BLACK KITE

THE BIGGEST Third-Party Risk in Manufacturing

A Wake-Up Call for an Industry Vital to a Web of Supply Chains

2024 REPORT

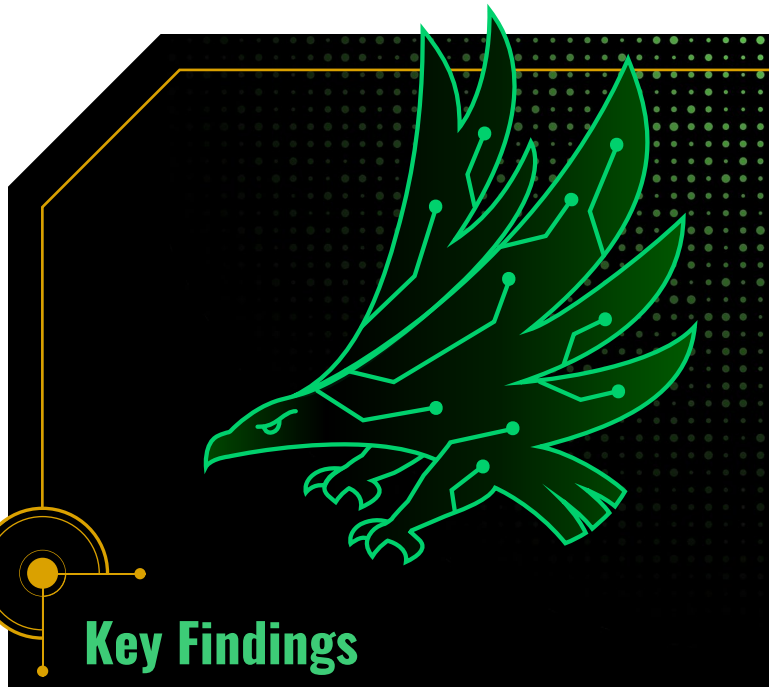
Table of Contents

Executive Summary: Critical Insights into Manufacturing's Third-Party Risk Landscape

What are the real-world risks posed to companies in the manufacturing industry by their third-party vendor ecosystems? And what exactly is at stake? To find out, the Black Kite Research & Intelligence Team (BRITE) conducted an in-depth analysis of a representative sample of manufacturing companies. This sample focuses on firms with annual revenues exceeding $1 billion operating in ten key sub-industries, representative of companies with robust third-party networks typically seen in the manufacturing sector.

Using the Black Kite platform, we evaluated these companies through multiple lenses to uncover the likelihood of data breaches and cyberattacks. We also drew specific insights from our latest ransomware report, State of Ransomware 2024: A Year of Surges and Shuffling focusing on how these threats impact the manufacturing industry.

As you explore this report, consider where your company falls within these statistics and what steps you can take to mitigate these risks.



Key Findings

- **Manufacturing is the top target for ransomware groups,** accounting for 21% of all ransomware attacks in the **past year.**
- **Ransomware Susceptibility Index® (RSI™)** scores for every manufacturing sub-industry on average exceed the critical threshold, placing them at significantly heightened risk. Companies in this range are 3.4 (or more) times more likely to suffer a ransomware attack compared to those in the lowest RSI range.
- **More than half of companies** in most sub-industries are in the critical "yellow," "red," or "dark red" RSI ranges, indicating high susceptibility to ransomware.
- **80% of manufacturing companies** have critical vulnerabilities, making them ripe for exploitation.
- **Poor patch management** is pervasive across the industry, representing an easily addressable yet widely neglected area of risk.
- **30% of companies** are in the critical zone for application security, underlining a pressing need for improvements.

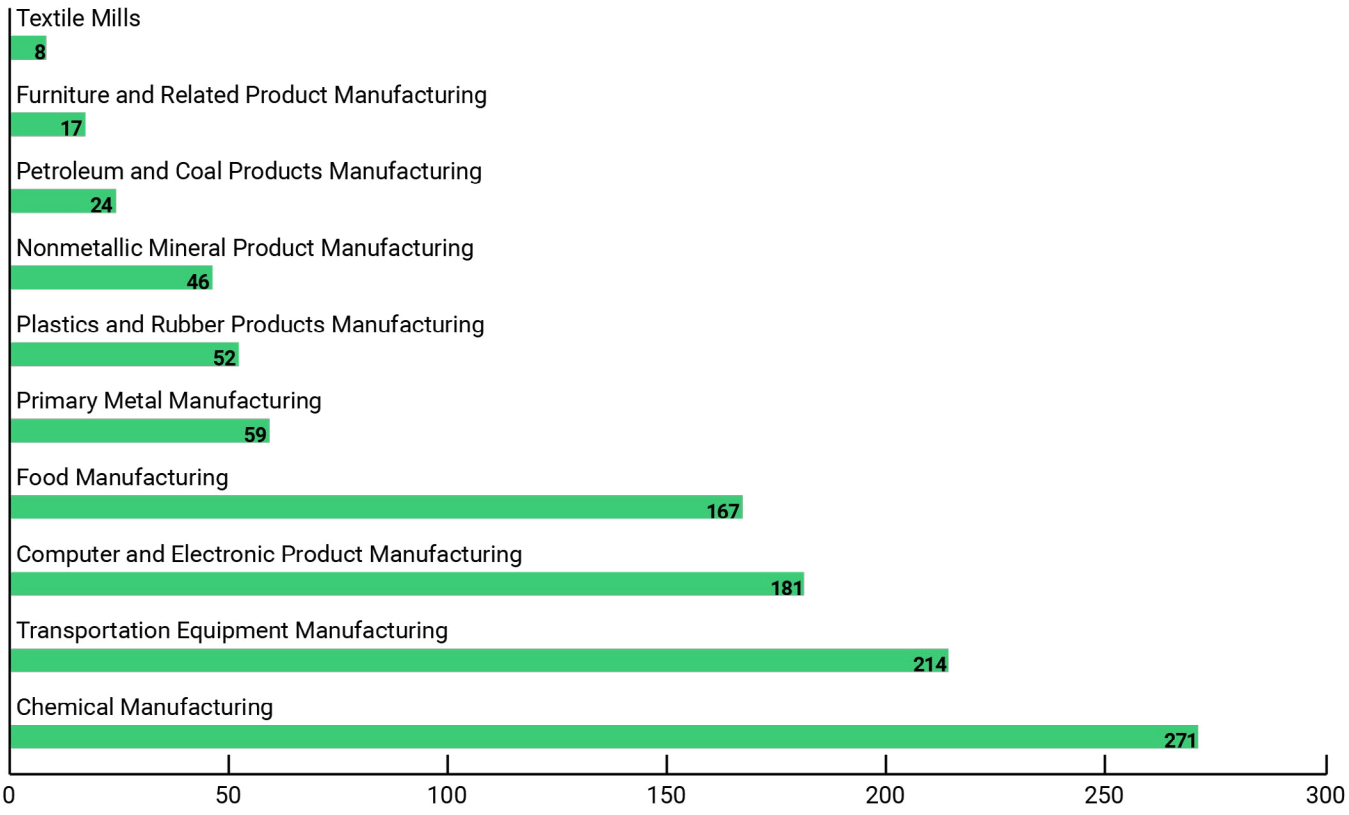
Research Scope

The companies analyzed were selected from the following sub-industry categories, all with annual revenues exceeding $1 billion. Source: Usearch

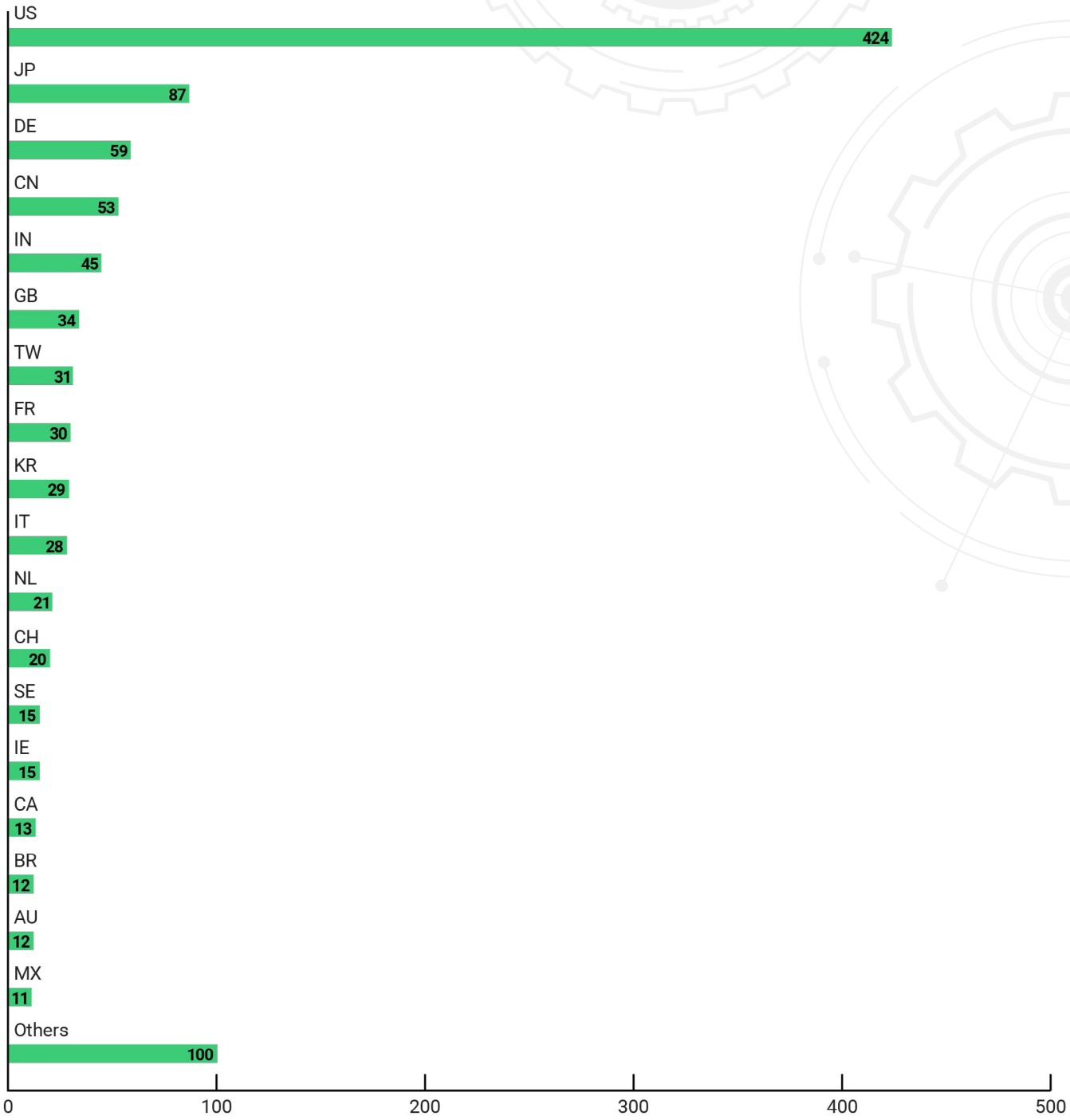
NAICS CODE	INDUSTRY NAME	NAICS CODE	INDUSTRY NAME
325	Chemical Manufacturing	311	Food Manufacturing
336	Transportation Equipment Manufacturing	331	Primary Metal Manufacturing
334	Computer and Electronic Product Manufacturing	326	Plastics and Rubber Products Manufacturing
327	Nonmetallic Mineral Product Manufacturing	337	Furniture and Related Product Manufacturing
324	Petroleum and Coal Products Manufacturing	313	Textile Mills

TOTAL SAMPLE SIZE: 1,039 COMPANIES

NUMBER OF COMPANIES IN EACH SUBINDUSTRY



COUNTRY DISTRIBUTION

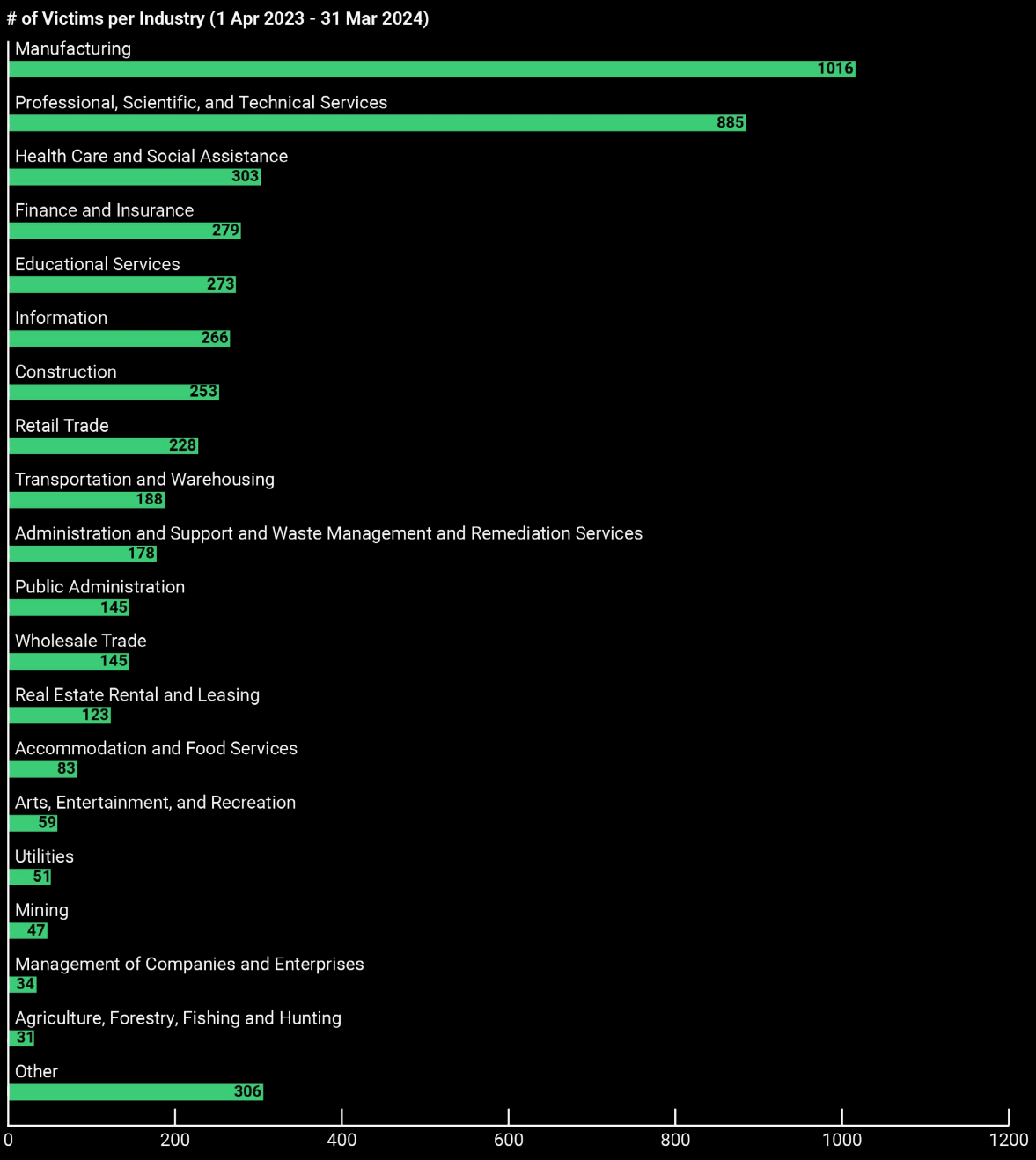


Ransomware: The #1 Threat

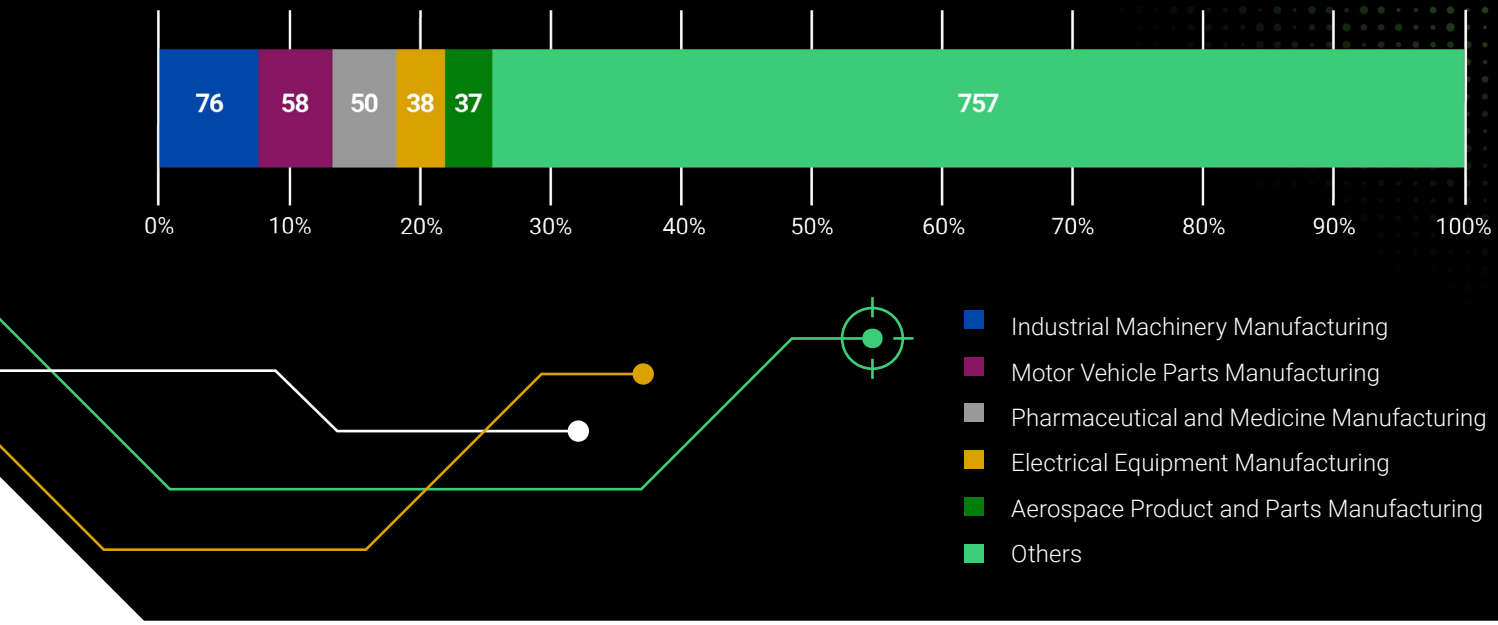
Historical Attacks

Across all industries, manufacturing is the number one target for ransomware groups, representing 21% of all ransomware attacks.

RANSOMWARE ATTACKS ACROSS INDUSTRIES



RANSOMWARE ATTACKS IN MANUFACTURING



Our Analysis

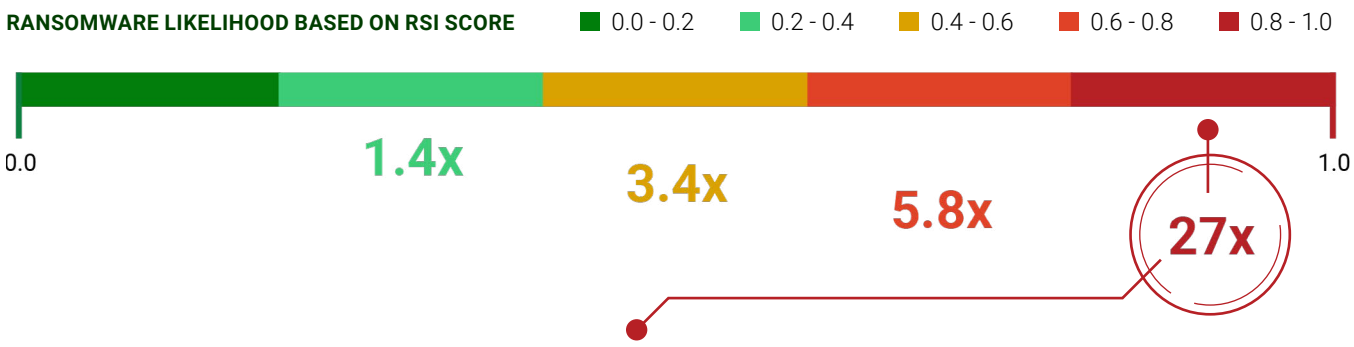
The manufacturing sector's rapid digital transformation post-COVID-19 has inadvertently turned it into a prime target for ransomware attacks. Cybersecurity defenses, often robust against operational technology (OT) threats, have not kept pace with the sector's expanded digital footprint, leaving a chink in the armor for cybercriminals to exploit. The industry, which leads with over a thousand ransomware victims, faces unique challenges due to the operational disruption that halts production lines, causing significant financial and reputational damage.

The pressure exerted by halting a manufacturing line is not lost on ransomware groups. They recognize the cascading effect of disrupting supply chains, as elucidated in our 2024 Third-Party Breach Report, which ranks ransomware as the second leading cause of third-party data breaches. Delving into the manufacturing sub-sectors, the spread of ransomware is indiscriminate. Industrial Machinery Manufacturing tops the list with 76 victims, followed by Motor Vehicle Parts Manufacturing at 58, and Pharmaceutical and Medicine Manufacturing at 50. Electrical Equipment and Aerospace Product and Parts Manufacturing are not far behind, with 38 and 37 victims respectively, highlighting the cybercriminals' calculated approach to inflict maximum disruption across various facets of the industry.

This assault on manufacturing is a clarion call for the sector to fortify its cyber defenses, aligning its security posture with the evolving threat landscape to mitigate the risk of becoming the next ransomware statistic.

Future Attacks

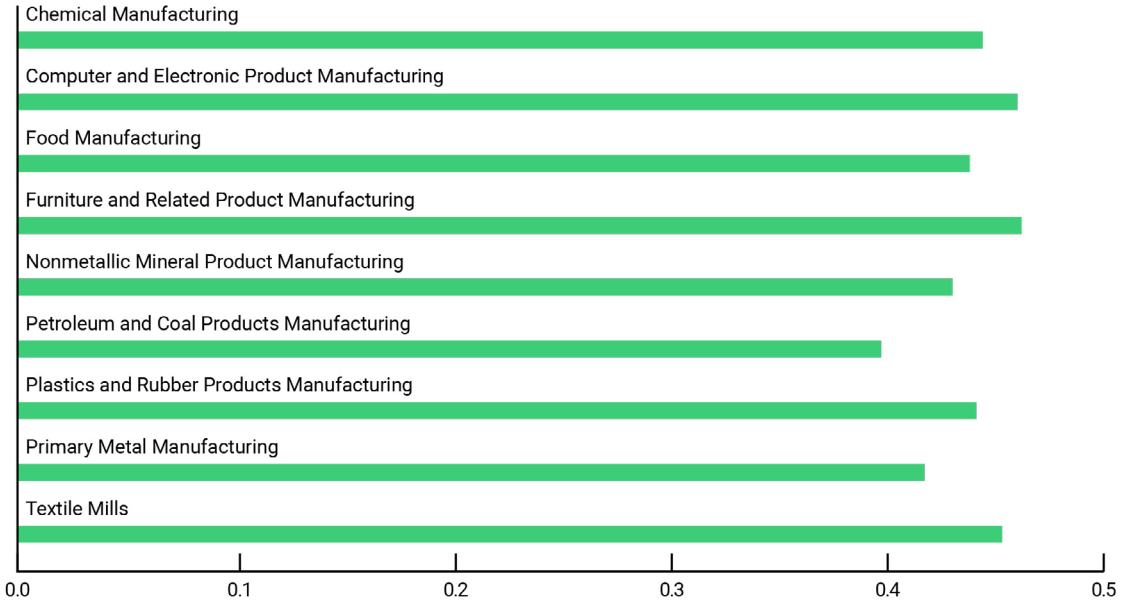
Ransomware Susceptibility Index® (RSI™) is a pioneering metric developed by Black Kite to measure the likelihood of a company falling victim to a ransomware attack. By analyzing relevant key risk vectors and using real-time data, the RSI™ provides a precise, quantifiable score that helps organizations identify their vulnerabilities, prioritize security improvements, and proactively defend against ransomware threats.



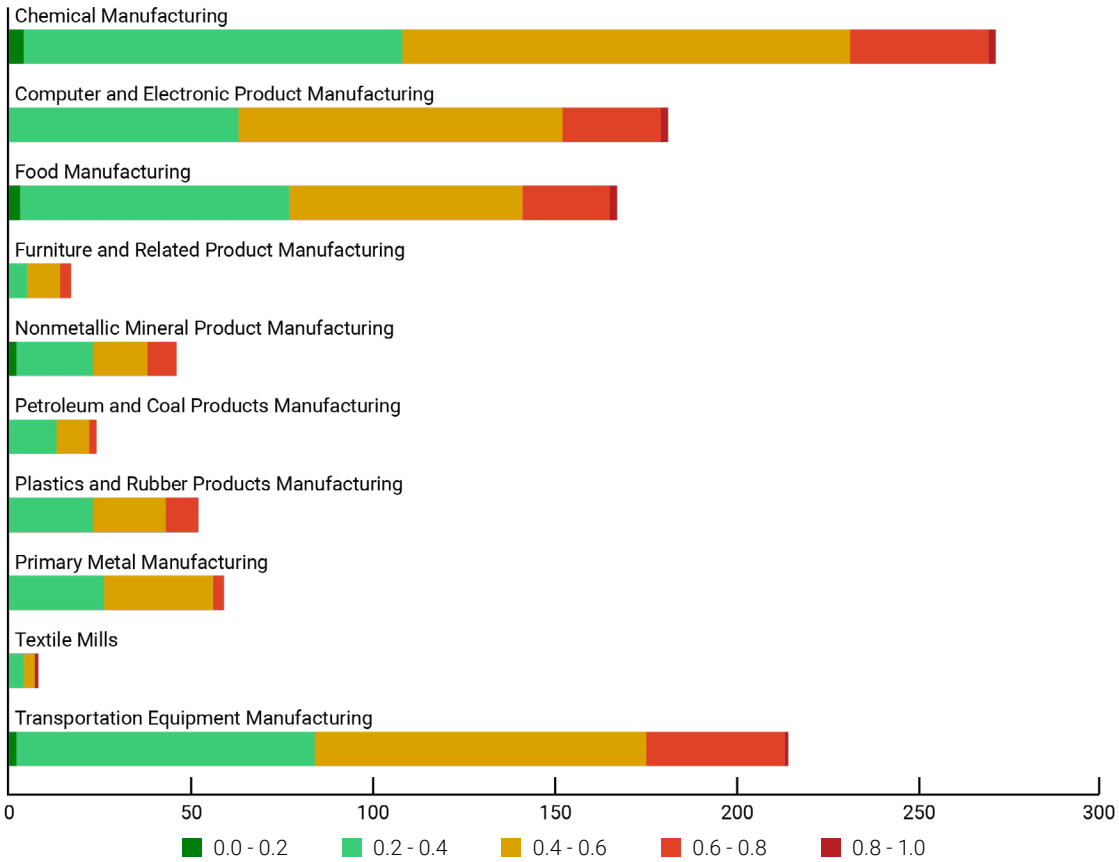
The companies with an RSI™ Value in this range are 27 times more likely to experience ransomware attacks than the companies with an RSI™ Value below 0.2.

Ransomware Susceptibility Index® (RSI™) scores indicate a critical risk across all manufacturing sub-industries.

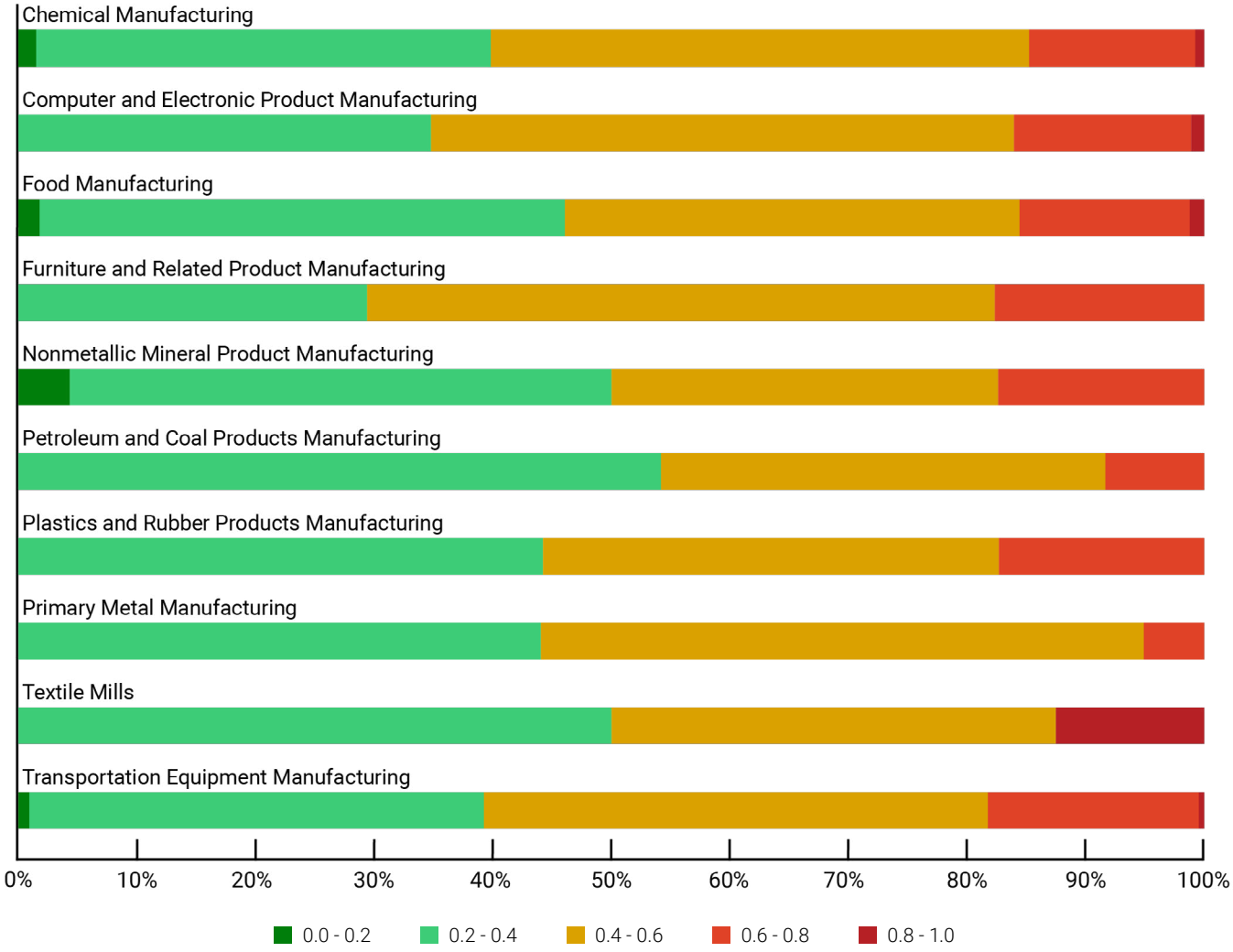
RSI AVERAGES



RSI DISTRIBUTION



RSI DISTRIBUTION IN %



Our Analysis

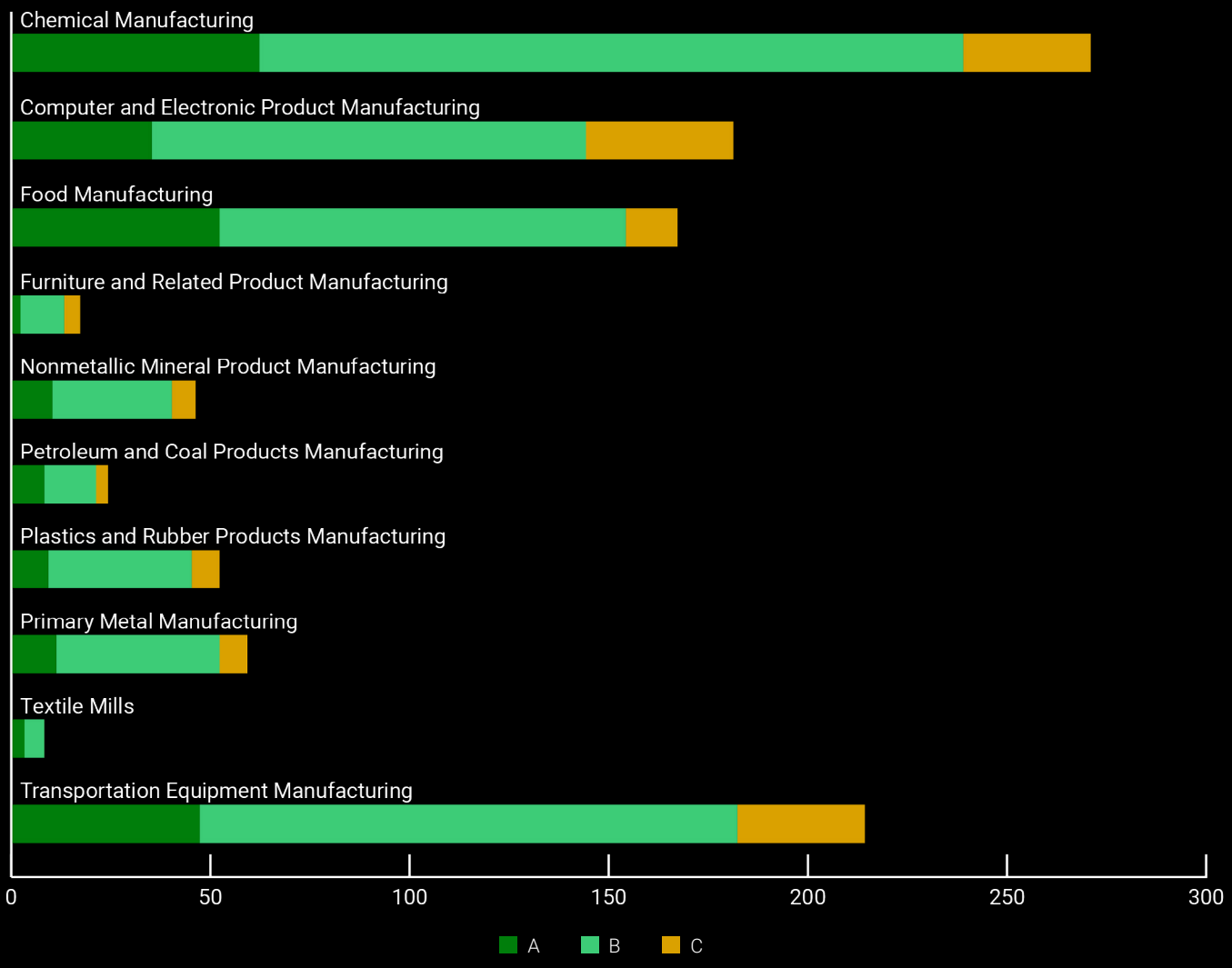
It's no surprise that manufacturing is the top target for ransomware groups, as revealed in the previous section, when we examine the RSI scores. Every sub-industry in manufacturing scores an average of 0.4 or greater, placing them in the critical category, meaning they are 3.4 times more likely to experience a ransomware attack than companies with RSI scores below 0.2.

When we analyze RSI scores by sub-industry, we see that more than half of the companies are highly susceptible to ransomware attacks. In Furniture and Related Product Manufacturing, for instance, 71% of companies fall into the critical category or higher. Furthermore, in sub-industries like Transportation Equipment Manufacturing, approximately 18% of companies are in the red zone, making them 5.8 times more likely to be attacked than a company with an RSI value below 0.2.

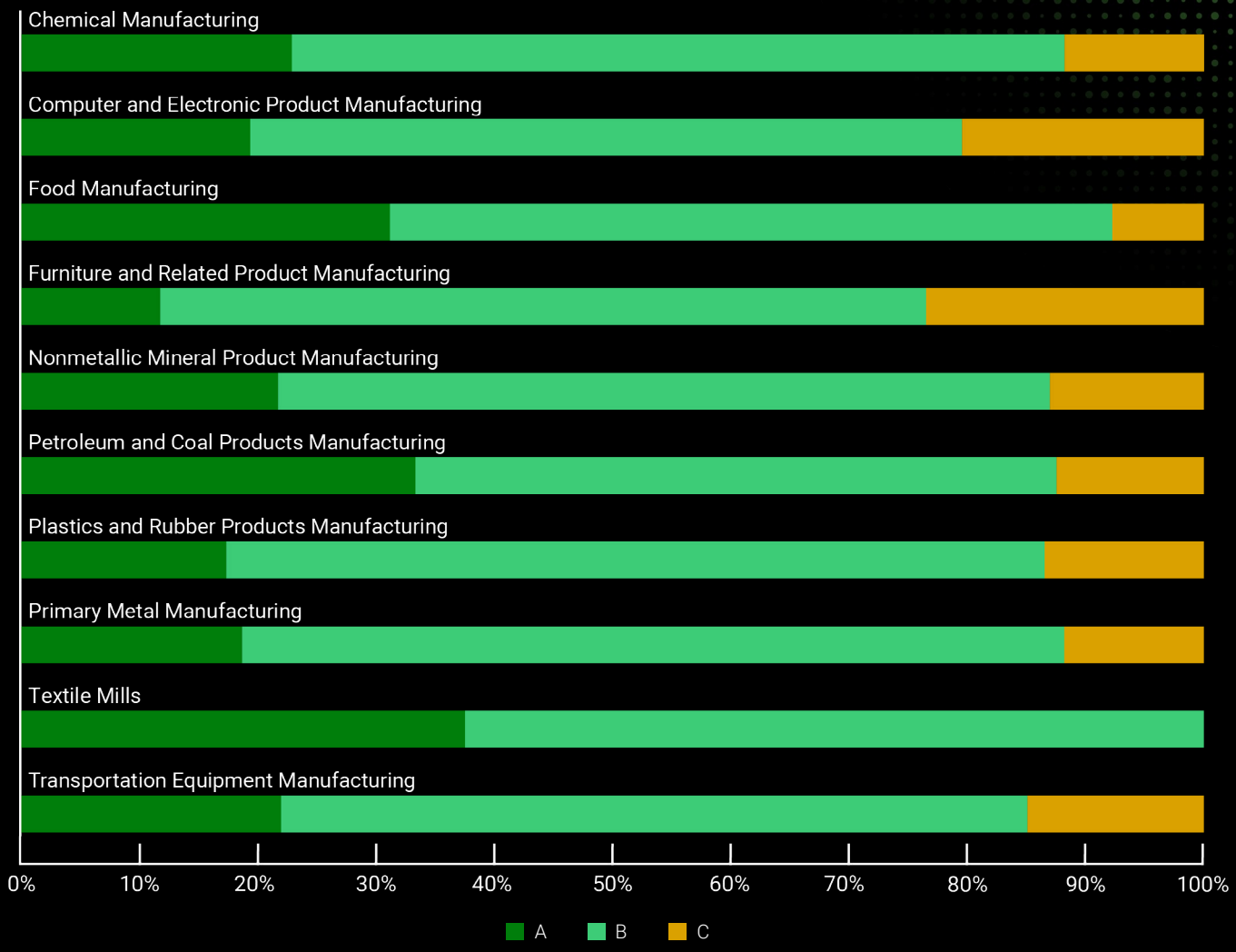
Cyber Ratings: A Snapshot of Cybersecurity Posture

Black Kite's cyber rating system offers a transparent and comprehensive evaluation of an organization's cybersecurity practices, drawing data from external sources, including open-source intelligence (OSINT), dark web monitoring, and publicly available information.

CYBER RATING DISTRIBUTION



CYBER RATING % DISTRIBUTION



Our Analysis

Every company has different thresholds for acceptable cyber risk. While an “A” rating is ideal, some companies may accept a “B” depending on their specific risk tolerance, industry requirements, and regulatory obligations. However, in the manufacturing industry, we see a significant number of companies with ratings lower than desired, signaling the need for urgent remediation efforts to meet security objectives.

Key Risk Indicators: Unveiling Hidden Dangers

Beyond the RSI and cyber rating scores, we looked at other critical vulnerabilities and risks in Manufacturing that are important to consider when assessing cybersecurity.

FINDING	# OF COMPANIES	% OF COMPANIES
Have critical vulnerabilities (CVSS score 8 and above)	829	80%
Have leaked credentials in the last 90 days	712	69%
Have at least one vulnerability from CISA's KEV Catalog	693	67%
Have broken crypto algorithms (SSL/TLS)	646	62%
Have poor email configuration	127	12%
Experienced a data breach in the last year	58	6%
Have poor name server configuration	52	5%
Experienced a data breach in the last 90 days	23	2%
Have denial of service risk	23	2%
Experienced a ransomware attack in the last year	22	2%
Experienced a ransomware attack in the last 90 days	6	1%

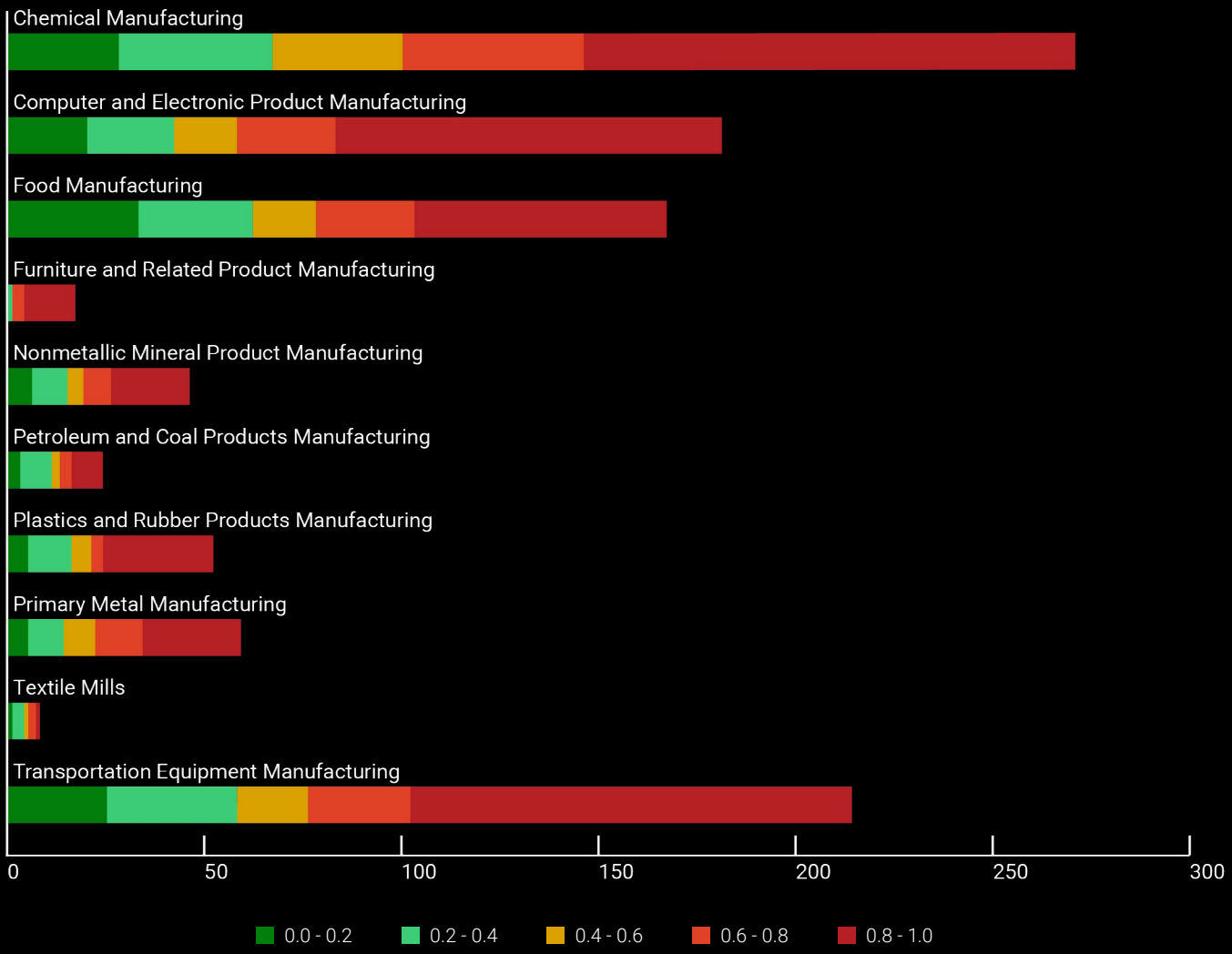
Our Analysis

A staggering 80% of manufacturing companies have critical CVSS-rated vulnerabilities, which represent severe security risks. Notably, the vast majority of manufacturing companies have leaked credentials and a shocking 67% have vulnerabilities listed in the CISA Known Exploited Vulnerabilities (KEV) catalog—weaknesses that are actively exploited by threat actors. These findings highlight crucial areas that need immediate attention and remediation.

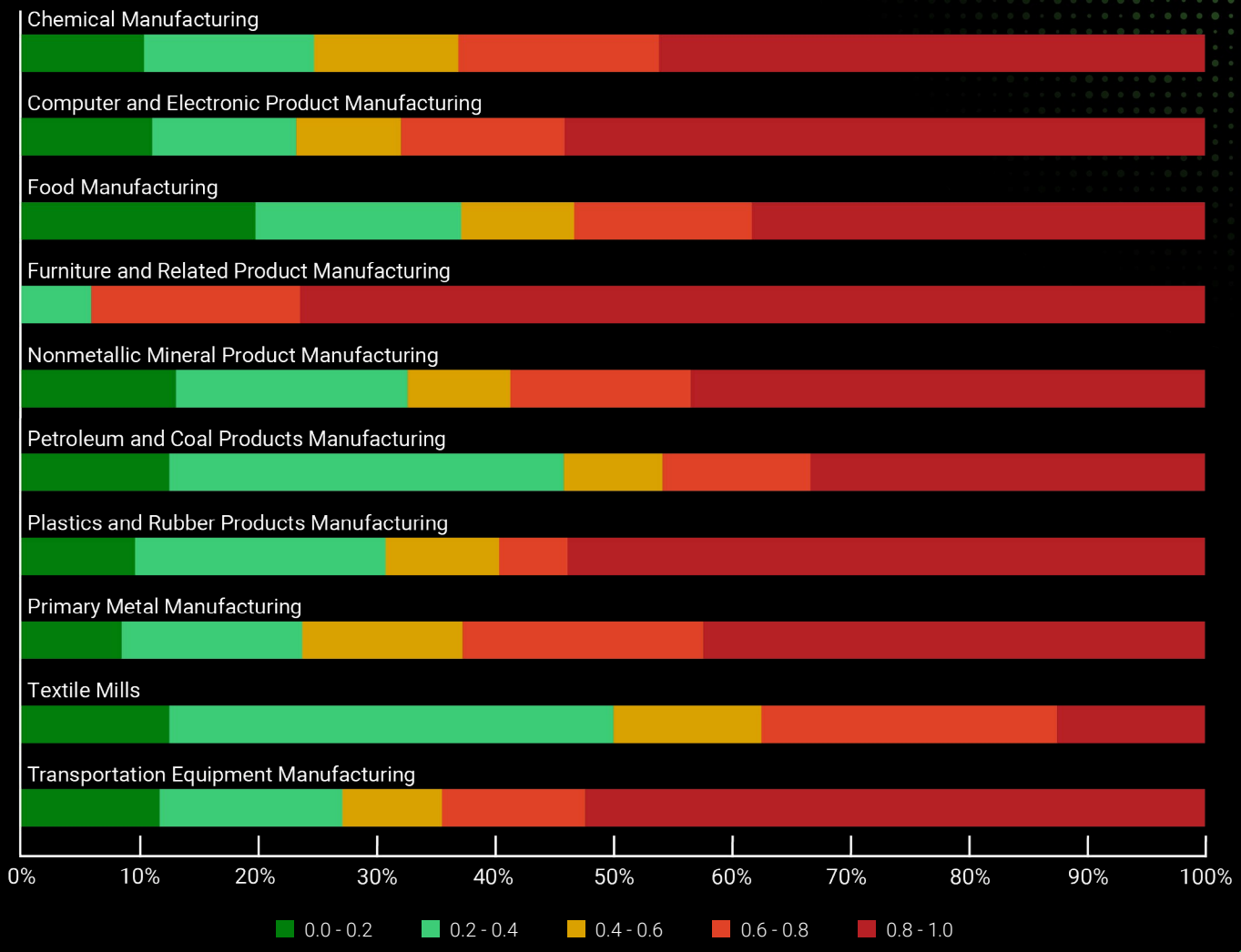
Patch Management: An Urgent Need

Next we looked at grades across key categories that should not be overlooked in managing a company's cybersecurity posture, starting with Patch Management.

PATCH MANAGEMENT GRADE DISTRIBUTION



PATCH MANAGEMENT % GRADE DISTRIBUTION



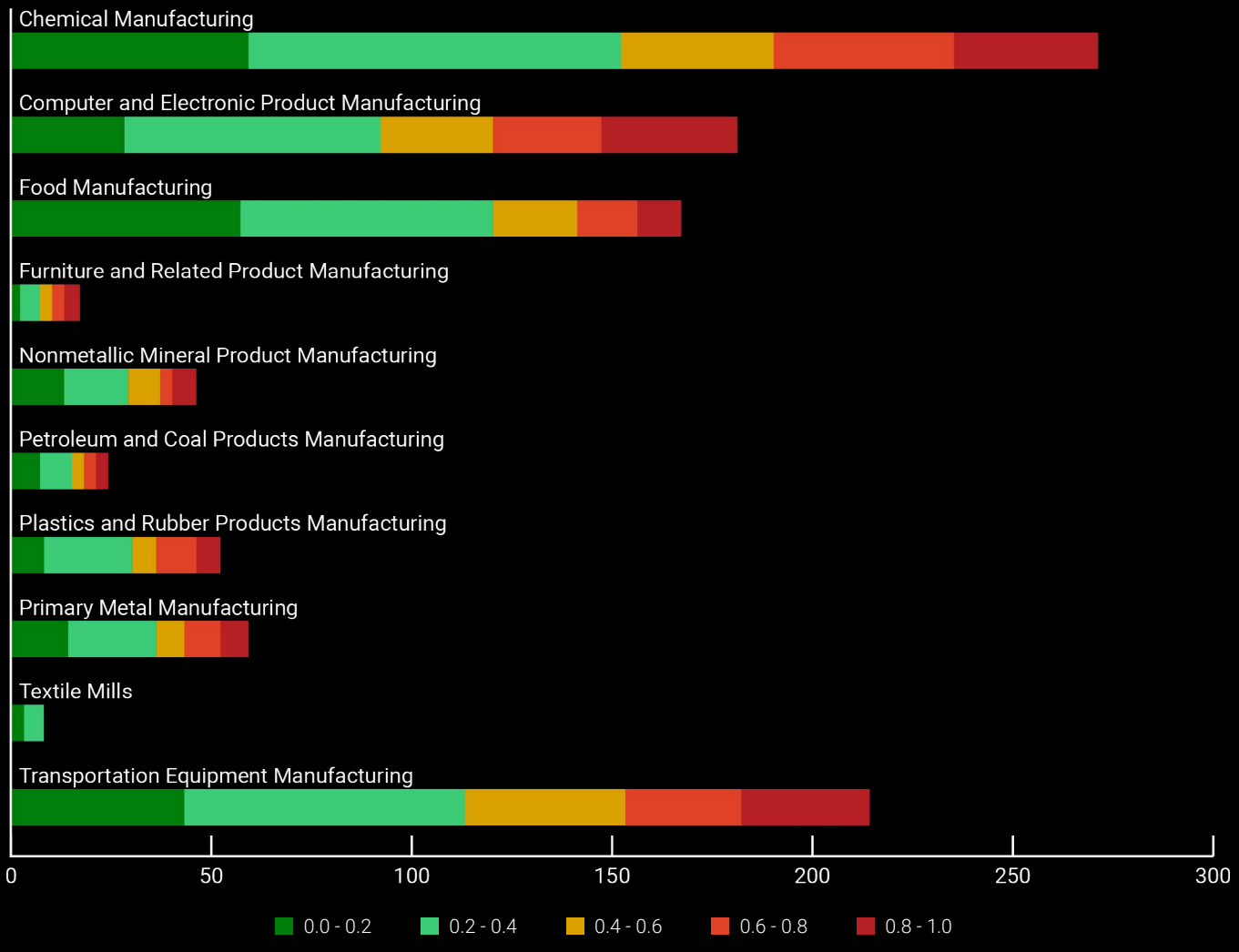
Our Analysis

Patch management is fundamental to a secure infrastructure, acting as the first line of defense against vulnerabilities. However, our **analysis reveals a concerning trend: poor patch management across the manufacturing sector.** For example, 94% of companies in the Furniture and Related Product Manufacturing sub-industry scored a D or F in patch management, which means that most of their assets have an outdated server/product that is vulnerable. This widespread neglect leaves many companies vulnerable to data breaches and other cyber threats, emphasizing the need for immediate corrective actions.

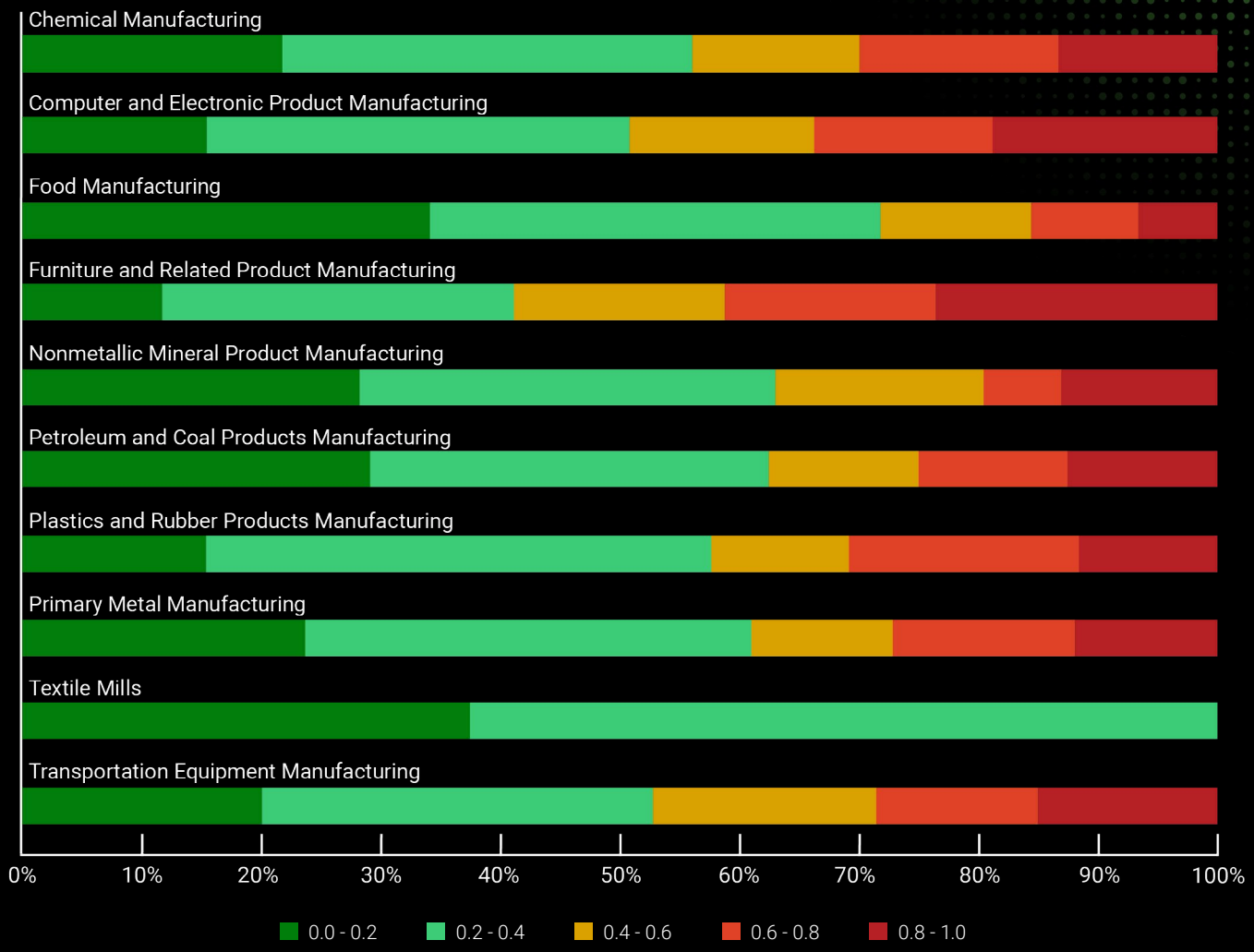
Application Security:
Securing the Digital Frontline

Applications serve as the backbone of business operations, but this reliance on software comes with inherent risks. Applications are often the first point of entry for cybercriminals seeking to exploit vulnerabilities, disrupt operations, or steal sensitive data.

APPLICATION SECURITY GRADE DISTRIBUTION



APPLICATION SECURITY % GRADE DISTRIBUTION



Our Analysis

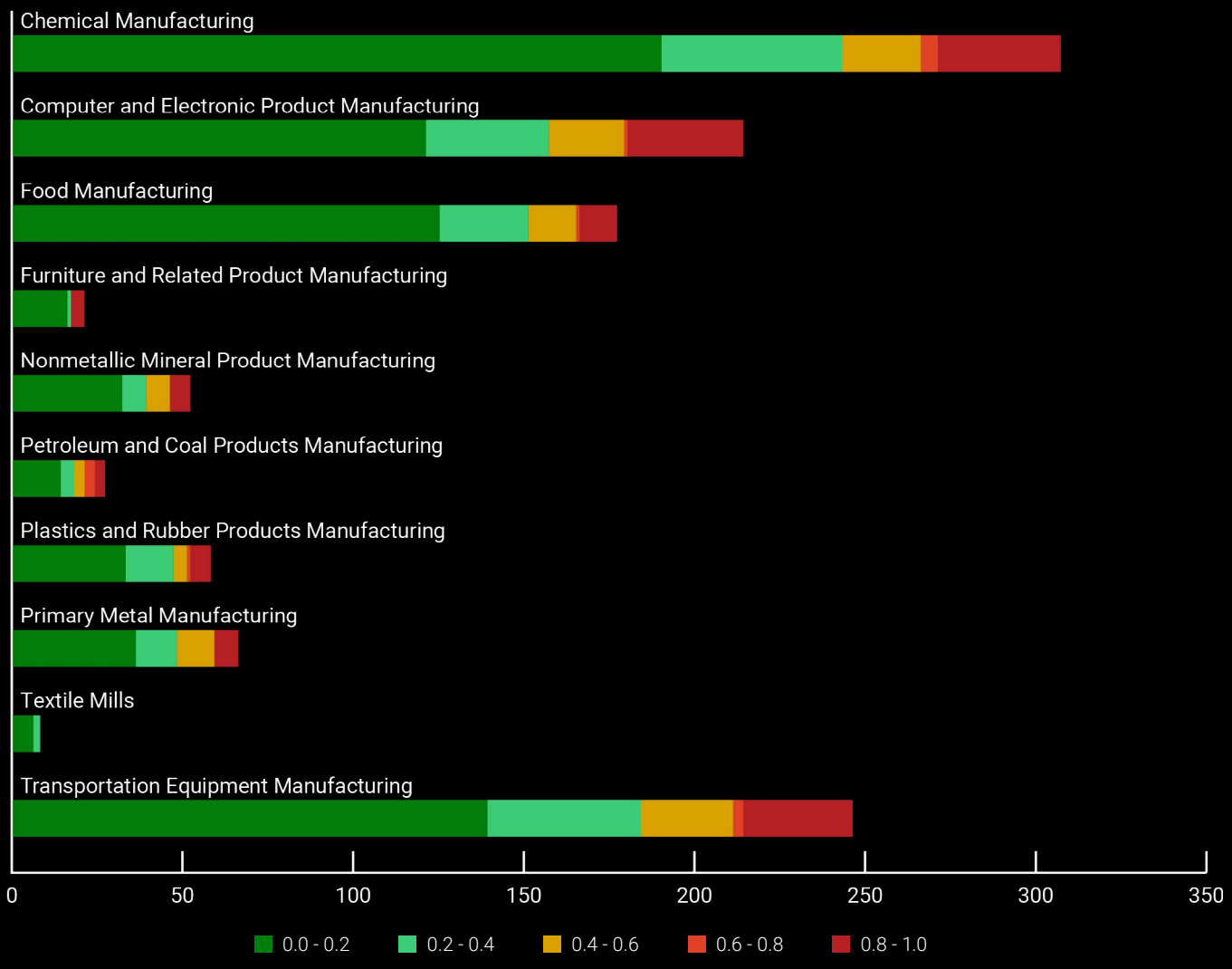
For manufacturing companies, where operational continuity and data integrity are paramount, robust application security is not just a necessity—it's a critical defense strategy. Although there are positive signs with a considerable amount of green among these scores, there's still work to be done. Approximately 30% of companies are in the critical zone with a score of D or F in application security, highlighting the need for ongoing vigilance and improvements to reduce the attack surface and protect the broader environment.

Approximately 30% of companies are in the critical zone for application security

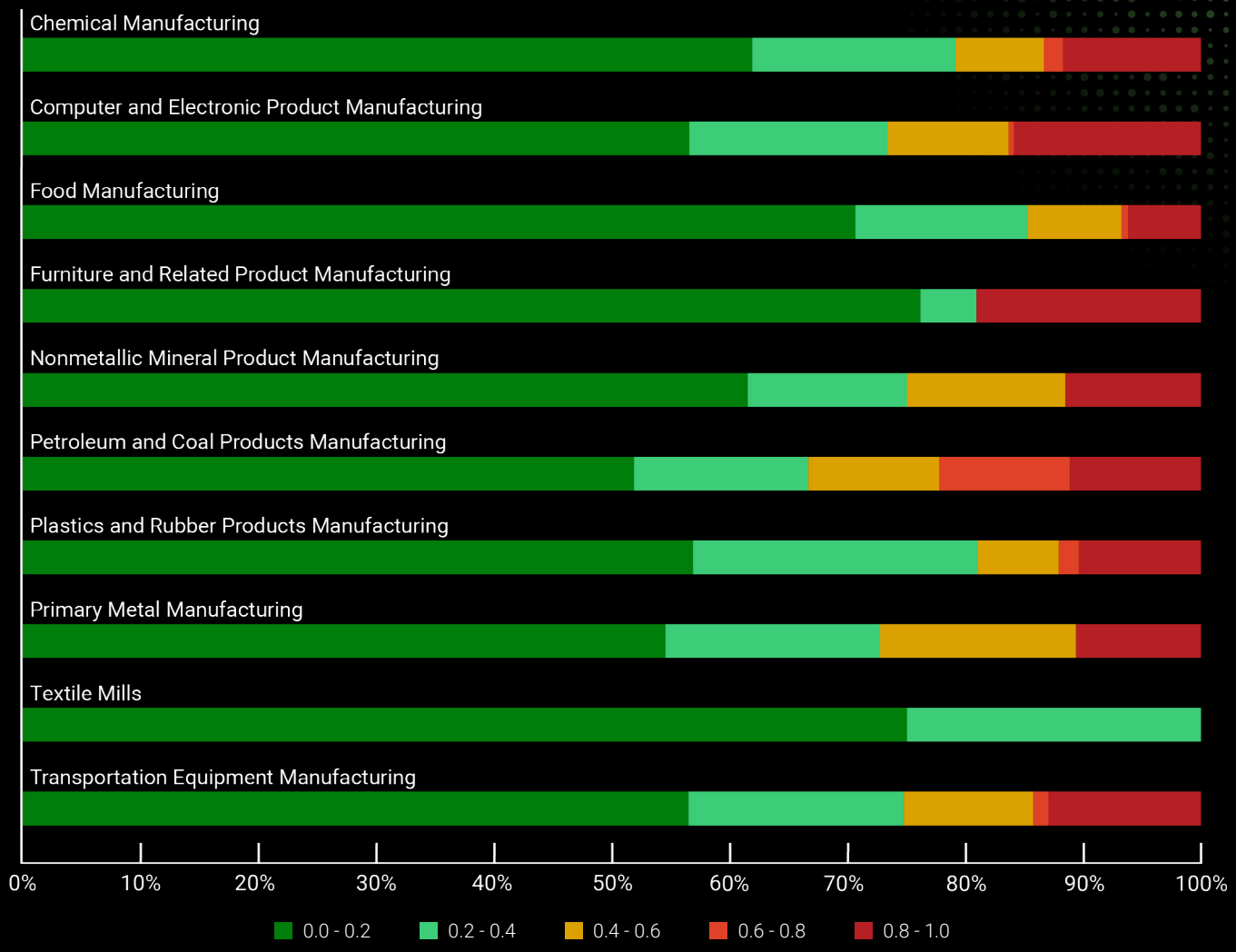
Email Security: Guarding the Gateway to Sensitive Information

Email is a primary communication channel and a frequent target for cyberattacks. Ensuring robust email security is essential for safeguarding sensitive information, preventing fraud, and maintaining organizational integrity.

EMAIL SECURITY GRADE DISTRIBUTION



EMAIL SECURITY % GRADE DISTRIBUTION



Our Analysis

While many companies demonstrate strong email security practices, there are concerning vulnerabilities within sub-industries such as Petroleum and Coal Products, Computer and Electronic Product Manufacturing, and Primary Metal Manufacturing. Companies in these sub-industries must address misconfigurations on their email systems with urgency, as these are weaknesses that can be exploited by threat actors.

Conclusion: Manufacturing at a Cybersecurity Crossroads

The manufacturing industry stands at a critical juncture, where the stakes of third-party risk have never been higher. The rapid pace of digital transformation has opened new avenues for efficiency and innovation but has also introduced significant vulnerabilities. As this report has highlighted, ransomware remains the most pressing threat, with manufacturing companies being prime targets due to their expansive third-party networks and critical role in global supply chains.

The pervasive issues in patch management, application security, and key risk indicators like CVSS scores underline the urgent need for comprehensive risk management strategies. While some companies have made strides in strengthening their cyber defenses, a significant portion of the industry still lags behind, leaving them vulnerable to potentially catastrophic cyber incidents.

As the industry moves forward, it is imperative that manufacturing companies adopt a proactive stance toward cybersecurity, prioritizing the remediation of critical vulnerabilities, enhancing patch management practices, and fortifying application and email security. By doing so, they can mitigate the risks posed by their third-party vendors and protect their operations, reputations, and bottom lines from the ever-evolving cyber threat landscape.

Understand your company's third-party risk and take the necessary steps to safeguard your business. **Schedule a demo** with Black Kite today.

About Black Kite

Get Proactive | Gain Control.

Black Kite gives companies a comprehensive, real-time view into cyber third-party risk so they can make informed and proactive risk decisions that help avoid business disruption, building resilience within their supply chain. With one-of-a-kind collaboration capabilities, companies can work directly with their vendors to report, mitigate, and minimize risk, improving their own business resilience as well as their vendors' organizations.

Through an automated process, and a combination of threat, business, and risk information, Black Kite provides cyber risk detection and response capabilities that are accurate, fast, and transparent.

Black Kite serves more than 3,000 customers in a wide range of industries and has received numerous industry awards and **recognition from customers**.

LEARN MORE WITH A FREE DEMO.

BLACK KITE

800 Boylston Street, Suite 2905, Boston, MA 02199

+1 (571) 335-0222 | info@blackkite.com

Copyright © 2024 Black Kite, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective holders.