SAFE

Safe's CRQ Calculator

Predicting The Cyber Health of Industries Over the Next 12 Months

Authors:
Erica Eager (erica.e@safe.security)
Nimmi Sharma (nimmi.s@safe.security)
Pankaj Goyal (pankaj.g@safe.security)

www.safe.security

What problem are we trying to solve?

Humans love predicting the future. What is the probability that a team will win? What is the probability of rain tomorrow? What will my day look like?

So much so, that big industries have been built on probabilities and predictions.
What is the probability of a person repaying a mortgage?
What is the probability of a driver getting into an accident that triggers insurance?
What is the probability of a vaccine being effective?

With cybersecurity risk becoming one of the most important enterprise risks to manage, is it useful to ask, *"What is the probability of a cyber attack over the next 12 months? If an attack happens, what is the potential financial loss my company can face?"*

The answer is **yes**. If you know your weaknesses, you can fix them and prevent attacks in the future. You can build an action plan that is prioritized by quantified impact. You can decide your cyber insurance coverage. You can evaluate the ROSI (Return on Security Investments). Understanding your risk profile helps you plan ahead, and manage cyber risk proactively.

But, how do you quantify cyber risk to start this journey??

What is Safe's CRQ Calculator?

Safe's CRQ Calculator aims to quantify the cyber health of an industry based on its external threat landscape and inherent risk profile.

Outputs of the Safe's CRQ Calculator are:

1. Probability of any cyberattack occurring in the next 12 months.
2. Probability of a specific attack (such as Ransomware attack, data breach, Business Email Compromise) occurring in the next 12 months.
3. Potential financial loss due to a ransomware attack.

The above numbers are calculated at an industry-level such as healthcare, retail, or financial services. To calculate the same numbers at a company-level, we need to account for its specific attack surface environment and controls' status.

Inputs for the Safe's CRQ Calculator are:

1. Industry: Different industries have varying levels of criticality and attractiveness to attackers. For instance, an average healthcare company with Personal Healthcare Information is more likely to be breached than an average manufacturing company. Note that the criticality and attractiveness of specific companies might be different - a manufacturing company engaged for a critical infrastructure product may be more susceptible to an attack than an average healthcare company.
2. Size (Revenue): The cyber threat to a company with annual revenue of $5 million is different from that of a company with a revenue of $5 billion.

The research behind Safe's CRQ Calculator

The lack of accurately reported data makes it difficult to build predictive models. Safe Security's research teams came together - we looked at multiple data sources and applied our expertise to build these models.

Safe's Threat Intel Research:

- We have telemetry from ~400K assets on our platform today. This helps us to understand macro patterns.
- We have performed hack analyses of ~100 breaches over the last 3 years.
- Attack specific reports from cybersecurity vendors such as Palo Alto Networks and CrowdStrike.
- Verizon Data Breach Investigations Reports.

Safe's Financial Cost Research:

To calculate the estimated financial impact of an attack, we looked at the following detailed data points:

1. Our proprietary database of attack costs and metadata collected from primary sources (such as SEC filings, regulatory reports, legal documents, and budget reports) covering more than 1,500 security incidents worldwide over the last 10 years.
2. Insurance claim reports from leading cyber insurance providers such as Cyentia, NetDiligence, Willis Tower, Coalition, and more.

Our financial model is based upon the assets targeted, the type of attack, and its resultant cost to the business.

1. Customizable cost drivers are used to estimate costs by category, instead of simulated ranges of sparse historical data points.
2. A "model company" is created for each industry by revenue size against which simulated attacks are normalized. This adjusts for differences in asset configuration within a given revenue range.
3. Probability and likelihood scores are then applied to the modeled financial impact of various attack types by industry.

Safe's Data Science Research:

- Our Bayesian network model has been co-developed with the MIT, Boston.
- We calculate the probabilities of a successful attack occurring in the next 12 months based on this Bayesian model.

As mentioned earlier, there are multiple gaps in publicly available data. To fill these gaps, we applied our internal cybersecurity threat expertise, and data science expertise.

Key findings

The research models show a mix of expected and unexpected results.

Attack likelihood by industry of companies greater than $5B revenue:

Healthcare and Financial Services continue to be the two most vulnerable sectors. Almost 1 in 4 healthcare organizations are likely to face a successful cyber attack. This is expected due to the financial attractiveness and strategic importance of these sectors. On the other hand, manufacturing and retail have lower risk.

Financial services	Healthcare	Technology	Manufacturing	Retail
20%	26%	18%	15%	13%

Ransomware attack likelihood by industry of companies greater than $5B revenue:

Ransomware continues to be a threat, but the frequency of ransomware attacks is expected to reduce.

Financial services	Healthcare	Technology	Manufacturing	Retail
6%	8%	5%	5%	4%

Data breach attack likelihood by industry of companies greater than $5B revenue:

Almost 1 in 10 healthcare organizations are expected to face data breach attacks.

Financial services	Healthcare	Technology	Manufacturing	Retail
9%	11%	7%	6%	5%

Potential loss due to a ransomware attack for companies with $5B-$20B revenue:

The actual ransom paid can be less than 10% of the total loss incurred due to a ransomware attack. Business interruption and incident response costs can add up significantly, especially in healthcare.

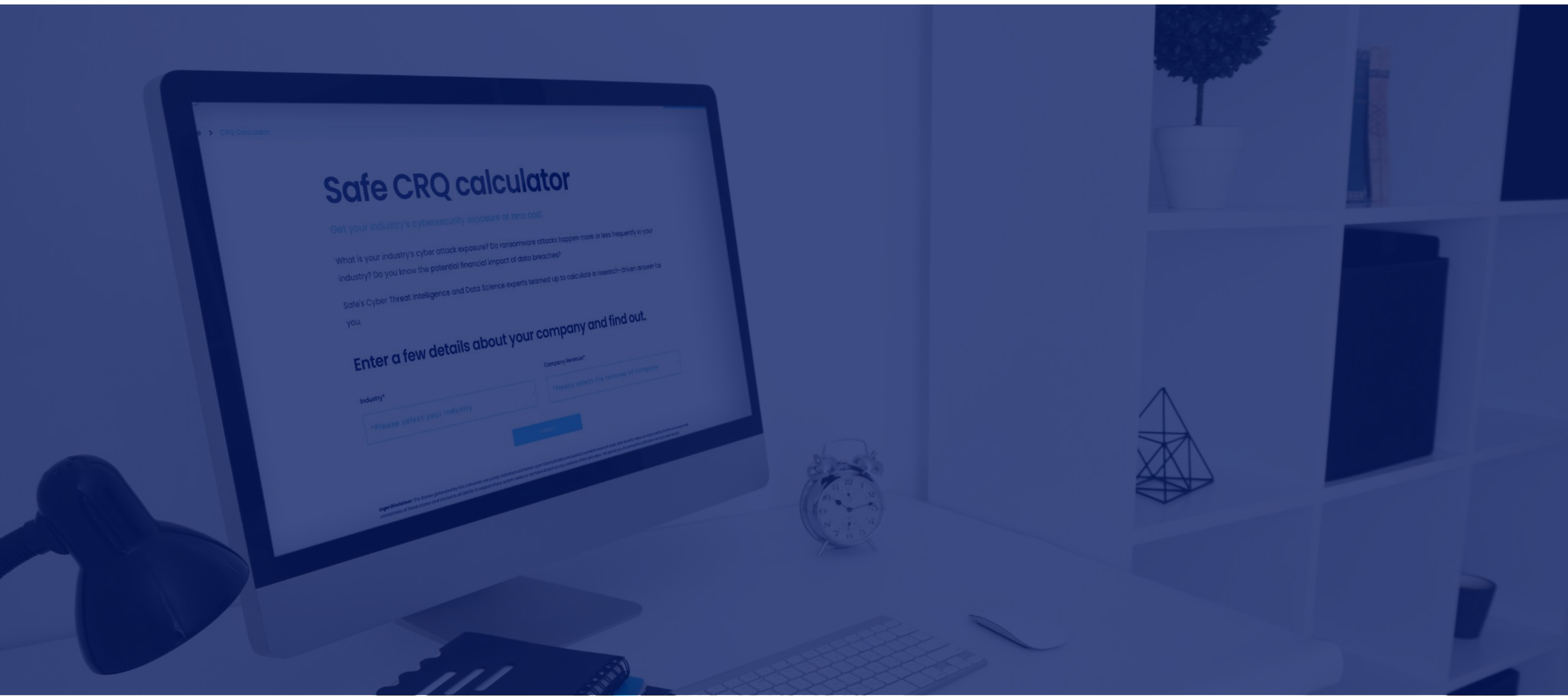
Financial services	Healthcare	Technology	Manufacturing	Retail
$41M	$85M	$43M	$43M	$62M

Potential loss due to a ransomware attack for companies with >$100B revenue:

However as the company size increases to revenues >$100B, manufacturing and retail business can have significantly larger losses. This is due to potentially large losses from business interruption and a higher number of PII records.

Financial services	Healthcare	Technology	Manufacturing	Retail
$533M	$547M	$357M	$968M	$804M

NOTE: This model will be updated as the external threat environment evolves.



CRQ Calculator

Safe CRQ calculator

Get your industry's cybersecurity exposure at zero cost

What is your industry's cyber attack exposure? Do ransomware attacks happen more or less frequently in your industry? Do you know the potential financial impact of data breaches?

Safe's Cyber Threat Intelligence and Data Science experts teamed up to calculate a research-driven answer for you.

Enter a few details about your company and find out.

Industry*

*Please select your industry

Company Revenue*

*Please select the revenue of company

Legal Disclaimer: The Scores generated by this calculator are purely indicative and based upon historical data and publicly available research data. Safe Security takes no responsibility for the accuracy and correctness of these scores and disclaims all liability in respect of any actions taken or not taken based on any contents of this calculator. We advise you to contact the Safe team for accurate results.

What does it mean for a company?

Whether you are in the CISO's team, the risk team, a C-Suite member, or a Board Member - you can use the industry data as a reference point to initiate quantified cyber risk management for your organization.

1. Benchmark: Where do you stand vs your peers? Are you best-in-class? How do you get to the best-in-class?
2. Translate: You can communicate technical risk in terms of business risk.
3. Plan and Assess: You can create action items for your team with ROSI (Return on Security Investment). You can also evaluate your cybersecurity investments.
4. Manage: You can make informed decisions based on quantified cyber risk metrics; which are your most critical risks, where should you invest, or how much cyber insurance to purchase?

If you are a cyber insurance broker or an insurance underwriter in cybersecurity, you can use the calculator to quantify a company's portfolio-level risk. Based on this information, you can tweak your pricing and/or coverage to manage the portfolio risk. Similarly, if you are a portfolio manager at a Private Equity holding company, you can use the calculator to quantify the financial risk of your portfolio companies due to cybersecurity risk.

Industry-level insights are a useful starting point to learn about company-specific cyber risk profiles. To understand and quantify cyber risk at a company level, the SAFE platform can help by ingesting real-time cyber signals from within a company's estate. This can be achieved in as quickly as 7 days.

To understand your company-specific cyber risk profile, reach us at getintouch@safe.security

SAFE

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306

www.safe.security
info@safe.security