RANSOMWARE RISK: AUTOMOTIVE MANUFACTURING IN 2021

Ransomware Trends in Automotive Supply Chains

BLACK KITE

TABLE OF CONTENTS

KEY FINDINGS

- Nearly half of the top 100 automotive manufacturers are highly susceptible to a ransomware attack
- More than 17% of automotive suppliers are likely to incur a ransomware attack
- Patch management Is the most prevalent vulnerability for automotive companies, with 71% having "F" or "poor" ratings
- 71% of automotive CIOs indicate they are most likely to increase investments In cyber and Information security In 2021

INTRODUCTION

Today, change in the automotive industry Is driven by technology. Automakers and parts manufacturers have shifted their engineering focus to connectivity, becoming more strategic with key technology investments.

However, automotive companies still fall behind other industries in terms of digital maturity and are struggling to move forward with a digital transformation plan.

In a recent Gartner survey [1], 71% of automotive CIOs indicate they are most likely to increase investments in cyber and information security in 2021 compared to 2020. This sweeping response follows an uptick in ransomware attacks, especially headlines including legacy automative companies.

A push for more resources and attention stems from:

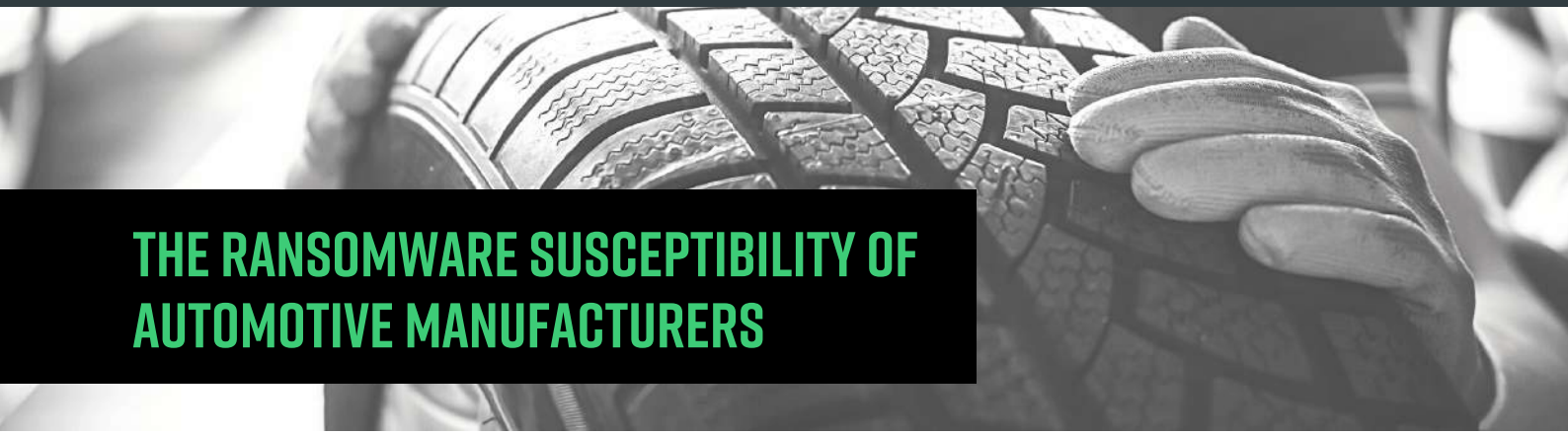
- **Digital transformation creates a larger attack surface.** One single original equipment manufacturer (OEM) fleet has more than 20 million vehicles on the road [1]. A cyberattack in one vehicle could cost human lives, property, and brand reputation.
- **Advanced driver assistance system (ADAS) capabilities require artificial intelligence (AI).** Vehicles are data centers on wheels. Personal information, electronic components, and automotive technology via bluetooth technology are now stored online.
- **Physical safety vs. online safety.** As technology advances and opens doors to fully self-driving cars, compliance standards such as ISO 26262, SOTIF and UL4600 are addressing safety concerns surrounding autonomous operation on the road. Many tech executives are still searching for the right technology to succeed with the evolving cyber landscape, as automotive technology is not always supported by traditional IT systems.
- **Automotive supply chains are becoming more complex**. Today's car software runs one million lines of code [1], opening doors to a multitude of vulnerabilities and security risks that need to be managed. For example, a vulnerability found in one ECU could affect an entire fleet of vehicles.

Automotive manufacturers are currently dealing with a serious shortage of semiconductors, affecting leading organizations such as Toyota, Ford Motor, Volkswagen and Honda [2]. Production has been forced to halt in recent weeks, interrupting supply chain logistics, hiking market prices and causing a destructive bottleneck of inventory. While the recent focus has centered around physical operations, hackers have not lost sight of additional opportunities to disrupt the automotive sector.

Ransomware attackers can shut down entire manufacturing supply chains. Earlier this year, Kia Motors was hit with a significant ransomware demand, impacting operations for weeks.

Losing control over data can have dire consequences for an automotive company. The diminished trust of consumers, lawsuits, intellectual property theft, and market delays due to cyber attacks all have real-world financial impacts.

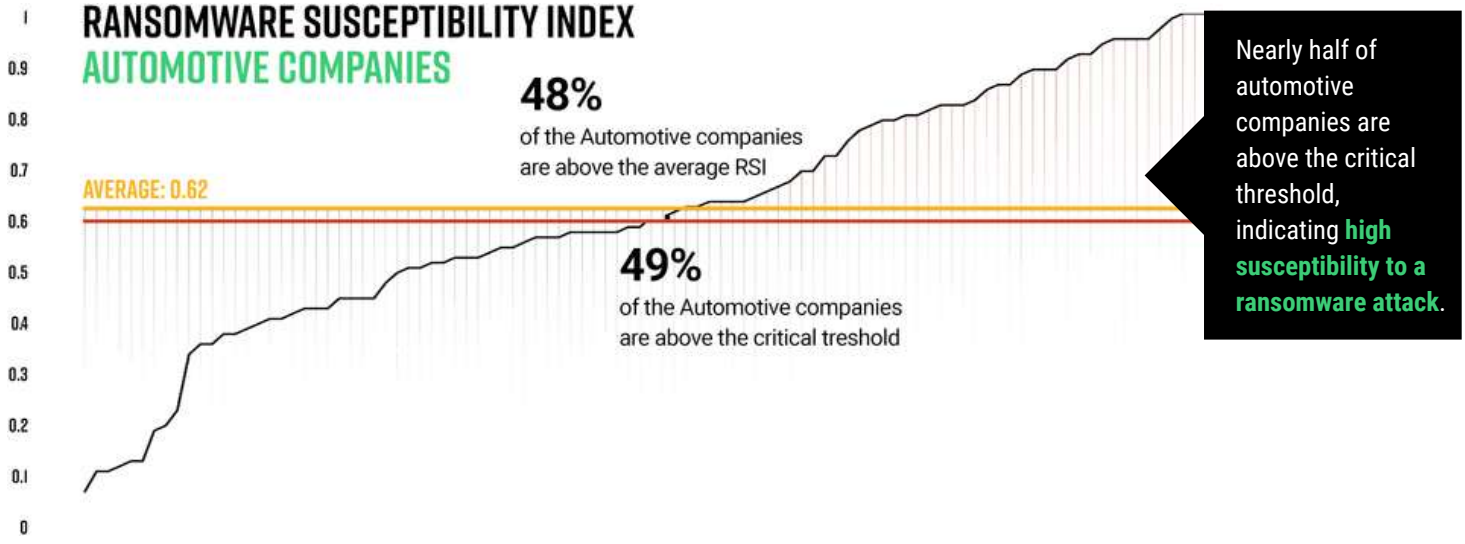
In this report, Black Kite researchers analyzed the cybersecurity posture and ransomware susceptibility for the top 100 automotive manufacturers [3] and the top 100 automotive suppliers [4]. Researchers conducted a detailed study around the automotive supply chains to identify the most common security issues, as well as the likelihood of a ransomware attack.



THE RANSOMWARE SUSCEPTIBILITY OF AUTOMOTIVE MANUFACTURERS

RANSOMWARE SUSCEPTIBILITY INDEX™ (RSI™): 0.62

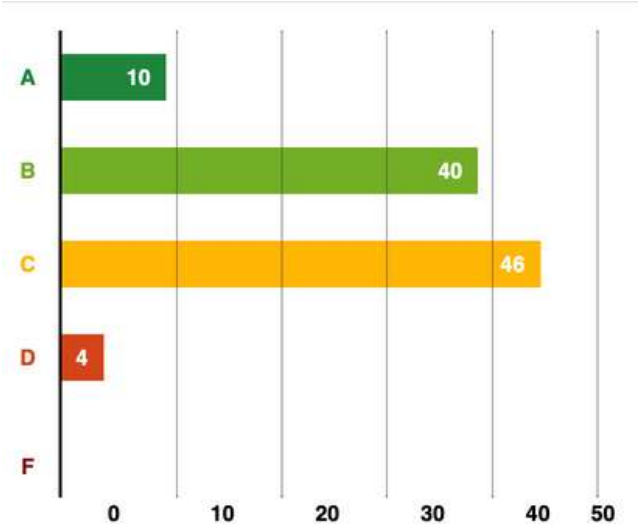
Black Kite's Ransomware Susceptibility Index™ determines how susceptible a company and its third parties are to a ransomware attack. Data is collected from various open source intelligence (OSINT) sources including internet-wide scanners, hacker forums, the deep/dark web, and more. Black Kite correlates each finding with 26 control items using data and machine learning in order to provide approximations. Black Kite's RSI™ scores range on a scale from 0.0 (least susceptible) to 1.0 (most susceptible).



It's important to note a low RSI™ score does not necessarily mean a company is immune to a ransomware attack. Cybercriminals, especially state-backed actors, may use zero-day vulnerabilities and craft sophisticated attacks, which a security automation tool may not detect or predict.

CRITICAL RANSOMWARE FINDINGS OF THE TOP 100 AUTOMOTIVE MANUFACTURERS

AVERAGE TECHNICAL CYBER RISK SCORE
AUTOMOTIVE COMPANIES



AT A GLANCE

On average, automotive manufacturing companies reflect a “C+”, or “average”, overall cyber risk rating.

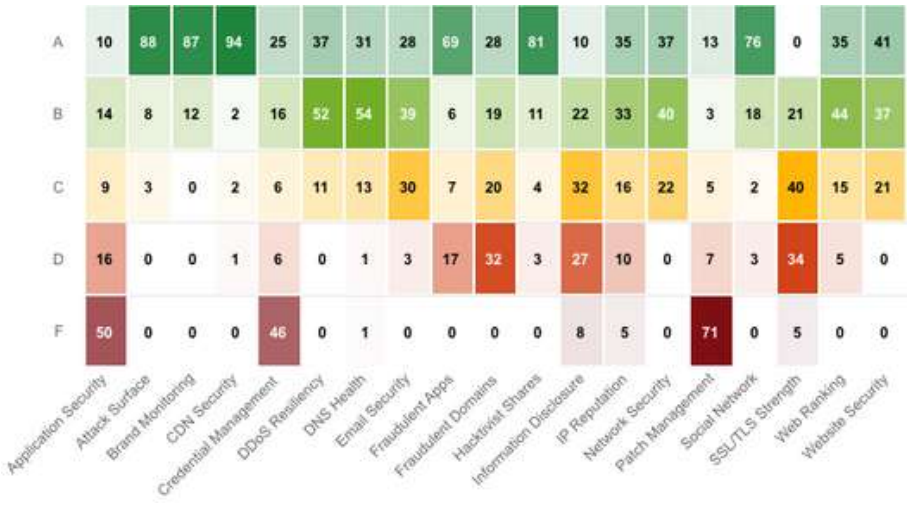
However, there are alarming security issues that lie underneath the surface including companies' susceptibility to phishing attacks, publicly visible ports, and credential management.

BENEATH THE SURFACE

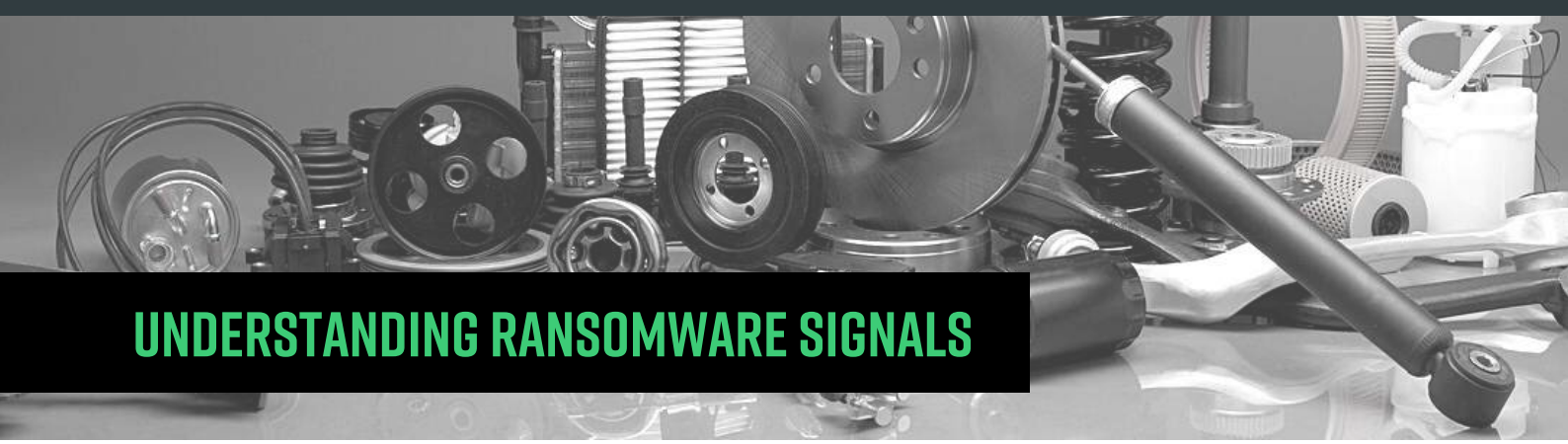
Credential management and **patch management** rank the lowest of the 19 cyber risk categories, with respective "F" ratings.

Based on Black Kite’s prioritized technical heat map, 46% of the 100 companies have "F" grades in credential management, and 71% have "F" grades patch management.

TECHNICAL GRADE HEAT MAP
AUTOMOTIVE COMPANIES



Why are credential and patch management so critical? Aside from reducing the risk of ransomware, fixing software and application vulnerabilities susceptible to a cyber attack is the key to reducing an organization’s security risk. Today, most malware attacks, particularly those that leverage ransomware, exploit vulnerabilities in servers and software applications [5]. In fact, software vulnerabilities were a common ransomware attack vector, used one in five times over the last three years.



UNDERSTANDING RANSOMWARE SIGNALS

5 MOST IMPACTFUL RANSOMWARE ISSUES FOR AUTOMOTIVE COMPANIES	RATE OF OCCURRENCE
At least one possible high-severity vulnerability due to out-of-date systems	91%
Susceptibility to phishing	90%
Publicly visible critical ports	84%
At least one leaked credential found in lists shared on deep web in the last 90 days	64%
Experienced data breach in the past	19%

- **At least one possible high-severity vulnerability due to out-of-date systems:** 91% of automotive companies have more than 1,000 leaked credentials on the deep web, which opens the door for phishing campaigns. Exploiting the vulnerabilities that allow remote code execution is trending in the ransomware community. Even though it is not as easy as using RDP ports, it is not as tiresome as (spear) phishing.

- **Susceptibility to phishing:** Although the number of phishing incidents associated with ransomware attacks is declining, it is still a major attack vector for ransomware variants, such as conit v2. It is essential to take necessary actions to prevent phishing/spoofing within cybersecurity departments across the board, no matter the attack vector.

- **Publicly visible critical ports:** A publicly visible critical port is a critical resource ransomware groups exploit. Although the use of ports is declining each year, it remains the easiest way to upload a ransomware kit. Cybercriminals can easily scan open ports with autonomous tools.

- **At least one credential found in lists shared on deep web in the last 90 days:** Phishing attacks, which commonly use leaked credentials, have historically been the #1 attack vector in ransomware attacks. Gaining access through credential-stuffing attacks has been one of the top methods for hackers in recent years. The combo lists shared on the dark web day after day and tools that automate the attacking process help increase credential-stuffing attacks. Accessing networks using leaked credentials bypasses many cybersecurity countermeasures and poses a significant risk for ransomware attacks.

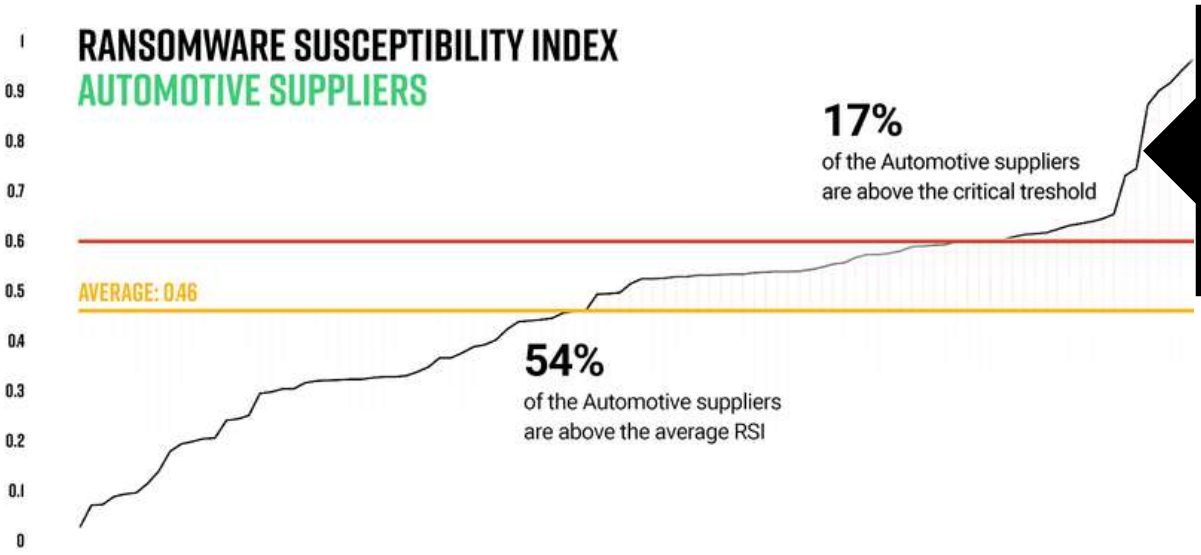
- **Experienced a data breach in the past:** History tends to repeat itself. Cybercriminals target organizations that do not consistently deploy due diligence and make cybersecurity a priority within the business. Cybercriminals anticipate security issues and vulnerabilities to remain present for exploitation if the cybersecurity investment is not adequate.

CRITICAL RANSOMWARE FINDINGS OF THE TOP 100 AUTOMOTIVE SUPPLIERS

RANSOMWARE SUSCEPTIBILITY INDEX™ (RSI™): 0.46

Ransomware threat actors have shifted their focus to supply chains in recent years and are now more likely to prey on small companies and their vendors, such as original equipment manufacturers (OEM). While the average RSI of automotive suppliers is lower than the companies themselves, parent organizations should maintain similar, if not more, focus on protecting their vendor ecosystems.

To better understand the current cyber posture of automotive manufacturers' third-party ecosystem, Black Kite researchers analyzed the technical findings of the top 100 suppliers.



Over 17% of automotive suppliers are above the critical threshold, indicating **high susceptibility to a ransomware attack**.

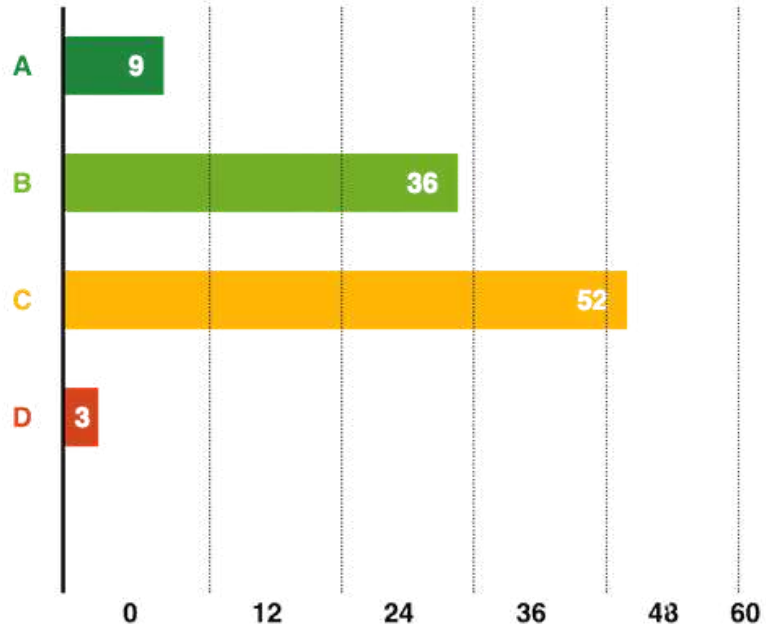
Today most malware, ransomware in particular, exploit vulnerabilities in servers and software applications. Among the attack vectors used by the top three ransomware variants [Sodinokibi, Conti, and Lockbit], software vulnerabilities continue to dominate various attack vectors.

5 MOST IMPACTFUL RANSOMWARE ISSUES FOR AUTOMOTIVE SUPPLIERS	RATE OF OCCURRENCE
At least one possible high-severity vulnerability due to out-of-date systems	87%
Susceptibility to phishing	85%
Publicly visible critical ports	81%
At least one leaked credential found in lists shared on deep web in the last 90 days	67%
Experienced data breach in the past	11%

TECHNICAL ANALYSIS OF AUTOMOTIVE SUPPLIERS

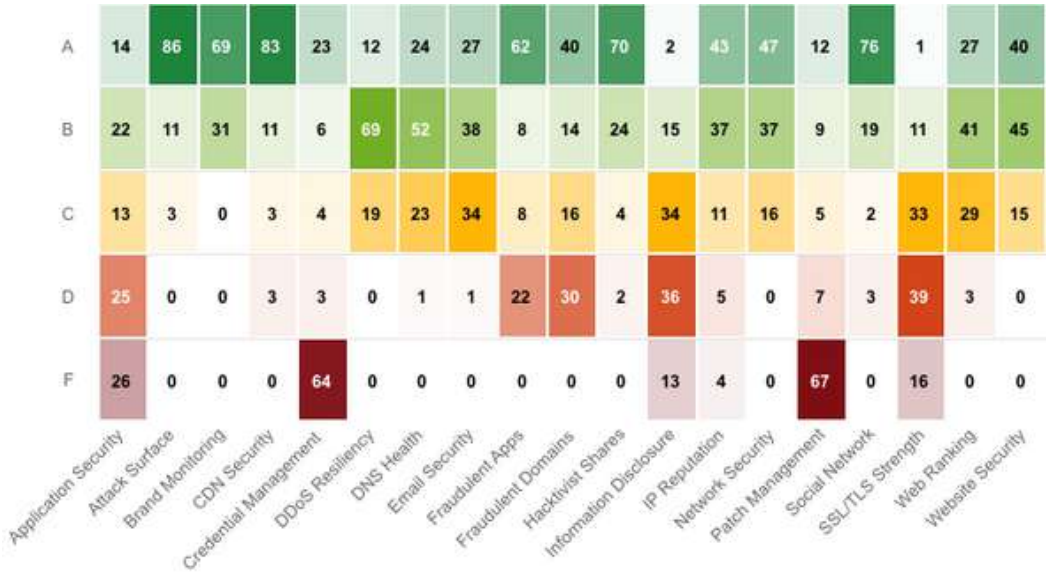
To uncover the factors leading to ransomware susceptibility, Black Kite researchers drilled down even further into the technical findings of the supplier group. The average automotive vendor reflects a “C-” rating or “below average” rating, which is consistent with the company ratings, indicating present critical security issues.

AVERAGE TECHNICAL CYBER RISK SCORE
AUTOMOTIVE VENDORS



Credential management and **patch management** ranked again among the lowest-scored categories, receiving a "C" and "C-", respectively. Based on Black Kite’s prioritized technical heat map, 63% of the 100 vendors received an "F" grade in credential management, and 67% received "F" grades patch management.

TECHNICAL GRADE HEAT MAP
AUTOMOTIVE VENDORS



RECAP & RECOMMENDATIONS

While the daily barrage of ransomware attacks can seem like a daunting challenge, there are proactive measures that automotive companies can take to reduce their threat surface and limit the susceptibility to attacks.

Adopt a Risk-Aware Approach for Vendor Ecosystems

1. Understand the crown jewels of your company. Not simply personal data, but items like IP theft are now top threats in the pharmaceutical industry.
2. Understand your risk. Adopt a quantitative approach to your risk management strategy, such as Open FAIR™, to make more informed business decisions. Remember, the cost is not just about the ransom payment for an attack, but also significant interruptions to overall business functions.
3. Understand your third parties and their associated risk. Supply chains and OEMs can be complex, increasing the likelihood of a ripple effect in the case of a cyber breach. Classify vendors, identify critical data sharing points, and adopt a continuous model for vendor risk monitoring. Point-in-time assessments do not cut it anymore. Automation is the key to vendor risk management.
4. Adopt an incident response strategy for post-breach.
5. Engage the company's board in cybersecurity risk. Quantification is the key to board engagement and understanding in cybersecurity risk management.

REFERENCES

[1] *10 Biggest Challenges Facing Automotive CISOs Tasked with Vehicle Cyber Security*
https://argus-sec.com/automotive-security-10-biggest-challenges-facing-oem-cisos/
[2] *2021 CIO Agenda: An Automotive Perspective*
https://www.gartner.com/document/3992214?ref=solrAll&refval=291872502
[3] *Top 100 Automotive Companies*
https://brandirectory.com/rankings/auto/table
[4] *Top 100 Automotive Suppliers*
https://www.automobil-produktion.de/files/content/noindex/apr/sonderausgaben/TOP%20100_2020_Internet.pdf
[5] *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound*
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

CONTACT
120 St. James Ave
Boston, MA 02116
+1 (571) 335-0222
info@blackkite.com

www.blackkite.com