KOVRR
Cyber Decisions. Financially Quantified.

Cyber Risk and Financial Resilience in the S&P 500®

Dr. Huw Goodall

www.kovrr.com

Executive Summary

What We Want to Know and Why

With the World Economic Forum reporting that cyber insecurity will be one of the top five market risks in the next few years, it is clear that concerns regarding cybersecurity and financial resiliency are top-of-mind across the globe. Vast amounts of capital, for instance, comprised of consumers' pensions and savings, are invested in a relatively small number of companies, rendering such issues particularly daunting. However, by ensuring their organizations are robustly prepared for the rapid growth in cyber incidents experienced in recent years, stakeholders can not only maintain financial resiliency and shareholder value but also provide economic stability across the marketplace.

To make optimal decisions regarding cyber risk management strategies, it's vital first to have an understanding of the financial implications cyber attacks can have on the organization. Cyber risk is a relatively new phenomenon that appeared in the last few decades. Nevertheless, the expanding reliance on information technology systems within companies and across their supply chains means that the criticality of cost-effective cybersecurity management has grown massively over the past few decades.

In the context of this increasingly risky interconnected digital landscape, Kovrr's Cyber Risk and Financial Resilience in the S&P 500® report addresses the question: **How financially resilient are the largest companies in the United States to cyber attacks?**

How We Answered the Question

This report leverages Kovrr's cyber risk quantification (CRQ) models to determine how cyber losses stack up against company profits and overall value, using the companies in the S&P 500 as a representative dataset, reflecting the largest entities across the US. Kovrr's on-demand models consume and subsequently enhance a company's available information to create a comprehensive and accurate firmographic and technological profile. This company profile is used to create a bespoke cyber event catalog as part of a Monte Carlo simulation that calculates the impact on each company and provides a detailed breakdown of incident costs. Larger attacks are modeled individually, and smaller, non-material incidents are grouped and modeled in aggregate.

The resulting output is a table of simulated cyber events with corresponding detailed information, including attack types, methods and actors, along with detailed cost breakdowns. These assessment results provide incredible amounts of insight into the frequencies and severities of a range of cyber attacks the company is likely to experience.

To assess the financial resilience of each company, this report compares:

- **Profitability Impact:** We compare a large but likely scenario against the profitability of the company, as reported in the prior year's income statement. This analysis shows the highest annual cost of cyber events expected within a 1-in-10-year probability, which is the sort of loss that would likely be experienced within the tenure of the current CEO. We also compare a high-severity low probability annual loss estimate for each company at the 1 in 100 probability against the profitability.
- **Long-Term Capital Impact:** To analyze the long-term resilience, we compare the

1-in-100-year probability against the available shareholders' capital. This view highlights a more extreme annual loss against the accrued financial strength of the company, where sustained losses start to erode its long-term financial strength.

Looking at these two perspectives gives both a likely scenario the company should be willing to absorb and recover from and the rarer yet more intense catastrophe, which may have longer-term impacts and solvency implications.

The Headlines

In the S&P 500

- Of the 473 companies with a positive Net Income, in the case of a 1-in-10-year cyber loss:
    - The median loss for a company is equal to 1% of its annual profit.
    - The losses would exceed 10% of profits for 8 companies. This would have a highly significant impact.
- Of the 468 companies with positive Shareholder Equity, in the case of a 1-in-100-year cyber loss:
    - The median loss is equal to 0.7% of their Shareholder Equity.
    - 251 companies would experience losses equivalent to <=5% of their Shareholder Equity.
    - Six companies would lose more than 10% of their Shareholder Equity value
- Overall, this indicates a reasonable level of financial resilience to cyber attacks across the S&P 500. However, there are a small number of companies that are at significantly higher risk of financial issues in the event of both expected (1-in-10) and rare (1-in-100) scenarios.

All these results are based only on companies in the S&P 500 with positive Net Income or Shareholder Equity.

The Full Story

Introduction

How resilient are the biggest companies in the US to the financial impacts of cyber attacks?

Stories of cyber attacks on large companies are increasingly commonplace in the media, but what is often obscured is how much these cyber attacks are costing the victims. Such obfuscation has not gone unnoticed by regulators, with the likes of the US Securities and Exchange Commission (SEC), for example, enacting legislation in 2023 requiring ’material’ cyber incident and risk disclosure. The EU and Australia, too, have passed similar regulations mandating this transparency. Simultaneously, investors and rating agencies are steadily waking up to the significant risk faced by almost all companies due to their cyber exposure.

In this report, we investigate the resilience of the largest US companies to the financial impacts of cyber attack by comparing their likely losses from cyber attacks with their published financial data, to quantify how financially resilient these companies are to cyber incidents.

Methodology

Kovrr's models allow for a complete internal modeling of a company's digital infrastructure and cyber control framework. For this study, we base the internal network and digital infrastructure on benchmarked information about each company and then augment it with specific technology profiles collected via a non-consensual outside-in scan. The profile of security controls applied at these companies is considered sensitive information, so we have made conservative assumptions for these control levels across industries and revenue bands.

Each S&P 500 company's cybersecurity posture and network architecture were integrated into Kovrr's cyber risk quantification models and assessed according to the full range of events and scenarios tailored to each company's exposure. The models evaluate a range of typical cyber event types to which a company may be exposed, not just those reported publicly. This includes data breaches, extortions, interruptions, and service provider outages. Excluded events include operational technology and physical damages, which can be modeled but require additional company exposure details.

We compare the results of the CRQ assessment with the balance sheet and income statement of each company (for the prior financial year, as published at the time of writing). We focus our analysis on two probability outcomes:

- **The 1-in-10-Year Loss**
  - There is a 10% probability of exceeding the specified financial loss in a given year.
  - This is the type of incident likely to occur during the tenure of senior executives, including the CISO, and one the company should be prepared to experience.
  - E.g., If the 1-in-10 loss is $5 million, then there is a 10% chance that the company will have a cyber attack that costs them $5 million or more in the next year.
- **The 1-in-100-Year Loss**
  - There is a 1% probability of exceeding the specified financial loss in a given year.
  - This scale of incident has a low probability of occurring but could nevertheless cause a significant loss to companies and, in extreme cases, may result in insolvency.
  - E.g., If the 1 in 100 loss is $1 million, then there is a 1% chance that the company will have a cyber attack in the next year that costs them $1 million or more.

To measure our cyber risk quantification results against the company's financials, we compare:

- The 1-in-10-year loss with the Net Income (profit)
- The 1-in-100-year loss with the Net Income (profit)
- The 1-in-100-year loss with the Shareholder Equity

We expect outliers because the situations of different companies can be highly variable. In this analysis, we omit companies that have negative Net Income (profit) or Shareholder Equity from the respective analyses. The reasoning is the metrics we have chosen do not compare in a straightforward way across positive and negative values of Net Income or Shareholder Equity.

Number Crunching

Short-Term Profitability Impact

Firstly, we compare the profit to the 1-in-10-year loss. Figure 1 illustrates the proportion of the 1-in-10-year loss to profit. With this metric, 100% would mean the 1-in-10 year loss is equal to the annual profit. A value of 10% would mean that the 1-in-10 year loss is equal to 10% of the annual profit.

For the majority of S&P 500 companies, a 1-in-10-year loss is within 2% of profits (median 1% of profit, mean 2% of profit), but an expected cyber attempt could exceed 10% of profits for 8 companies. On an individual company scale, the two largest proportions are 71% and 29% of profits. While these outliers are valid, they are mainly driven by the ratio of Revenue to Net Income, thereby providing a snapshot of the current state of these companies, which may not necessarily be their 'normal status.' This is an important reminder that cyber risk does not exist in a vacuum but as one of a multitude of operational risks that the board must assess. If a company has other financial issues (e.g., other large operational losses), it will be less financially stable, and a cyber attack may have an outsize financial impact. These outliers and long-tailed distributions also indicate that the median will be the most useful metric throughout the report.

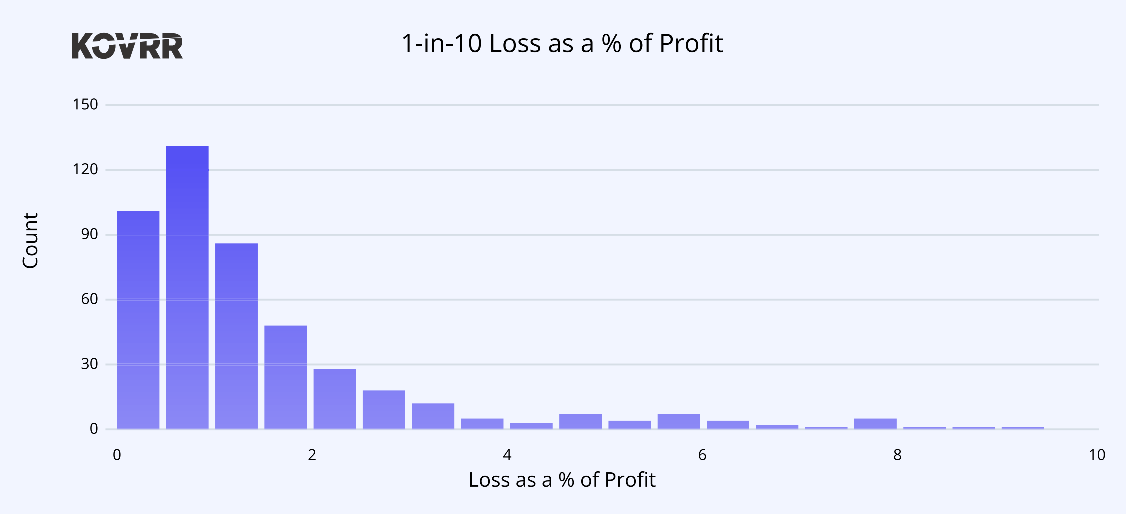

Figure 1: Histogram of 1-in-10-year loss as a % of profits. Outliers at 71%, 29%, 26%, 14%, 12% and three at 13% have been omitted for clarity.

When comparing the 1-in-100-year loss with the profit, in Figure 2 below, we see that losses from a rare cyber event could exceed 10% profit for 19% of companies, 20% of profit for 8% of companies, and 50% of profit for 2% of companies. The mean and median percentage of profit that would be lost in a 1-in-100-year event are 9% and 5%, respectively.

At the extreme end, we observe three entities where a 1-in-100-year event would more than wipe out the company's annual profit, with losses amounting to 1.2, 1.3, and 3.5 times the annual profit due to cyber attacks. While risk appetites will vary between different stakeholders, this risk level should be enough to make anyone stop and think.

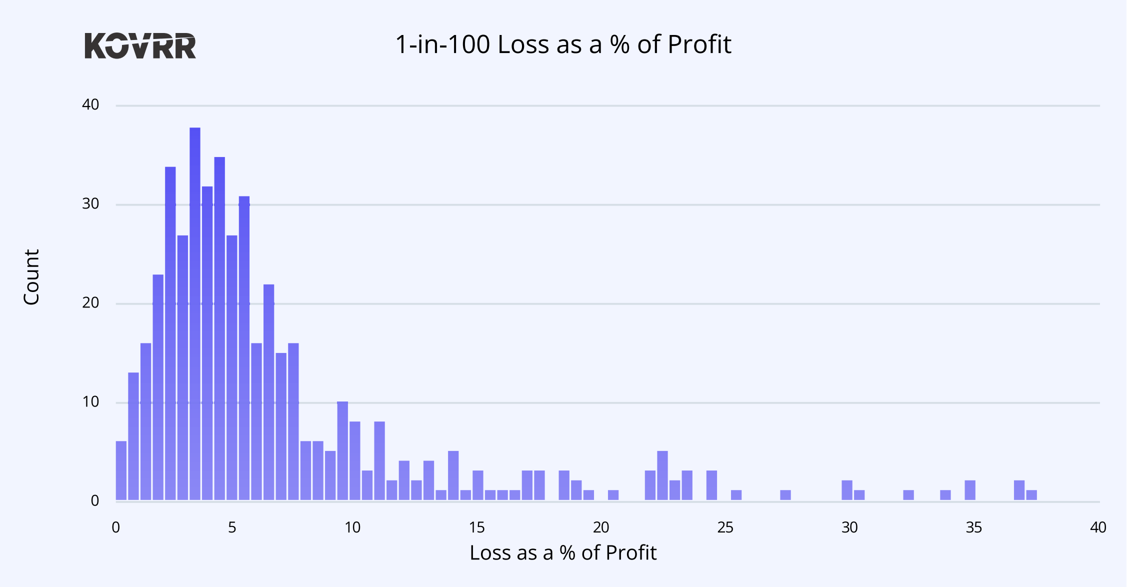

Figure 2: Histogram of 1-in-100-year loss as a % of profit. For clarity, 7 outliers between 40 and 100 have been removed, as well as outliers at 115%, 127%, and 346% have been omitted. Companies with a negative profit are also omitted.

Long-Term Capital Impact

Looking at the longer-term value of the company, we also compare its value (Shareholder Equity) with the 1-in-100-year loss. For example, in Figure 3, we see that a rare but plausible attack will, on average, produce a median loss equal to 0.7% of the Shareholder Equity (1.8% mean).

As always, the average does not tell the whole story, and there are some big potential losses out there. The largest is a company for which the 1-in-100-year event would mean a loss 2.2 times as large as the company's value. The second most impacted company is financially affected much less, with a smaller but still significant loss of 50% of Shareholder Equity. All the remaining companies experience a loss of less than 21%.

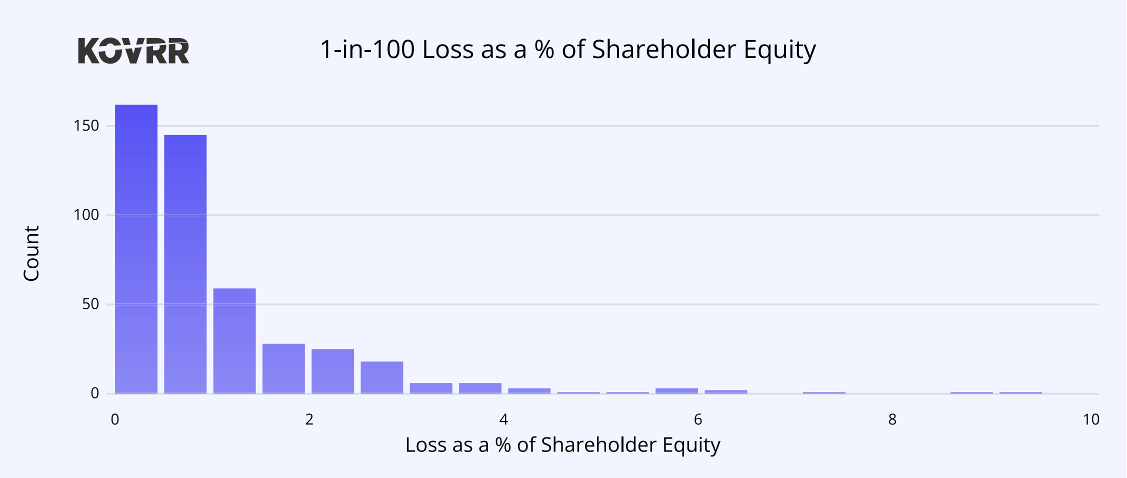

Figure 3: Histogram of 1-in-100-year loss as a % of Shareholder Equity. For clarity, an outlying value has been omitted at 219% as well as at 5 counts between 10% and 50%. Companies with negative Shareholder Equity are also omitted.

Breakdown by Revenue

When breaking down the 1-in-10-year loss vs. company profit in Figure 4, the median loss is fairly similar between all revenue bands at around 1%. The 100-200B revenue band is the exception. This is likely due to the specific industry mix that sits in this revenue band.

The results become more interesting when we look at the 1-in-100-year loss vs. the Shareholder Equity in Figure 5. We see a clear increase in median value as revenue increases, with the exception of the highest revenue band. (It's about to get a bit finance-heavy, so bear with me.) We propose this relationship exists because the size of the Shareholder Equity as a percentage of a company's assets is typically smaller for a larger company. This is because larger entities typically have diversified risks and are, therefore, less likely to be impacted by a single event, necessitating less reserved capital.

An example would be if there are two companies, Company A, which is small and operates only in California, and Company B, which is huge and operates globally. Company A would need a much higher proportion of Shareholder Equity to handle a cyber attack that wipes out power on the West Coast of the USA than Company B would, as only a small percentage of Company B's business occurs in California. This means that as a percentage of revenue, less capital needs to be kept aside in Shareholder Equity to manage the risk effectively. As a result, when a large (1-in-100-year) cyber attack occurs, if it results in a 5% revenue loss across both companies, then the larger Company B will end up with a higher proportion of its Shareholder Equity impacted. We don't draw any conclusions from the largest revenue band because there are relatively few companies that have revenues greater than $200 billion.

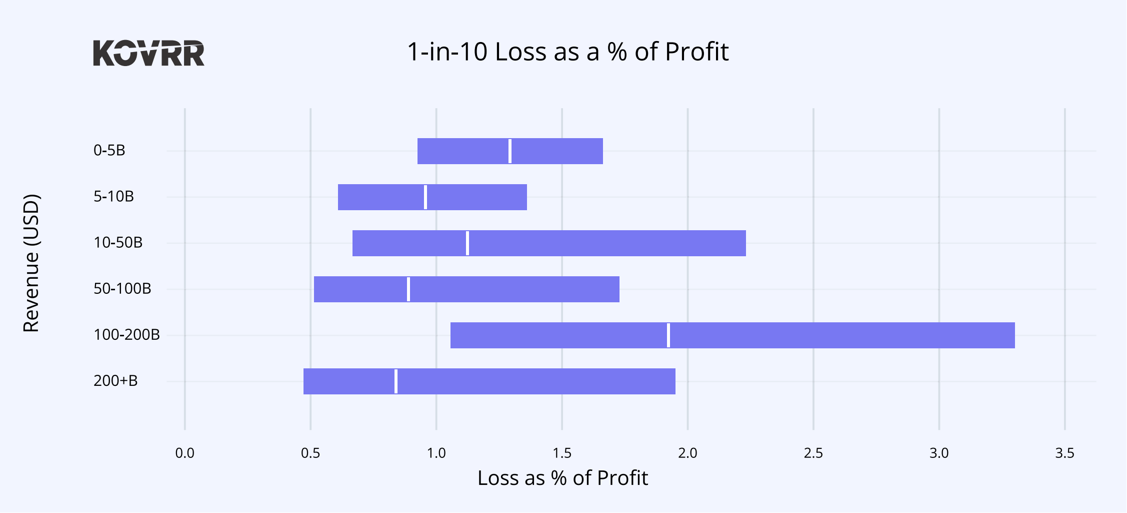

Figure 4: Box plot of 1-in-10-year loss vs. company profit by revenue band. Boxes show the median, upper, and lower quartiles.

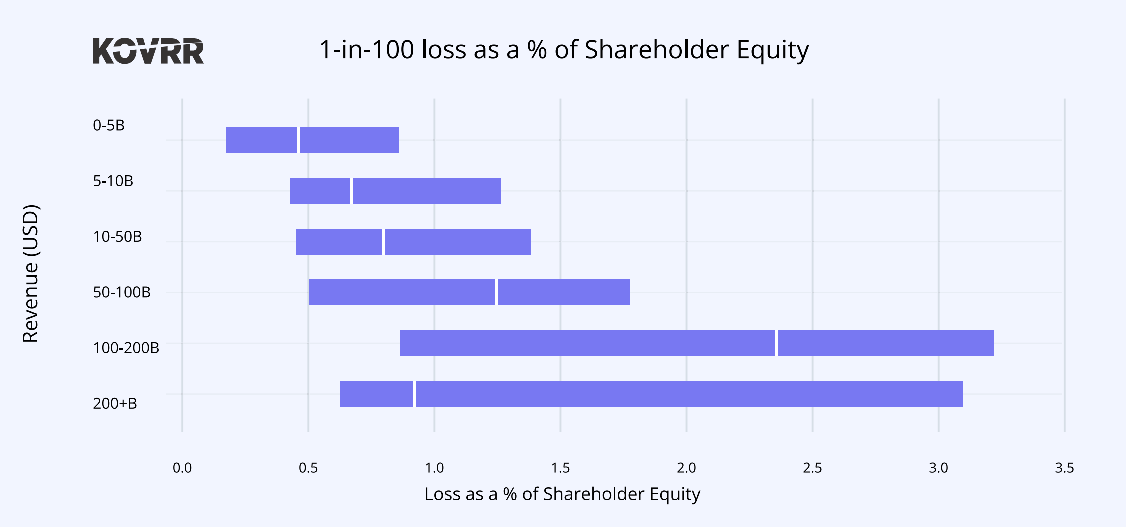

Figure 5: Box plot of 1-in-100-year loss vs. Shareholder Equity by revenue band. Boxes show the median, upper, and lower quartiles.

Breakdown by Industry

When we break down the 1-in-10-year loss by industry, Finance has the lowest cost median, along with Retail Trade at ~0.5% of profit. Services and Transportation communication electric, gas and sanitary. has the highest median at 1.4% of profit. There is little to differentiate between the medians of other industry groups, which sit between 1-1.4%. Wholesale Trade has a distribution that skews to the right more than other sectors.

Investigation of the 1-in-100-year loss as a percentage of Shareholder Equity finds Finance as the industry with the lowest relative impact (median 0.3% of Shareholder Equity), but this time, Retail Trade is impacted the most with a median of 1.8%. All other industry groups have median values of 0.5-1%.

Generally, the relative impact is highly similar between the short and long-term measures of impact, but Retail Trade is the exception here. It goes from one of the lowest in the 1-in-10 to the highest in the 1-in-100.

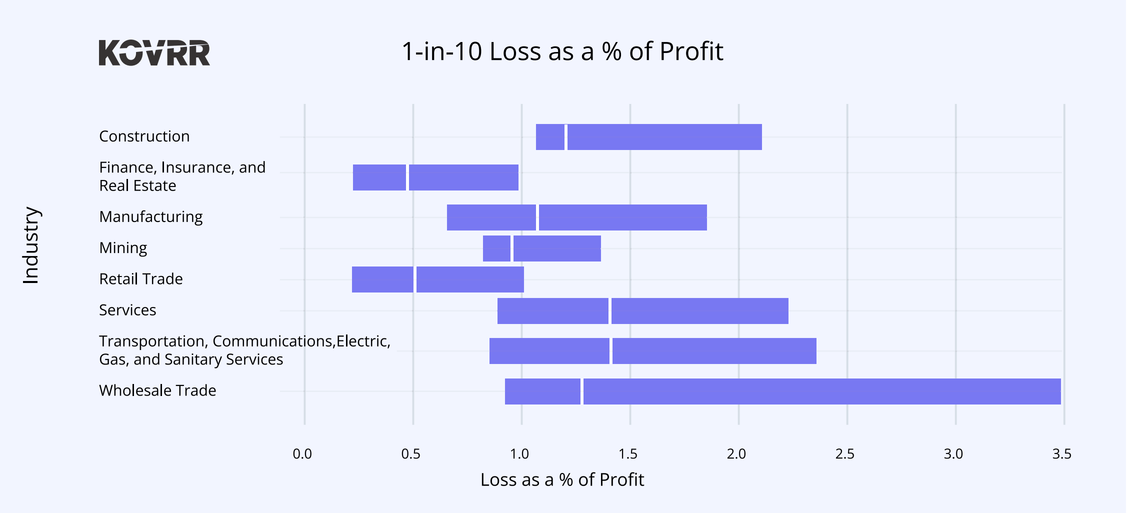

Figure 6: Box plot of 1-in-10-year loss vs. company profit by industry. Boxes show the median, and upper and lower quartiles.

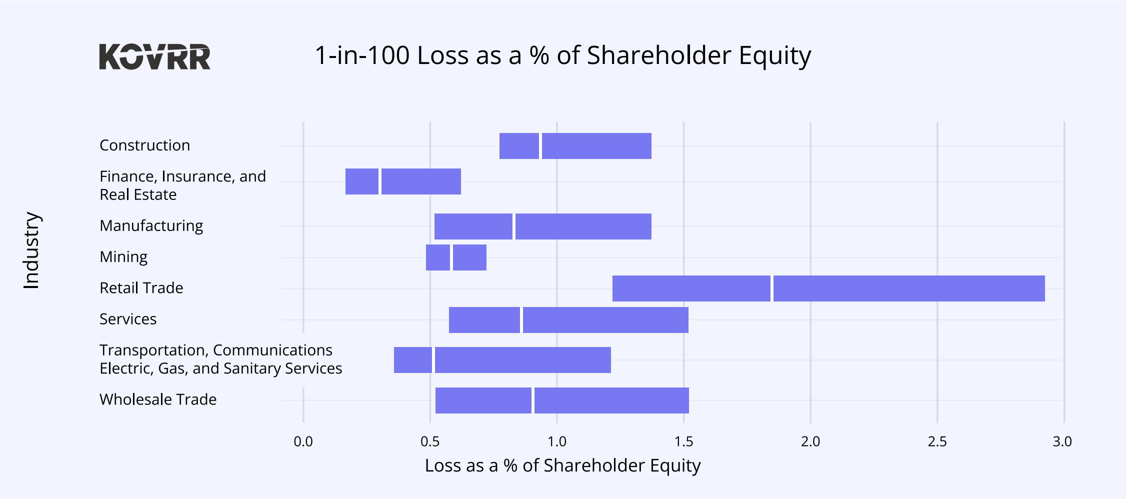

Figure 7: Box plot of 1-in-100-year loss vs. Shareholder Equity by industry. Boxes show the median, upper, and lower quartiles.

Summary: Nice Numbers, But What Do They Mean?

So, how financially resilient are the largest companies in the US to cyber attacks?

Well, of the 473 companies in the S&P 500 running in profit, 439 would experience a loss of <=5% of their profit if they experienced a 1-in-10-year event. This means they should still have plenty of financial resources to deal with other unrelated risks if they arise. However, there are three companies that may lose over 20% of their profits and 8 companies that could lose more than 10% of their profits. These companies are much less financially resilient to these likely scenarios.

When we look at the rare but still plausible 1-in-100-year events, the headline news is that there is at least one company that would almost certainly become insolvent if it experienced a 1-in-100-year attack and one other company that would experience losses of at least a third of their Shareholder Equity. However, of the 467 companies with positive Shareholder Equity, 251 would experience losses equivalent to <=5% of their Shareholder Equity in a 1-in-100-year attack. These companies would face difficult times but stand a good chance of remaining solvent.

In this report, we have omitted companies with negative profit and Shareholder Equity. However, these companies may be at serious risk of insolvency if faced with a significant cyber attack, though the risk will vary. Another consideration is risk transfer mechanisms. Cybersecurity insurance is a growing market and is a common way of reducing the financial risk of cyber attacks. These factors indicate that our results likely lean a little on the conservative side when considering the impact relative to profit or Shareholder equity.

Overall, we observe that S&P 500 companies that are running in profit and have positive overall value are reasonably financially resilient to losses from cyber attacks. A small proportion of them are likely to have serious financial issues when faced with a significant (1-in-10 or 1-in-100-year) cyber attack. However, cyber attack exposure is merely one of the many risk factors organizations must consider when balancing their overall risk management strategies. Cyber attack exposure sits under the wider umbrella of operational risk, which in turn typically makes up around 5-10% of the company's overall risk capital allocation.[1]

[1] *Source: https://www.theirm.org/media/6809/irm_operational-risks_booklet_hi-res_web-2.pdf This is based on companies that are required to comply with solvency II solvency capital requirements, which is EU legislation. However, it offers a rare window into the capital risk modeling of large entities.*

For context on the magnitude of financial losses, we determined the probability of certain recent events occurring in any of the companies within the S&P 500 in a given year. The $110 million loss incurred by MGM in 2023 has a 50% probability of occurring, while the $550 million loss experienced by Delta Airlines due to CrowdStrike this year has a 25% chance of occurring. It is important to note that these probabilities only apply to the S&P 500 as a whole, not when considering a single company.[2]

Given the potentially large losses we have explored in this report, it remains a question for each company: Do you have the capital to cover these events in line with your chosen or regulated risk profile?

By quantifying the risk of cyber attacks and highlighting their likely monetary implications, CISOs and other cybersecurity leaders can facilitate a more informed decision-making process at the C-suite level and in the boardroom. With the more tangible impact metrics, these executives can, for instance, more appropriately allocate budget and determine optimum risk transfer mechanisms.

For cybersecurity professionals, Kovrr's on-demand CRQ models can also offer direct insights into the return on investment regarding security control upgrade implementation, a metric high-level executives intrinsically value. Moreover, they provide continuously updated information on the cyber threat landscape, tailored specifically to an organization's exposure. With this capability, stakeholders have access to the data necessary for achieving a state of cyber resilience.

[2] *For the insurance fans out there, we calculated these probabilities by crating an aggregated Occurrence Exceedance Probability curve.*

Definitions:

- **The 1-in-10-Year Loss**
  - This means there is a 10% probability of exceeding the specified financial loss in a given year.
  - This is the type of incident likely to occur during the tenure of senior executives, including the CISO, and one the company should be prepared to experience.
  - E.g., If the 1-in-10 loss is $5 million, then there is a 10% chance that the company will have a cyber attack that costs them $5 million or more in the next year.
- **The 1-in-100-Year Loss**
  - There is a 1% probability of exceeding the specified financial loss in a given year.
  - This scale of incident has a low probability of occurring but could nevertheless cause a significant loss to companies and, in extreme cases, may result in insolvency.
  - E.g., If the 1 in 100 loss is $1 million, then there is a 1% chance that the company will have a cyber attack in the next year that costs them $1 million or more.
- **Net Income**
  - Also known as Net Profit, calculated by:
    - » *Net Income = Total Income - Total Expenses*
  - Can be thought of as how much profit a company makes in a year (we use annual rather than quarterly profit in this report).
- **Shareholder Equity**
  - Also known as Stockholder Equity is calculated by:
    - » *Shareholder Equity = Total Assets - Total Liabilities*
  - Can be thought of as how much is the company worth to its owners after it has paid all it’s liabilities from it’s assets.