cowbell®

Cyber Round-Up Q1 2022

Precise Underwriting for SMEs

The Leading Provider of Cyber Insurance for SMEs

Q1 2022

TABLE OF CONTENTS

3 **FOREWORD**
The Importance of Cyber Resiliency

5 **SECTION ONE**
Cowbell Factors for Continuous Assessment of Cyber Risk

7 **SECTION TWO**
The SME Perspective on Cyber Insurance

9 **SECTION THREE**
Setting Expectations for Cyber Insurance Premiums

12 **SECTION FOUR**
Going Deeper: Software Supply Chain Cowbell Factor

14 **CONCLUSION**

FOREWORD

Dear Reader,

According to the World Economic Forum's (WEF) Global Cybersecurity Outlook 2022, "88% of global cyber leaders indicate that they are concerned about cyber resilience of small- and mid-sized enterprises (SMEs) in their ecosystem." Our economy is increasingly global, digitized, and interconnected with supply chains involving transactions between large companies and SMEs, so this concern is very valid. Typically, SMEs do not have the same resources as their larger counterparts do to spend on cybersecurity, so they are seen as vulnerable targets in these supply chains. The unfortunate truth is that SMEs are often targeted as a means to ultimately victimize another company in the supply chain. In fact, the WEF also reports that "Nearly half (44%) of the surveyed CEOs indicated that software supply chain attacks will have the greatest influence on their organization's approach to cybersecurity in the future." So, what can be done to remedy this?

To secure supply chains overall, each link along the chain must be secured. This starts with creating a culture of cybersecurity at all levels.

Stated simply, cybersecurity refers to a set of technical measures implemented to safeguard against cyberattacks, like phishing, ransomware, and social engineering.

Cyber resilience is a broader term that incorporates these technical measures and supplements them with a prevention-oriented and preparedness mindset embodied by each employee and each company along the supply chain, which also enables the business to recover quickly when an incident occurs. For the past few years now, organizations have operated under the assumption that they will fall victim to a cyber attack at some point. As a consequence, detection and prevention, the primary domains of cybersecurity, are no longer sufficient. Preparedness and the ability to recover effectively and maintain operations in the event of a cyber incident is **cyber resiliency.**

It is recognizing that cybersecurity best practices are everyone's responsibility and that it is a continuous journey, not a destination. Bad actors and their tactics are constantly evolving, so, too, should an organization's cyber resilience.

Furthermore, cyber resilience encompasses the aftermath of an attack and acknowledges that cyberattacks do not end when the ransom is paid, for example. Rather, the affected organization should have an incident response plan in place to facilitate business continuity in the event of a cyberattack, as well as share lessons learned from the incident with others so that similar incidents can be prevented in the first place.

The aftermath of a cyberattack is often wrought with reactive measures and questions like "How can we afford this ransom payment?" and "How will we recover our lost data?" If an organization does not have a well-thought-out incident response plan with trusted and tested backups in place, a cyberattack can be devastating. Practicing cyber resilience, however, can help tremendously. A part of cyber resilience is acquiring cyber insurance. While simply buying a cyber insurance policy may not make an organization fully immune to a cyberattack, it will reduce the financial uncertainty involved in how the organization responds.

Cowbell's continuous risk assessment and closed-loop risk management provide businesses with peace of mind, knowing that they are doing everything in their power to defend themselves against a cyberattack, and if one still manages to penetrate their walls, the effects will not wreak total havoc on the business.

Cowbell's cyber policies encourage the adoption of cybersecurity best practices, like MFA and cybersecurity awareness training across the whole organization. Having a cyber insurance policy alone is not enough, but it is certainly a step in the right direction to achieving cyber resilience.

In this quarter's Cyber Round-Up, we discuss how Cowbell Factors are being utilized to inform better, more accurate underwriting, how SMEs perceive cyber insurance, and the ways in which cyber insurance premiums vary by industry.

- Isabelle Dumont, SVP of Marketing and Technology Partnerships, Cowbell Cyber

SECTION ONE

Cowbell Factors for Continuous Assessment of Cyber Risk

What are Cowbell Factors?

Cowbell Factors provide a relative rating of an organization's risk profile against Cowbell's risk pool of 23 million accounts as of Q1 2022. Cowbell Factors constitute the basis for risk selection and cyber insurance underwriting with real-time, continuously updated risk exposure insights. The Factors are specifically designed for insurance purposes and anchor risk selection and underwriting for cyber insurance. Stated simply, the higher the factors, the more insurable the risk.

Cowbell Factors are compiled using more than 1,000 data points and risk signals from a variety of sources including public databases, third-party vendors, proprietary external scanners, dark web intelligence, and exploits and vulnerability repositories. Cowbell applies artificial intelligence and machine learning algorithms to normalize collected signals, model risks, and compile Cowbell Factors.

Furthermore, Cowbell Factors incorporate additional inside-out data when connectors to service providers or security vendors are activated. Example: When a business using Microsoft 365 (aka Office 365) activates Cowbell's Microsoft connector, Cowbell Factors deliver an even more refined assessment of risk with timely insights and recommendations to improve the organization's risk profile.

In December 2021, we reported on our population of policyholders with activated Cowbell Connector for Microsoft. This showed a positive impact on their company's risk profile based on the additional insights provided by inside-out data.

The cyber risk profile of an organization is constantly evolving as criminals continue to innovate new tactics emerge. Cowbell always captures new data and continuously recompiles Cowbell Factors, offering organizations direct and always up-to-date visibility into their relative cyber risk exposures.

How can Cowbell Factors be applied?

Based on Cowbell Factors, Cowbell also compiles two aggregate factors for the organization and its class of business. This offers a benchmark that compares the organization's overall level of risk, the "Aggregate Company Factor" to its industry peers. Cowbell Factors become that much more meaningful when compared to industry averages. In this way, they can be used by the policyholder as a peer benchmarking tool.

All told, Cowbell Factors are the first filter used by the Cowbell platform for risk selection and pricing.

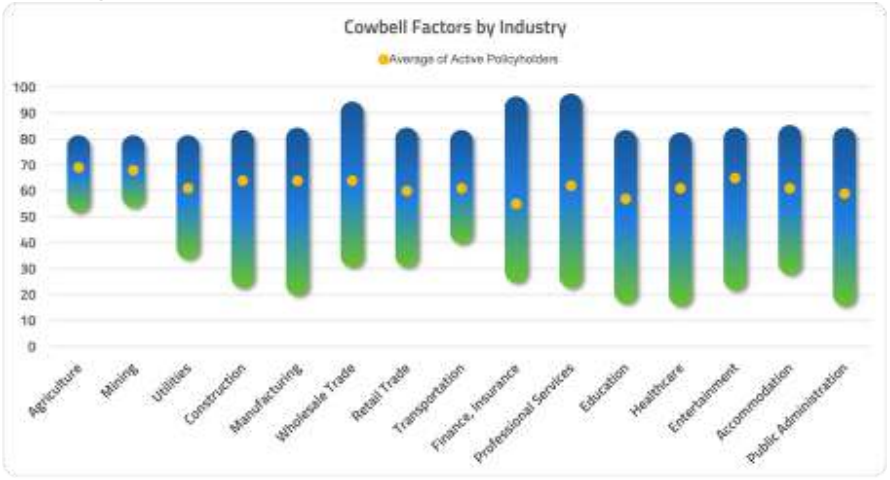


Figure 1: Range of Aggregate Cowbell Factors by Industry for Accounts Assessed for Cyber Insurance along with Average for Active Policyholders

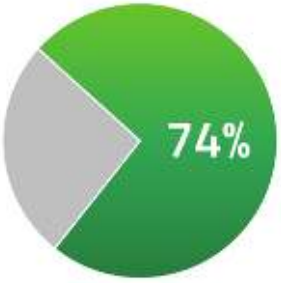
Figure 1 above illuminates how the Cowbell Factors differ by industry. Furthermore, Cowbell Factors allow underwriters to compare a potential policyholder's risk profile to that of its peers within the same industry. Comparison within an organization's industry as opposed to comparison across all industries allows for greater precision in underwriting and encourages risk improvement.

SECTION TWO

The SME Perspective on Cyber Insurance

Given that Cowbell's product is designed for businesses with up to $250 million in revenue, the focus is on SMEs. In January, we surveyed Cowbell policyholders (SMEs) to gain insight into their perceived value of cyber insurance. The results indicate that 79% of policyholders believe cyber insurance is worth the cost and 74% of policyholders agree that they have improved their cybersecurity awareness as a result of acquiring cyber insurance.

79% of Cowbell policyholders believe cyber insurance is **worth the cost**



74% of Cowbell policyholders agree that they have **improved their cybersecurity awareness** as a result of acquiring cyber insurance

It is clear that having a cyber insurance policy alone is not enough, but it is certainly a step in the right direction in achieving cyber resilience. With this in mind, Cowbell educates policyholders on the importance of cyber safety by bundling with our cyber policies on-demand access to peer benchmarks and risk insights that help them address security weaknesses, and keeps them informed through monthly newsletters that highlight cybersecurity's important and current topics, such as ransomware best practices.

We also asked policyholders what additional services they would like to see from their cyber insurer: 71% would like their cyber insurer to give recommendations to minimize risk exposure and 48% would like cybersecurity awareness training for employees.

These policyholder responses are aligned with the services Cowbell provides, such as our Cowbell Insights, Cowbell's risk engineering team that provides guidance on incident preparedness and risk mitigation, and the ability to set up a cybersecurity awareness training program for employees. We're continuously working to improve and add to these services, all to provide our policyholders with the best value.

SECTION THREE

Setting Expectations for Cyber Insurance Premiums

When it comes to matters of cybersecurity and insurance, SMEs, and our potential policyholders, often question whether they truly need cyber insurance. The reason for this is not only that they might not feel at risk of a cyberattack, but also because they have little to no frame of reference for the cost of a cyber insurance policy and the benefits it will yield.

How are policy premiums determined?

Generally, policy premium tables are defined by actuaries at insurers based on sophisticated models accounting for many parameters that define the risk. Every policy is then modeled by experienced cyber underwriters based on the unique specifications of the account.

For cyber, it can be even more complex than for other well-established lines of insurance that are modeled based on decades of historical data. Because past threats and incidents are not always sufficient indicators of future cyber risk, modeling needs to rely on time-sensitive information that captures the complexity of an enterprise's digital footprint. In addition, policy contracts account for many parameters that inform the policy premium in different ways, and include the following:

- **Revenue:** Generally, companies with higher revenue have higher premiums. In Figure 2 below, it can be seen that companies with revenue of $1m-$10m, for example, are 60% below the average premium baseline.
- **Class of business (industry):** Premiums vary significantly by industry as shown in Figure 2 below.

- **Security posture and controls:** A company's commitment to implementing and maintaining cybersecurity best practices can significantly impact their policy premium. For example, knowing that an insured has adopted the practice of Multi-Factor Authentication (MFA) company-wide would result in a lower premium.
- **Aggregate limits:** The level of coverage requested has a direct impact on the insurance premium.
- **Deductibles:** Typically, higher deductibles translate to lower premiums.
- **Selected coverages and endorsements**: A policy might offer a variety of customizable coverage options. The inclusion of additional coverages, endorsements, and their related limits will directly affect the premium because of the resulting increased or decreased coverage.
- **Type and volume of processed data:** The type of data, records, and customers to which a company has access changes its premium. A greater volume of this type of information will increase the importance of having cyber insurance, and will, therefore, raise the premium. Similarly, more sensitive data (i.e., Personally identifiable information) will have the same effect.

The Baseline: By the Numbers

Many variables listed above are discussed in relation to a baseline. For this report, the "baseline" represents the average premium of Cowbell policyholders ($0m - $250m) for the entire 2021 year. This baseline is the point of comparison we use in the subsequent figures.

In the graph below, the average premium for businesses with revenue between $50 million and $100 million is more than 100% higher than the baseline, and so on.

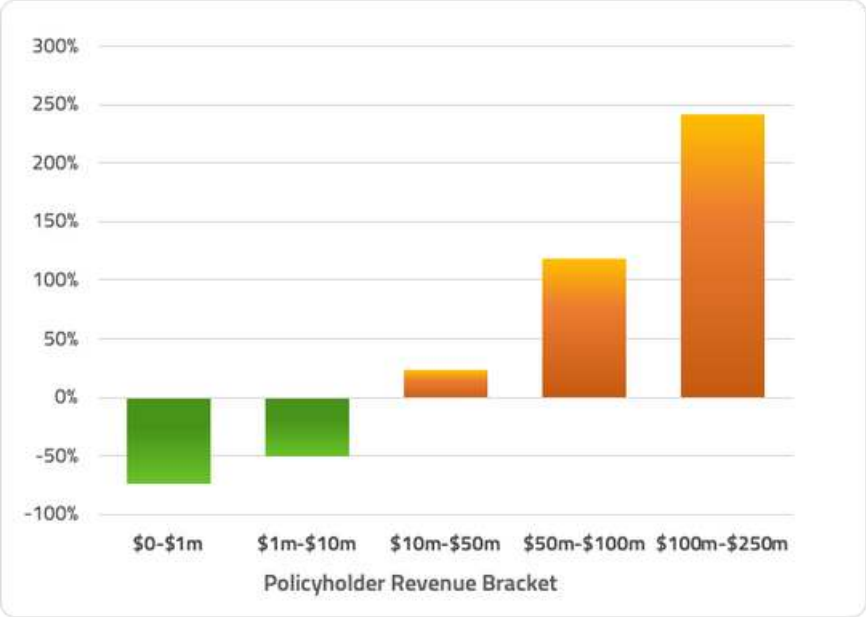


Figure 2: Deviation from Average Premium
(Population of active policyholders with $1 million aggregate limit)

Similarly, in the graph below, the average premium by industry based on NAICS two-digit codes is compared to the overall average.

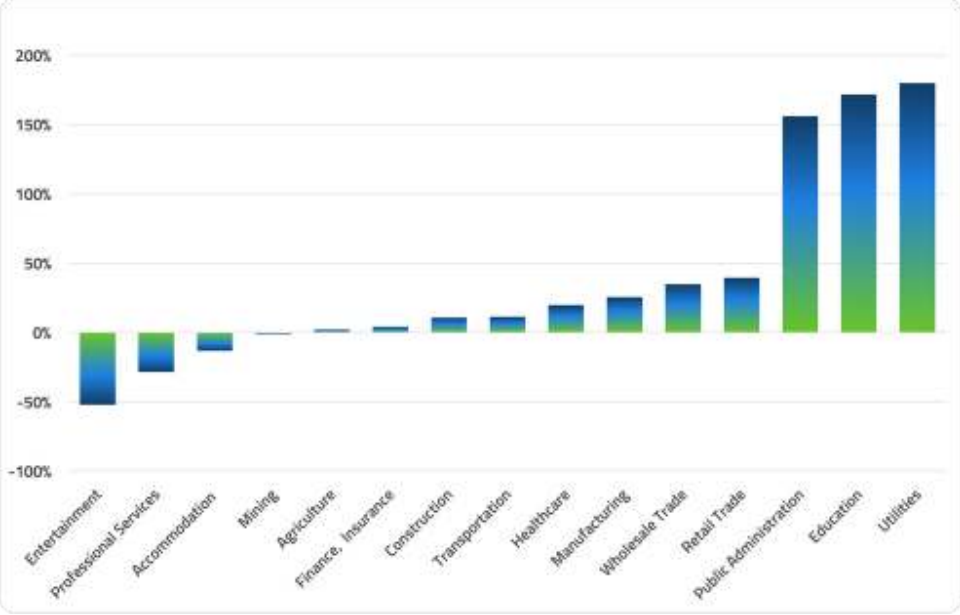


Figure 3: Deviation from Average Premium By Industry
(Population of active policyholders with $1 million aggregate limit)

SECTION FOUR

Going Deeper: Software Supply Chain Cowbell Factor

Why is the Software Supply Chain Cowbell Factor important?

According to the report, 2021 State of the Software Supply Chain, by Sonatype, the world witnessed a 650% increase in software supply chain attacks related to open source software in 2021, aimed at exploiting weaknesses in upstream open source ecosystems. The Cowbell Factors cover a wide array of insights, to include Dark Intelligence, Network Security, Cyber Extortion, and more. Most recently, Cowbell added a new Factor: Software Supply Chain, in response to recent events and the extraordinary aforementioned increase in supply chain attacks. Cowbell's inclusion of the Software Supply Chain Cowbell Factor acknowledges the use of open source software.

What is the Software Supply Chain Cowbell Factor?

Two characteristics are predominant when evaluating an organization's risk for Software Supply Chain Risk:

- Is the organization highly dependent on software, especially open source?
- Is the organization applying strong controls and security best practices to minimize its exposure to software supply chain risks?

At the industry level, the compilation of the Software Supply Chain Cowbell Factor for a large population of businesses, validates common sense on software supply chain exposures and also informs how the overall risk plays out when combining the above two characteristics.

Similar to the above industry-based analysis, below is a graph that breaks down the Software Supply Chain Cowbell Factor, specifically, by industry. From this analysis, we can see that:

1. Industries with the highest risk exposure to Software Supply Chain (low Cowbell Factor): this is due to either high dependency on software or weak controls or both: accommodations (hospitality and food services) and mining.
2. Industries that stand out for weak controls over their software supply chain overall: public services, education, and transportation (in addition to accommodation).
3. Industries worth standing out for high dependencies on software but with very strong controls, resulting overall into a lower risk for software supply chain: Financial services and entertainment (media).

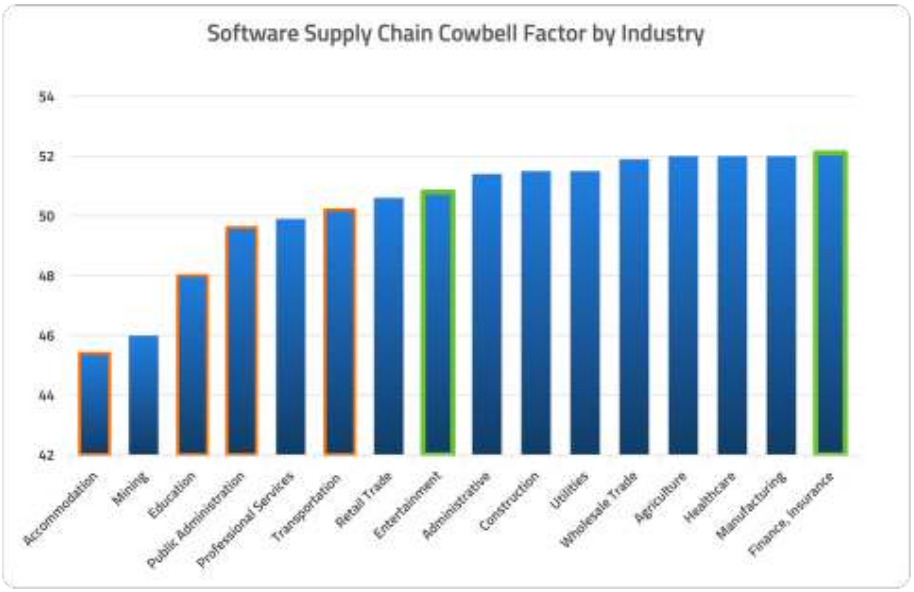


Figure 7: Software Supply Chain Cowbell Factor By Industry
(Industries highlighted in green have the best controls over Software Supply Chain risks, while industries in red have the weakest controls)

While Software Supply Chain was the latest addition to the roster of Cowbell Factors and a primary focus of this Round-Up report, Cowbell's recognition of the issue goes deeper. In addition to identifying vulnerabilities, we work to improve policyholders' posture through our **Spotlight** capabilities. This will be discussed in more depth in the next quarterly Round-Up.

CONCLUSION

Cowbell Cyber is the pioneer in cyber risk underwriting based on vast amounts of structured and unstructured data, machine learning and artificial intelligence models, and proprietary rating factors and the team is excited to continue to deliver much-needed innovation in closed-loop risk management in 2022. In this first quarterly Cyber Round-Up report, our objective was to equip SMEs with relevant data to make informed decisions on cyber insurance. In future quarterly Cyber Round-Up reports, we will continue to offer insight into how premiums evolve based on market trends and highlight other Cowbell Factors, such as Dark Web Intelligence and Cloud Security.

Disclaimer: Data and analysis provided above are for general, informational purposes. Businesses should always consider their individual circumstances to understand their level of insurability. Nothing in this document is intended to define any policy commitment offered by Cowbell. However, should you need further information or assistance, please do not hesitate to reach out to us at Cowbell - we would be happy to help with any questions or concerns that you may have.