cowbell®

Cyber Round-Up Q2 2022

Closing the Loop: Enabling SMEs to Continuously Improve Their Cyber Risk Profile

The Leading Provider of Cyber Insurance for SMEs

Q2 2022

TABLE OF CONTENTS

03 **FOREWORD**

06 **SECTION ONE**
Cowbell Factors: An Anchor for Individual and Aggregated Risk Evaluation
- Individual Risk Evaluation
- Evaluation of a Risk Portfolio

10 **SECTION TWO**
The Happy Path Toward Coverage: Eligibility and Insurability

11 **SECTION THREE**
Staying Ahead of New Threats with Spotlight

13 **SECTION FOUR**
Dark Web Exposures are Critical

15 **SECTION FIVE**
Continuous Underwriting: The Future of Cyber Insurance

17 **APPENDIX I**
NAICS Sector Descriptions

FOREWORD

Dear Reader,

February 5, 2022 marked exactly one year since the New York Department of Financial Services published its **Cyber Insurance Risk Framework**. This Framework outlines seven best practices relevant for property/casualty insurers and should be applied on an individualized basis to insurers depending on their respective amount of risk.

In tandem with the rise of remote work and digitization, cybercriminals have increased in numbers and are also more sophisticated. This is evident when one looks at the sheer increase in ransomware attacks, cyber crimes, and other incidents. Though these trends in cybersecurity are acknowledged, society still has a great deal of ground to make up when it comes to awareness, prevention, and preparedness, not to mention recovery. Both the cybersecurity and cyber insurance industries can benefit from one another. The Framework recognizes the interdependence of cyber risk with cyber insurance for both underwriters and policyholders; so, too, does Cowbell Cyber.

A key element of the Framework is “Educate insureds and insurance producers.” This is significant because cyber insurance is about more than just coverage in the event of an incident; it is also about prevention and continuous improvement. An organization's risk rating determined by Cowbell Factors can be influenced by the completion of internal cybersecurity awareness training. By prioritizing and incentivizing cybersecurity education, Cowbell promotes taking preventative measures and quells worries about business continuity with its closed-loop approach to risk management.

Cowbell empowers risk managers to build resiliency and continuously improve the risk profile of their organization. Closed-loop risk management encompasses continuous risk improvement in four steps: **ASSESS, INSURE, IMPROVE, and RESPOND**. From initial discovery of the risk, all the way to recommendations to remediate cybersecurity weakness, Cowbell's closed-loop risk management is present each step of the way.

Furthermore, Cowbell supports continuous risk improvement and closed-loop risk management with four organizational pillars: Data Science, Underwriting, Risk Engineering and Claims.

Data Science

- 1,000+ risk signals
- Outside-in & inside-out
- Risk pool: 24M accounts
- 8 Cowbell Factors
- Spotlight

Underwriting

- Instant quoting/binding
- Dynamic UW referral
- Heatmap: dynamic risk portfolio assessment

Risk Engineering

- Cyber risk experts
- Pre & post bind
- 100s calls per month
- Stream of cyber advice to policyholders

Claims

- In-house cyber experts
- Respond fast
- Better insights on claims information
- Lower claim severity

Policyholders, agents, reinsurers and carriers greatly benefit from Cowbell's closed-loop risk management. Specifically, benefits include:

1. Proactive loss control (frequency and severity);
2. Sustained engagement of policyholders on mitigating cyber risk throughout the lifecycle of their policy;
3. Direct engagement with IT/Security contacts at policyholders, not just the administrator of the insurance policy;
4. Active guidance on risk remediation through calls with Cowbell's risk engineering team;
5. Increased perceived value of cyber policies - Cowbell shifts the value of insurance from a hypothetical "promise to pay" to tangible services and resources; and
6. Increased policyholder loyalty and satisfaction.

One of the reasons Cowbell Cyber is so cutting-edge is that we understand that successful cyber insurance policies depend on establishing strong cyber hygiene within an organization and outside of it (i.e., throughout the supply chain and across all third parties). This is of particular importance to Cowbell Cyber because we focus on businesses with revenue up to $250 million.

These are small- to medium-sized enterprises (SMEs) that may not inherently have the resources to prioritize cybersecurity awareness; yet SMEs are part of the backbone of many critical supply chains. Furthermore, a cyber incident at a small business can lead to damaging business interruptions for an entire sector.

In this quarter's Cyber Round-Up report, we discuss how we brought the evaluation of cyber risk performed through Cowbell Factors at the individual level to any portfolio or aggregated level. We also cover the mechanisms behind Cowbell's ability to proactively prevent cyber incidents by engaging policyholders throughout the lifecycle of a policy, what we refer to as Cowbell's Closed-Loop Risk Management.

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

SECTION ONE

Cowbell Factors: An Anchor for Individual and Aggregated Risk Evaluation

Individual Risk Evaluation

Cowbell's Q1 SME Cyber Round-Up report introduced Cowbell Factors: what they are, what they mean, and how we use them in underwriting. This quarter, we are introducing a new representation that is being rolled out to everyone on our technology platform - agents and brokers, policyholders and applicants, MSSPs, carriers, and reinsurers.

One important characteristic of Cowbell Factors is that they are a measure of an organization's risk relative to Cowbell's risk pool, which comprises more than 24 million SMEs. It is noteworthy that there are about 32 million SMEs in the U.S., so Cowbell's risk pool covers about 75% of Cowbell's target market. Cowbell Factors grade each organization on a curve, showing where it stands compared to the overall population of similar accounts. Similar accounts include those in the same class of business, or industry peers.

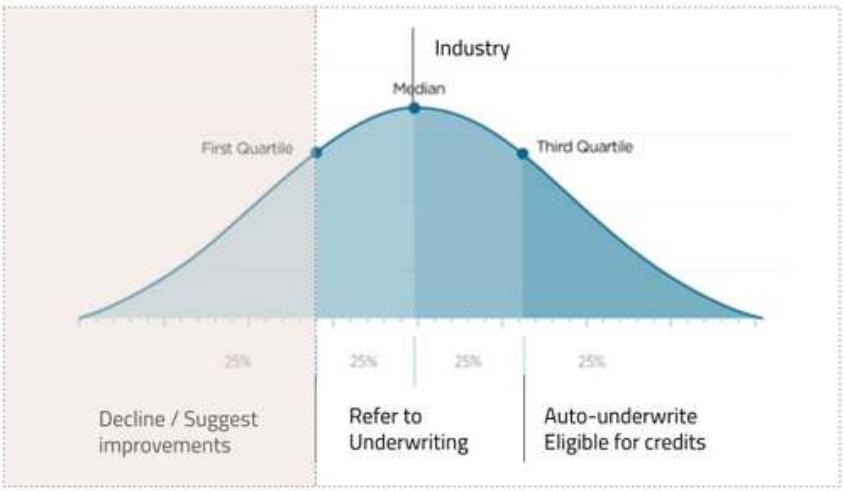

Figure 3: Grading risk on the curve

Based on the above, the most important information when interpreting any individual Cowbell Factor for an organization is to compare it to the industry average.

As a representation improvement to the representation, we are now making available the full representation of the Cowbell Factors with their industry averages, along with the minimum and maximum for each industry.

With the new representation (see figure 4), organizations can more easily understand where their cyber risk profile stands, whether they are more or less secure than industry peers and how close they might be to the extremes. Red and green color coding also gives an immediate indication of whether a specific Cowbell Factor is below or above the industry average.

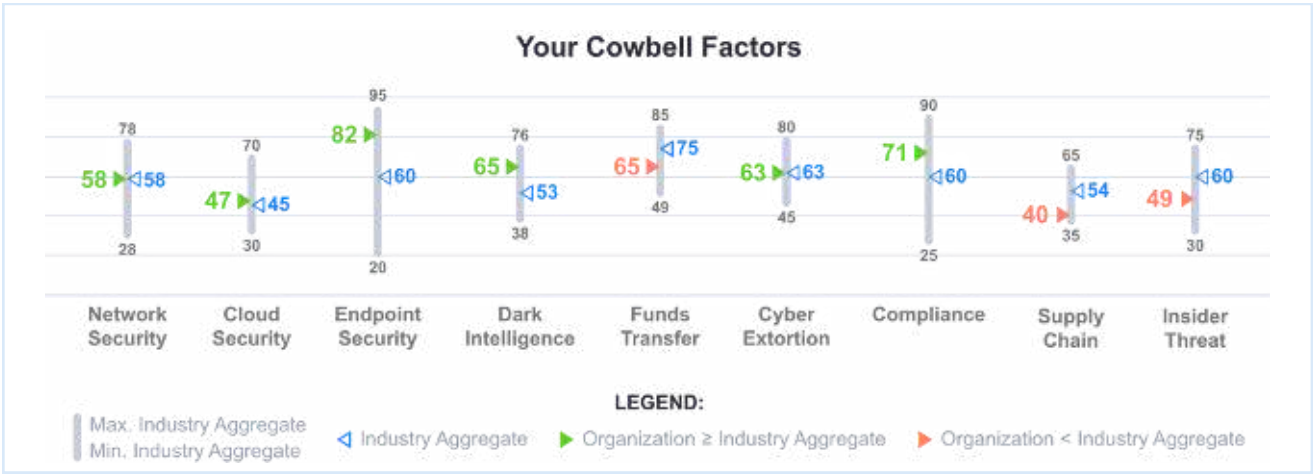

Figure 4: New representation of Cowbell Factors.

Evaluation of a Risk Portfolio

In addition to providing each account with a richer view of their risk profile, we introduced in May 2022 another innovation: the cyber risk heatmap. Agencies, brokerage firms, carriers, and other insurance entities with purview over a group of accounts can now gain immediate visibility into the health of a group of accounts.

The cyber risk heatmap is the market's most data-rich and dynamic evaluation of cyber risks for any group of accounts, relying on multivariate risk ratings - Cowbell Factors - which tap into more than 1,000 risk signals for each account.

The Cowbell Cyber Risk Framework underlying Cowbell Factors incorporates security controls from multiple standards (i.e., NIST Cybersecurity Framework, COBIT, Payment Card Industry Data Security Standard (PCI DSS) and the most recently revised NIST Cybersecurity Supply Chain Risk Management (C-SCRM) program) and is augmented by Cowbell's own controls. Through this Framework, Cowbell can capture and assess an individual organization's cyber posture in a single framework by normalizing outside-in and inside-out data collected during the insurance application process. The same information can be collated to analyze a portfolio of accounts at an aggregate level.

The complexity of assessing a cyber risk portfolio on a continuous basis is compounded by the complexity of assessing risk at the individual account level, creating blindspots for insurers where they face the most significant exposures, leaving uncertainty with regard to what to do about it. With data and AI, Cowbell reestablishes a direct link between the individual risk and the health of a risk portfolio.

Rajeev Gupta, Co-Founder and Chief Product Officer says, "With this new heatmap, we can analyze in minutes the standing of any insurance book of business. The Cyber Risk Framework gives us the confidence that every covered risk is assessed individually in the most rigorous manner while the heatmap contributes to maintaining a balanced book of business with each of our partners."

Cowbell's partners - agencies, carriers and re-insurers - as well as underwriters gain immediate visibility into the distribution of covered risk in their portfolio. The heatmap highlights the concentration of undesirable risk by class of business.

With such improved visibility, Cowbell and its insurance partners - brokers, insurance carriers and reinsurers - can team up to develop a balanced book of business and manage growth for profitability but also engage pools of policyholders into remediation actions improving the overall risk profile of the portfolio.

Figure 5: Heatmap for all accounts evaluated on Cowbell platform.
See Appendix I for descriptions of 2-digit NAICS codes

It is worth comparing the above with the population of accounts that carry an active cyber policy with Cowbell to see risk selection in action using Cowbell Factors.

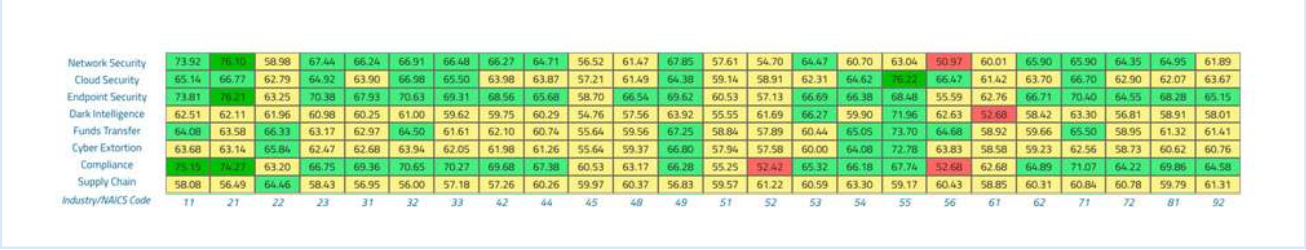

Figure 6: Heatmap for all accounts with an active Cowbell cyber policy.
See Appendix I for descriptions of 2-digit NAICS codes

SECTION TWO

The Happy Path Toward Coverage: Eligibility and Insurability

Many businesses seek to have a policy with Cowbell, but not all are accepted. For this report, we also looked at the population of businesses that requested cyber coverage with Cowbell, and the various factors that contributed to rejection.

This is where we can distinguish between two steps that businesses must validate.

Out of the initial account population automatically rejected by our digital process, 35% were ineligible for missing basic application information such as class of business or revenue, and we were not in a position to automatically retrieve and identify this information from our various third-party partners.

Out of the remaining eligible accounts, insurance rejection was due to the following:

- **83%** lack of encryption (sensitive data and communications)
- **8.5%** had a cyber claim history (note that Cowbell does not systematically reject accounts with claims but additional controls and validation is typically required on such accounts)
- **4%** for absence of security contact
- Poor controls, lack of cybersecurity awareness training covered the remaining of the rejections.

SECTION THREE

Staying Ahead of New Threats with Spotlight

Spotlight is an advanced feature of the Cowbell platform that dynamically matches zero-days to potentially impacted organizations. It allows Cowbell to react quickly to zero-days and the latest vulnerabilities as they make the news. Sourced from a variety of data channels (i.e., news feeds, Twitter handles, security companies and research teams), Cowbell Spotlight applies AI modeling to detect time sensitive risk and then notify affected policyholders of the vulnerability so they can address it. As a result, Cowbell is constantly ingesting and analyzing vulnerability intelligence. It is crucial to remedy these types of vulnerabilities before they become publicized and bad actors exploit them. Without Spotlight, Cowbell would be seeing many more claims.

Given the frequency with which risk changes, it is important for Spotlight to be agile and constantly updating. If a vulnerability is detected on a zero-day crawl, Spotlight identifies it in a proactive manner. The placement of a Spotlight on an account updates the Cowbell Factors in real-time and amplifies their risk exposure.

A Spotlight can be put on any risk attribute, manually or automatically. It is time-stamped and bound by a duration horizon that depends on the threat. When a Spotlight is put on a particular account, the risk attribute uses a proprietary decay algorithm to allow it to fade away over time. This may have a negative impact on the account at present, but after the vulnerability is eliminated and Spotlight resolved, it is important to stop penalizing accounts that have taken appropriate actions.

With 24 million accounts in Cowbell's risk pool, a spotlight can be attached to policyholders and non-policyholders. The Cowbell team proactively contacts policyholders that are flagged with a spotlight and engage them in active resolution of the risk exposure.

If placed on non-policyholder accounts, underwriters will automatically be notified of the amplified risk when the account is applying for cyber insurance. A similar process as with policyholders follows to help applicants address the vulnerability.

Though Spotlight is a relatively new addition to Cowbell's capabilities, there are already plans in place for its evolution going forward. Primarily, Cowbell sees a future in which every step of identifying zero-days and updating systems with risk information is fully automated.

In recent months, Spotlight and its external scanners were invaluable components in Cowbell's response to new threats, vulnerabilities with potentially broad impact such as the Apache Log4J vulnerabilities discovered in December 2021. The concept of Spotlight is used beyond software vulnerabilities to flag heightened cyber threats due to unexpected events - such was the case with the Russia/Ukraine conflict.

Utilizing external scanners, Cowbell was able to identify policyholders with assets, interactions, or other communications that would link them to Ukraine in order to proactively notify them and encourage precautionary measures. Proactive actions were obviously taken with active policyholders.

Overall, Cowbell estimates that it prevented hundreds of cyber events every month by proactively engaging policyholders in continuously improving their risk profile.

SECTION FOUR

Dark Web Exposures Are Critical

In Cowbell's Q1 SME Cyber Round-Up report, we reported on the range of values of Cowbell Factors (minima and maxima) for all accounts submitted for insurance. Last quarter, the analysis was only provided for the aggregate Cowbell Factor. This quarter, we focused on the Dark Intelligence Cowbell Factor, which is primarily driven by the amount of data exposed on the dark web that we discover through our partnership with DarkOwl.

Our findings can be found in the figure below. It is worth noting the spread of ratings. While the maxima are somewhat consistent across all industries, the minima tell the story of industries challenged by data leakage: Healthcare and Retail Trade.

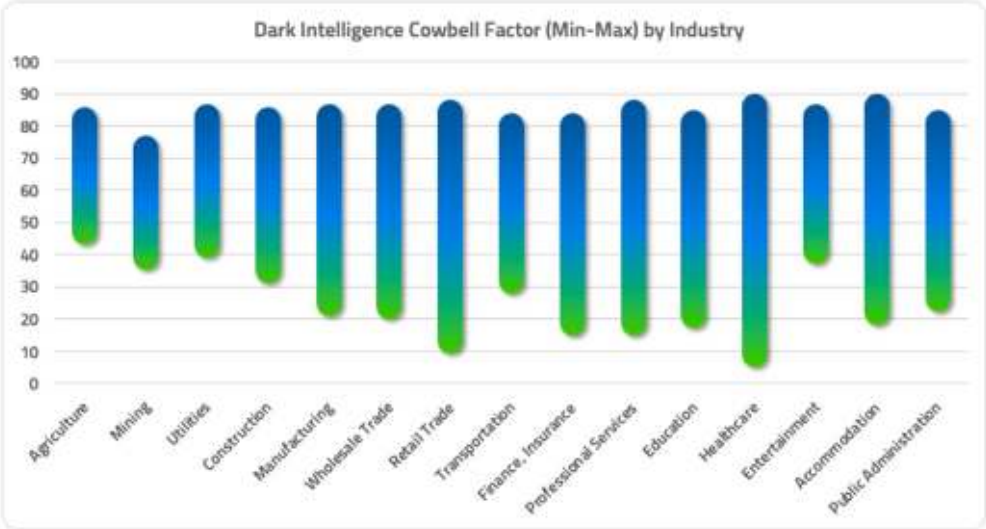

Figure 7: Dark Intelligence Cowbell Factor - min and max by industry

Having information leaked on the dark web is a reliable sign that your organization might soon fall victim to a cyber incident if the compromised data includes credentials. For more information on this topic, please refer to our recent blog post, "Your information is on the dark web, now what?", in which Cowbell's risk engineering team provides recommendations on what to do when sensitive information is discovered on the dark web.

SECTION FIVE

Continuous Underwriting: The Future of Cyber Insurance

A key distinguishing feature of the Cowbell experience is our ability to continuously underwrite risks. This means that Cowbell is constantly, and continuously, reassessing policyholder risk and exposures in light of the ever-changing climate of the risk pool, and using that information to underwrite.

The Gallagher Re Q1 Global Insurtech Report asserts, "While technology can certainly help to reduce costs, can support underwriting decisions, assess capital optimization across portfolios of risk etc., pricing risks correctly and having the experience to deliver well-strategized underwriting plans are still at the heart of insurers who will be profitable." In other words, there is a gap between portfolios and the risk that is covered. Cowbell seeks to reestablish that link and continuously monitor it by adding clarity to the written risk, as well as how that risk changes due to evolving cyber threats. The agility and adaptability of this process benefits policyholders as they are able to mitigate some of this risk on an ongoing basis.

Cowbell underwriters put context on the above challenges. In past roles, they might have used as many as five different tools to get to basic information needed to underwrite cyber. At Cowbell, not only do they get access to a lot more information about every risk they underwrite, but the information is already sanitized and readily available in one place. This allows underwriters at Cowbell to process 10 times as many accounts and do so with more precision than they were able to in previous roles. Better yet, all the information about the accounts' profiles and risk exposures are accessible in one place.

Here are some of the specific comments that our underwriters shared and what they consider to be the best part about underwriting with the Cowbell platform.

"The readiness, the quickness, the robustness, I can go on and on. But the key feature is how free-flowing and fluid it is and this makes it incredibly efficient to use on a daily basis."

"The ability to make quick and smart decisions due to the open-ended underwriting guidelines, which are designed to help us assess unique risks creatively and analytically rather than box-underwriting. We can apply our cybersecurity expertise and demonstrate our understanding of the risk and its inherent deficiencies via the Cowbell Factor model. I couldn't ask for more!"

"I love how you can quickly dive into a risk and see the scans. The automation is great!"

"Using Cowbell Factors and Cowbell Insights. The data provides a level of comfort understanding and having the insured address the security requirements."

The above comments illustrate Cowbell's unique underwriting approach which is not only beneficial for underwriters but also for policyholders: Cowbell shares all findings back with insurance applicants including opportunities to rapidly improve their cyber risk profile. All around, Cowbell's continuous risk assessment and continuous underwriting process are the linchpins of our closed-loop approach to risk management that distinguishes Cowbell from competitors in the market.

APPENDIX I

There are twenty sectors included in the NAICS at the two digit level. Below are the descriptions:

SECTOR	DESCRIPTION
11	Agriculture, Forestry, Fishing and Hunting
21	Mining, Quarrying, and Oil and Gas Extraction
22	Utilities
23	Construction
31-33	Manufacturing
42	Wholesale Trade
44-45	Retail Trade
48-49	Transportation and Warehousing
51	Information
52	Finance and Insurance
53	Real Estate and Rental and Leasing
54	Professional, Scientific, and Technical Services
55	Management of Companies and Enterprises
56	Administrative and Support and Waste Management and Remediation Services
61	Educational Services
62	Health Care and Social Assistance
71	Arts, Entertainment, and Recreation
72	Accommodation and Food Services
81	Other Services (except Public Administration)
92	Public Administration