risk Quantification Report: Healthcare, Manufacturing & Utilities

Report Finds Ransomware Attacks Can Cost 30%+ of Operating Income

When talking about the cost of cyber risk, people prefer seeing headline-catching figures. A recent IBM report puts the average cost of an attack at $4.35m. However, that average attack figure takes into account a large number of incidents that cost relatively little (less than $25k) and a few that cost a lot. The question is - does the average apply to you?

Three factors must be analyzed to be able to answer that question:

- What is the cost to you as a company based on your specific operating environment?
- What comprises potential losses, and in what time-frame would the payouts occur?
- Most importantly, how can you prioritize your cyber investments to best mitigate the impact based on financial metrics?

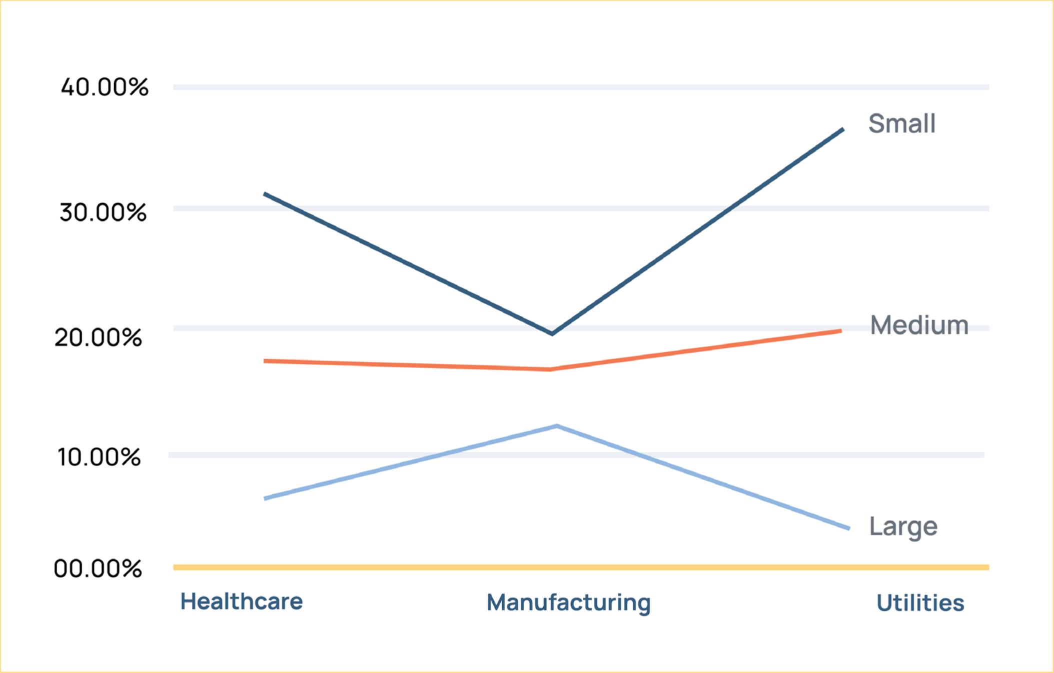


[1] https://www.ibm.com/reports/data-breach

1. A Better Way To Look At Exposure

A better way to look at the cost of a cyber attack is to look at the cost to you as a company. Cyber attack costs vary by industry and company size. The National Cyber Strategy, stemming from the Biden administration, outlines a number of approaches to protecting critical infrastructure. However, a common question still remains - What is the financial risk these industries face?

ThreatConnect examined the losses faced by small, medium, and large companies with revenues of $500MM, $1.5B, and $15B, respectively, and what the median cost of a ransomware attack would be based on past losses in their cohort using the ThreatConnect RQ product. The most interesting part of the analysis wasn't the magnitude of the impacts - it was the percentage of operating income a company could lose.



% of operating income at risk for Critical Industries based on company size

Operating income, also called income from operations, takes a company's gross income, which is equivalent to total revenue minus COGS, and subtracts all operating expenses. According to the above chart, some of the critical industries outlined in the Biden Cyber Security Strategy – Healthcare, Manufacturing, and Utilities – have an average percentage of operating income at risk as high as 30%.

The chart below displays the median - not maximum - losses a company could face in a ransomware attack. These medians are based on actuals -not theoretical scenarios - and paint a much more complete, better picture of how the impact of an attack can damage a company.

		Ransomware Losses			
Industry	Gross Revenue	Median Ransomware Loss	% of Gross Rev Lost	Estimated Operating Income	% of Estimated Operating Income Lost
Healthcare	$ 500,000,000	$ 15,286,095	3.06%	$ 49,527,375	30.86%
Healthcare	$ 1,500,000,000	$ 26,845,023	1.79%	$ 174,802,500	15.36%
Healthcare	$ 15,000,000,000	$ 101,213,365	0.67%	$ 2,056,500,000	4.92%
Manufacturing	$ 500,000,000	$ 9,775,103	1.96%	$ 44,289,250	22.07%
Manufacturing	$ 1,500,000,000	$ 26,063,061	1.74%	$ 156,315,000	16.67%
Manufacturing	$ 15,000,000,000	$ 186,748,253	1.24%	$ 1,839,000,000	10.15%
Utilities	$ 500,000,000	$ 17,756,494	3.55%	$ 57,698,438	30.77%
Utilities	$ 1,500,000,000	$ 30,271,999	2.02%	$ 230,793,750	13.12%
Utilities	$ 15,000,000,000	$ 67,454,000	0.45%	$ 3,077,250,000	2.19%

Financial Analysis of Ransomware attacks against gross revenue and operating income

Ultimately, when you are evaluating your financial exposure to cyber attacks, make sure to utilize a number that matches your business based on industry and size instead of only using the industry average.

2. What Type Of Loss Are We Talking About?

Average numbers don't always tell the complete story. Ransomware attacks tend to cause operational disruptions for your business. This means you won't be able to manufacture products, order materials, or operate your business. Those kinds of disruptions directly impact your gross revenue, which is a key measurement of the health of a company.

The table below shows the top types of loss a company would typically face due to a ransomware attack.

		Top Types of Loss	
Industry	Gross Revenue	Revenue	Remediation
Healthcare Small Organization	$ 500,000,000	$ 8,915,984	$ 5,445,111
Healthcare Medium Organization	$ 1,500,000,000	$ 16,063,640	$ 8,771,080
Healthcare Large Organization	$ 15,000,000,000	$ 72,484,936	$ 23,830,930
Manufacturing Small Organization	$ 500,000,000	$ 5,258,245	$ 3,747,858
Manufacturing Medium Organization	$ 1,500,000,000	$ 10,214,747	$ 9,149,315
Manufacturing Large Organization	$ 15,000,000,000	$ 118,219,152	$ 62,862,042
Utilities Small Organization	$ 500,000,000	$ 9,262,336	$ 3,845,168
Utilities Medium Organization	$ 1,500,000,000	$ 15,000,000	$ 6,076,000
Utilities Large Organization	$ 15,000,000,000	$ 42,000,000	$ 15,854,000

This table shows that revenue losses can be quite large for certain sectors - for example, the healthcare company Scripps, lost almost $91M in revenue or Maersk, which lost over $250MM in revenue. Remediation costs are the second highest cost and are increasing in frequency and cost across the industry.

Importantly, ransomware isn't the greatest risk for every industry. The healthcare industry experiences large ransomware attacks but also faces large costs due to data breaches. The greatest risks to manufacturing, for example, are ransomware attacks due to production systems being essential to the industry's operations.

Cyber risk is very business-specific, and you need to understand what type of loss you might face - revenue, remediation, legal settlement, or otherwise - in order to best plan your own strategy.

3. What Can You Do About The Risk

Three things every company should do to manage cyber risk:

- Understand the overall impact
- Identify what the key loss types are
- Prioritize their cyber investments to best mitigate the risk

The final reason an "average losses" figure can be misleading is that they don't provide any insight into how you should be mitigating your risk. Informing someone they may be at risk without providing any guidance on how to mitigate that risk is akin to saying their car might be broken into but not providing guidance on how to lock the doors.

This is an area, prioritization of cyber investments, that is still lacking in the current National Cyber Security Strategy and in most other published guidance. The investments you need to best defend your business are based on your own business.

Almost all companies have some level of cybersecurity in place today. The key to understanding how to prioritize your investments is to look at the risks to your business and your current cyber security posture. This way, you can more easily assess your risks and how you should prioritize mitigations.

As an example, we ran an analysis on a small portion of a manufacturing company's business. The table below shows which NIST CSF Controls should be improved first based on financial risk reduction. Apply the cost of the investment, and you'll have a prioritized list of cyber mitigations based on how much business value they provide.

NIST CSF		
Functions	**Categories**	**Risk Reduction**
Identify	Asset Management	$ 1,700,000
Protect	Identity Management, Authentication, and Access Control	$ 1,500,000
Protect	Protective Technology	$ 525,000
Detect	Anomalies and Events	$ 450,000

Example list of cyber investments prioritized by financial risk reduction

Summary

The purpose of this article is not to instill fear, uncertainty or doubt, but to help companies understand that your cyber risk is yours and that your risk isn't adequately represented by an "average number." The financial impact you face can be material for your business, whether it's a hit to operating income or revenue, understanding the impact - and your business - is essential.

Finally, you should be taking steps that best mitigate the risk using financial measurements. Too often, security investments are couched in technical jargon when what's needed is the ability to prioritize and invest in solutions that best mitigate financial risk.

As we've outlined in the paper, using "average" values to measure your financial exposure to cyber attacks doesn't work. Quantifying - and more importantly mitigating - cyber risk is challenging and unless you take a look at what the risk is to your environment, you run the risk of significant losses.

The good news is that there are solutions to the problem. ThreatConnect RQ was built to quantify cyber risk in financial terms based on industry data and your attack surface so that companies can see their exposure and build mitigation plans that reduce financial risk. More information on RQ and how we're changing the paradigm on cyber risk here https://threatconnect.com/risk-quantifier/

Methodology:

The data in this report was compiled using loss modeling from ThreatConnect Risk Quantifier and is based on thousands of actual losses due to cyber breaches. RQ computes two numbers: financial loss magnitude and how likely an attacker is to breach your defenses. Each computation uses different methods.

On the financial loss side, RQ uses historical data to build out loss models. Those models are built using a variety of methods, including polynomial regression and machine learning (ML) techniques. What allows us to use Machine Learning is separating the probability and loss components and effectively treating them as two separate phases of the attack. We have a large library of loss data from a variety of sources - some paid, some open source, some created in-house- which lets us build ML models using that data.

RQ computes the probability of an attacker bypassing a company's defenses by using a simplified attack pattern analysis. Attack patterns are created from analysis of past attacks mapped to the MITRE ATT&CK framework and from internal attack analysis. The main flow of the model is essentially an absorbing Markov chain, in which the states that make up the chain correspond to the details of the simulated attack. The probabilities used in the computation come from the RQ team's testing and analysis and may represent primitive actions or may use the results of submodels in order to calculate the probability of specific complex actions. The math that underpins what an attacker can do includes probabilistic methods such as Absorbing Markov Chains, Stochastic Error Functions, and Monte Carlo Simulations.

ThreatConnect.

By operationalizing threat and cyber risk intelligence, The ThreatConnect Platform changes the security operations battlefield, giving your team the advantage over the attackers. It enables you to maximize the efficacy and value of your threat intelligence and human knowledge, leveraging the native machine intelligence in the ThreatConnect Platform. Your team will maximize their impact, efficiency, and collaboration to become a proactive force in protecting the enterprise. **Learn more at www.threatconnect.com.**

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708