Analysis of Cowbell Factor for Software Supply Chain

(Preview of Findings on Small and Mid-Size Businesses)

INTRODUCTION

Cowbell Factors provide an organization's cyber risk profile as a relative rating against Cowbell's risk pool. The factors are specifically designed for insurance purposes and anchor risk selection and underwriting for cyber insurance - the higher the factors, the more insurable the risk.

To capture the complexity of cyber risks, Cowbell Factors define an organization's cyber risk profile in seven areas: Network Security, Cloud Security, Endpoint Security, Dark Intelligence, Funds Transfer, Cyber Extortion and Compliance. With the rise of massive attacks on the Software Supply Chain, Cowbell is introducing an eighth factor to evaluate the exposure to and strength of an organization's controls against such attacks.

Figure 1: Example of Cowbell Factors on an anonymous account

The compilation of the newly developed Cowbell Factor for the Software Supply Chain is based on more than twenty data sources including data and risk signals from firmographic and technographic third-party databases, proprietary scanners, historical claim compilations, and public libraries of exploits and vulnerabilities. Overall more than 750 data points and risk signals are ingested on each account to model and compile Cowbell Factors.

SOFTWARE SUPPLY CHAIN EXPOSURES - INDUSTRY ANALYSIS

Industries with the lowest Supply Chain Cowbell Factor and therefore representing the greatest risk associated with Software Supply Chain risk are Mining and Hospitality (Accomodation and Food Services). The low rating is due to a combination of high exposure to Software Supply Chain risks and weak controls over such risks.

The four industries with lowest exposure overall (due to either low exposure, strong controls, or both) are Agriculture, Arts and entertainment, Financial Services, and Healthcare.

As part of our modeling and compilation of this new Cowbell Factor, four industries were identified as standing out for weak controls over software supply chain cyber exposures: Public Services, Education, Hospitality, and Transportation. Financial Services and Entertainment (media) stand out for strong controls:

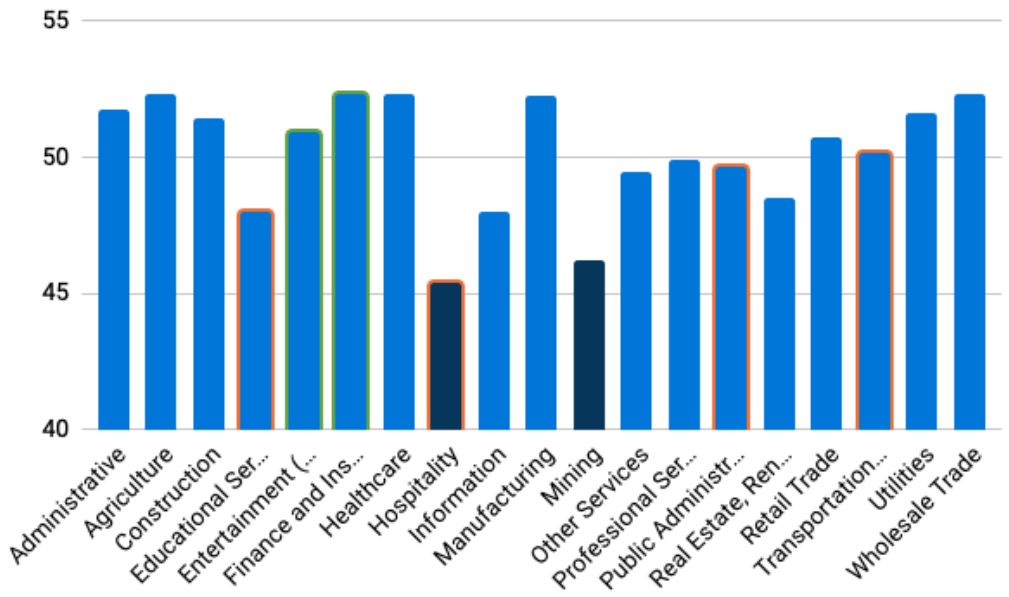

Figure 2: Supply Chain Cowbell Factor by Industry

(Legend: Industries highlighted in green have the best controls over Supply Chain risks, while industries in red have the weakest controls)

THE IMPACT OF OPEN SOURCE SOFTWARE

According to the 2021 State of the Software Supply Chain[1], the world witnessed a 650% increase in software supply chain attacks in 2021, aimed at exploiting weaknesses in upstream open source ecosystems.

The model supporting the compilation of the Supply Chain factor includes the use of Open Source software. The analysis validated that Education is one of the industries facing great exposure to open source both in terms of broad use of open source and weakness of controls applied, by comparison to industries like healthcare or manufacturing.

The analysis found frequent use of open source software in the Education sector in internet facing infrastructure among others, along with a general lack of systematic deployment of security best practices such as patching.

DISTRIBUTION OF THE SUPPLY CHAIN COWBELL FACTOR

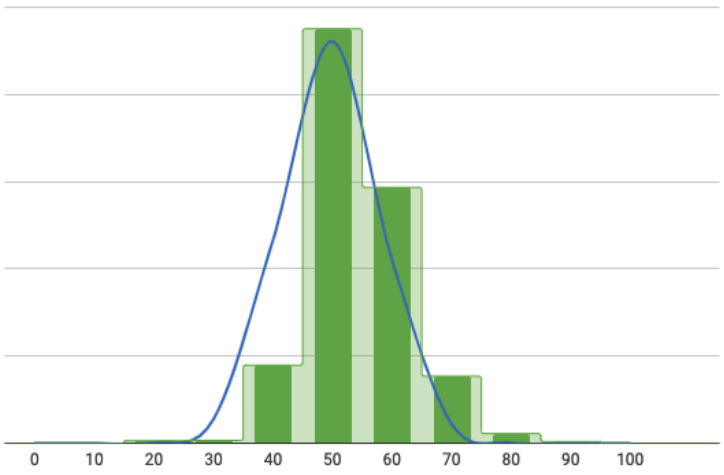

Figure 3: Distribution of the Supply Chain Cowbell Factor

Distribution of Supply Chain Cowbell Factor - accounts <$100 million of revenue

The average Supply Chain Cowbell Factor for accounts with less than $100 million in revenue is 50.0 with a minimum at 16.8 and a maximum at 89.5.

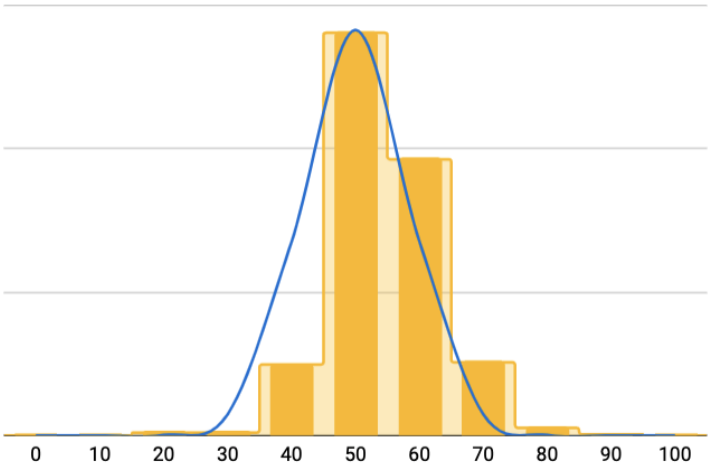

Figure 4: Distribution of the Supply Chain Cowbell Factor for analyzed accounts with less than $100million in revenue

Distribution of Supply Chain Cowbell Factor - accounts >$100 million of revenue

The average Supply Chain Cowbell Factor for accounts with more than $100 million in revenue is 49.9 with a minimum at 29.9 and a maximum at 79.1.

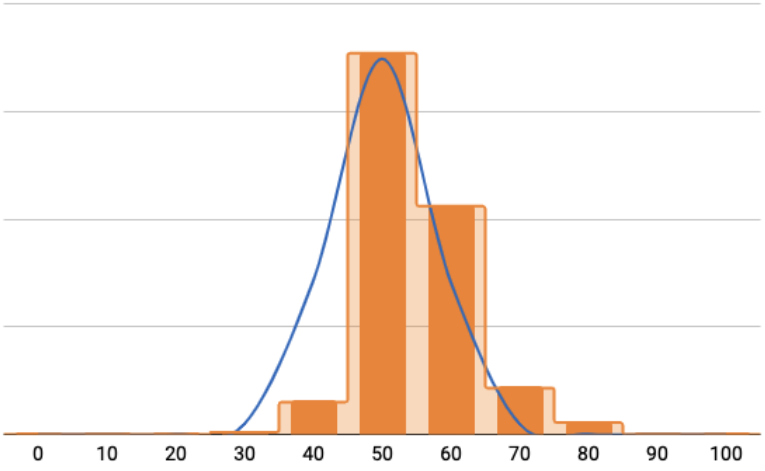

Figure 5: Distribution of the Supply Chain Cowbell Factor for analyzed accounts with more than $100million in revenue

Range of Supply Chain Cowbell Factor by Industry

Cowbell Factors vary significantly within an industry. The level of digitization and cybersecurity investment to maintain deployed IT infrastructure along with related security controls are unique to each organization creating risk exposure disparities as measured by Cowbell Factors, and, in this case, Cowbell Factor for Software Supply Chain.

While Utilities seems fairly homogeneous, Professional Services, Construction, Manufacturing, Wholesale Trade and Financial Services have the greatest disparity with organizations scoring from low two-digits up to 90.

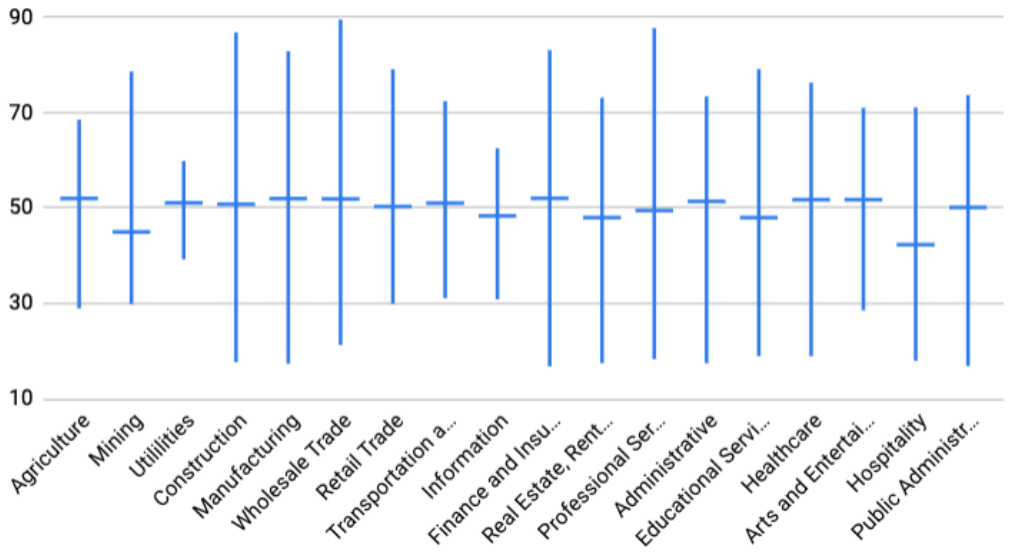

Figure 6: Range (max, min and average) of Supply Chain Cowbell Factor by Industry

STATE ANALYSIS

Surprisingly, a large state like New York appears as a state with one of the highest Cowbell Factor for Supply Chain representing the lowest exposure to Software Supply Chain risk. This could be explained by a concentration of financial institutions which have historically deployed a strong set of controls on software.

Worth noting is Nebraska being singled out as a state with great exposure to the software supply chain.

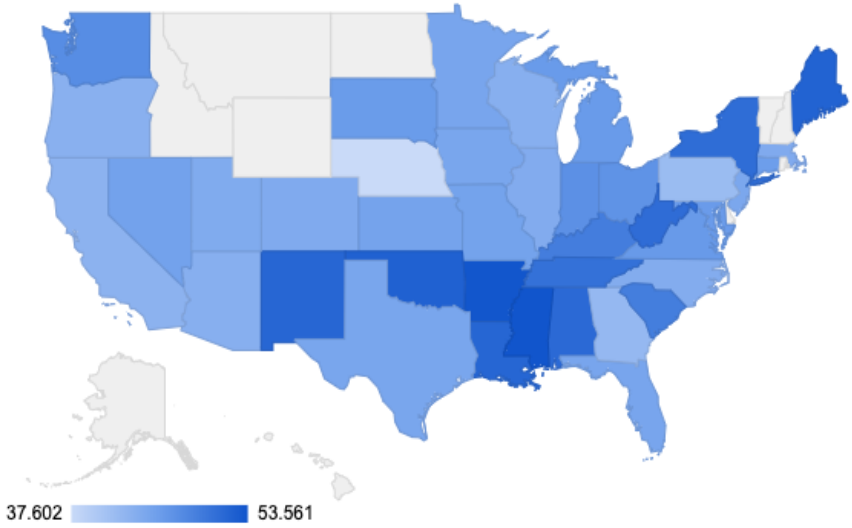

Figure 7: Supply Chain Cowbell Factor by State

(Note: for this initial analysis, 10 states were excluded from the results for insufficient representation in the analyzed account population. They appear in grey in the above map.)

Methodology:

This initial analysis of the newly deployed Cowbell Factor for Software Supply Chain is based on a dataset sampled from Cowbell's risk pool that now represents more than 50% of U.S. small and mid-size businesses.

All available data sources and risk signals were applied to the model providing a complete assessment of the sample for Software Supply Chain risk.

Sources:

[1]Sonatype: The 2021 State of the Software Supply Chain