cowbell®

CYBER ROUND-UP REPORT

# The Positive Impact of Inside-Out Data

Q3, 2023

As an emerging line of insurance, the cyber insurance market continues to establish its foundation to sustain profitable growth, drive adoption in underserved market segments (i.e., the small and medium-sized enterprise (SME) market), and bring visibility, if not predictability, to the risk covered.

Identifying, quantifying, monitoring, and ultimately predicting cyber risk is an interesting challenge. On one hand, the threat landscape itself is rapidly evolving – historical data is no predictor of the future – but consistently collecting thousands of cybersecurity data points for each organization in a large population of businesses is daunting given that every organization uses a different technology stack. Normalization, categorization, and comparison of the information collected is incredibly complex. This is where data science and artificial intelligence become instrumental, providing scale to any experienced analysts in the field.

In this report, we will examine the challenge of collecting useful data along two dimensions: areas where the data is already normalized and areas where the quality of the data is significantly better because of its inside-out nature, meaning that it was provided directly by the organization.

Likewise, outside-in information is incredibly useful to evaluate the cyber risk profile of an organization. Data about the scope of a company's internet footprint, its attack surface, the presence of compromised information on the dark web, the use of unpatched software on its internet-facing infrastructure and much more are all necessary information to collect. In most cases, such information is already normalized by design, making comparison across businesses feasible.

It can get a lot more complicated when collecting inside-out data on the tech stack of organizations as there are no two companies that deploy the same technology in the same fashion.

Except in the cloud...in many, if not most, cases.

Cloud deployment of commonly used tools and applications brings a level of consistency that is a game changer when it comes to understanding the relative exposures of an organization against a set population.

In the SME market, collaboration tools such as email services and web properties often represent the majority of the digital footprint of an organization and are the primary targets for cyberattacks. Obtaining inside-out risk data from Microsoft 365, Google Workspace (Gmail and GSuite) and broadly deployed web security tools such as Cloudflare has been a focus of Cowbell.

In the cloud deployment of email services such as Microsoft 365 (formerly known as Office 365), we can examine and compare the relative risk related to a deployment of Microsoft 365.

This report analyzes the risk profile of accounts that have proactively provided Cowbell with inside-out data by activating an integration with one of their infrastructure providers. At Cowbell, we call these "Connectors." More specifically, this report focuses on the connector to Microsoft Secure Score which centralizes visibility into **your current security posture and identifies potential improvements across all your Microsoft 365 workloads including Microsoft 365 for email service.**

## Policyholders providing inside-out risk information show lower level of risk

As shown in figure 1, Cowbell policyholders that took the step to activate the Cowbell connector to Microsoft show on average a much better risk profile compared to the entire population of Cowbell policyholders and also as they relate to their industry peers. Cowbell measures the risk profile of an organization through its Cowbell Factors, which consist of the overall Company Cowbell Factor and specific factors for each main cyber risk area: Network Security, Cloud Security, Endpoint Security, Dark web, Extortion, Fraudulent fund transfer, Compliance, and Software Supply Chain.

***Note**: "Non-policyholders" represents accounts submitted to Cowbell for cyber insurance that did not result in a policy. These accounts were either declined or opted for another provider.*

***(*)Note**: All Cowbell policyholders on Cowbell Prime 250 cyber insurance are incentivized to optimize their premium by activating a connector and getting eligible to a 5% premium credit.*

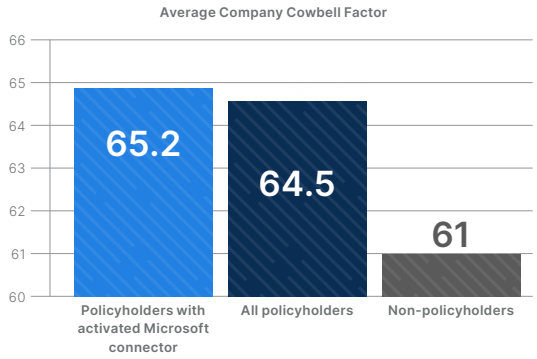


**Figure 1** - comparison of the average of the company level Cowbell Factor across three populations

We attribute this positive comparison to the following:

1. **Strong culture of cybersecurity**: the organization has a strong culture of cybersecurity and takes advantage of every resource available to evaluate and improve their cybersecurity posture and risk profile. As such, the organization seeks out and optimizes their insurance experience by taking advantage of risk management resources bundled with every Cowbell policy.
2. **Faster identification and remediation of security weaknesses**: The Cowbell connector to Microsoft provides direct visibility into the level of adherence to security best practices for Microsoft 365 and other components of Microsoft cloud services. This allows the organization to immediately remediate identified gaps and vulnerabilities.
3. **Insurance premium sensitivity**: the organization is price sensitive and looks for avenues to optimize its insurance premium. With Cowbell, organizations that activate a connector become eligible to a 5% premium credit(*) regardless of the insights to which we gain access.
4. **Audit call with Cowbell Risk Engineering Team**: if the organization took advantage of Cowbell's cyber risk engineering resources, they most likely had the opportunity to better understand the value and benefits of activating connectors.

## Industries where the Cowbell connector for Microsoft has the most significant impact

Not all industry sectors treat cybersecurity with the same level of priority. This is evident in their risk profiles as we compare the policyholders with an activated connector to Microsoft to their respective industries.

Policyholders in the seven industries highlighted in the graph below have activated the connector to Microsoft and show even more improvements in their risk profile than other industries.

It is no surprise to see policyholders in Finance & Insurance with the highest positive delta to their industry average. Those that activate the connector will make the full use of it.

We can also attribute the high performance of healthcare, education and public administration sectors to the closer attention from Cowbell Risk Engineering Team, since these industries have historically lacked resources for comprehensive cybersecurity.

## The positive delta is even more significant for the Extortion Cowbell Factor

It's notable that Cowbell policyholders outperformed their industry peers across every single Cowbell Factor, but the Extortion Cowbell Factor is especially significant. The Extortion Cowbell Factor measures an organization's potential exposure to extortion-related attacks such as ransomware, so it is particularly interesting to analyze how policyholders with an active connector to Microsoft are performing with regards to that exposure. The Cowbell connector to Microsoft brings insights focused on the security configuration of Microsoft Cloud Services including collaboration tools such as email or video conferencing. These insights have a direct influence on the Extortion Cowbell Factor.

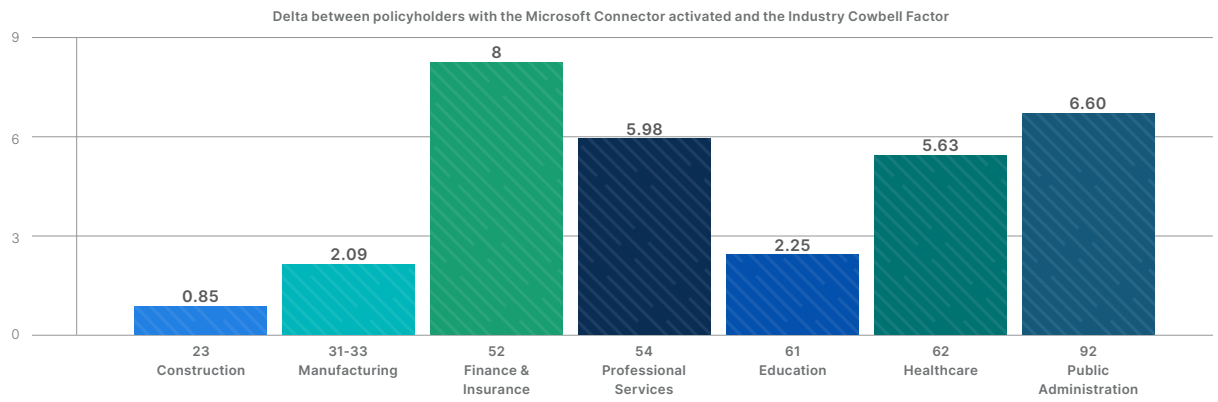


**Figure 5** - delta between Policyholder Cowbell Factor and the industry Cowbell Factor for key industries and policyholders with the Microsoft Connector activated

Again, the population of policyholders with an active connector to Microsoft is presenting a much better risk profile than any other population.

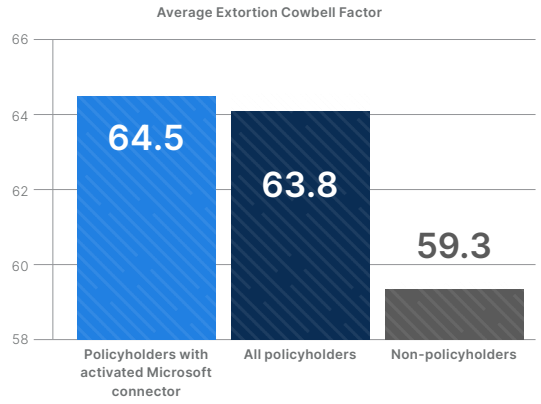


**Figure 4** - comparison of the average of the Extortion Cowbell Factor across three populations

## The same industries show a significant delta compared to the industry average

It is important to note the same graphical trend when redoing the same comparison as in Figure 2 for the Extortion Cowbell Factor.

## Summary

It is often reported that SMEs are more susceptible to cyber incidents than their larger counterparts because they don't have adequate resources to properly tackle cybersecurity challenges.

Cowbell is a cyber insurer focused on solving for this insurability gap by intentionally serving the SME market and in this report, we wanted to showcase the wealth of information we make available to SME policyholders so that they can rise to the challenge and build cyber resilience with the services made available to them through a cyber policy. The Cowbell connector for Microsoft is one of the many tools that comes bundled free of charge with every policy issued by Cowbell. Access to cybersecurity awareness training for employees and risk engineering services to remediate identified exposures are some of the most in-demand solutions that have made a difference for thousands of organizations and prevented cyber incidents.

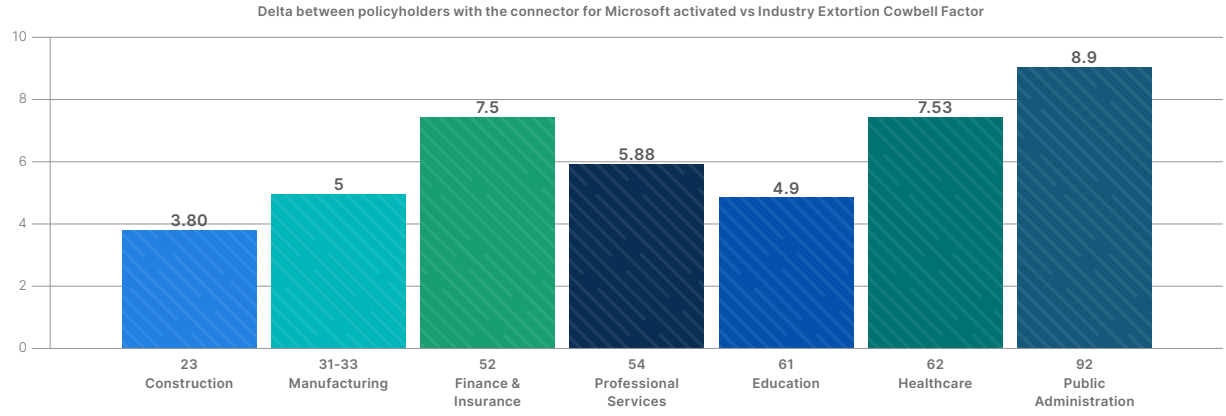


**Figure 5** - delta between Policyholder Cowbell Factor and the industry Cowbell Factor for key industries and policyholders with the Microsoft Connector activated

# Adaptive Cyber Insurance

support@cowbellcyber.ai

(833) 633-8666

cowbell.insure