THE 2021 RANSOMWARE RISK PULSE: PHARMACEUTICAL MANUFACTURING

Ransomware Trends in Pharmaceutical Supply Chains

BLACK KITE

TABLE OF CONTENTS

KEY FINDINGS

- Nearly 10% of pharmaceutical manufacturers are highly susceptible to a ransomware attack
- More than 12% of pharmaceutical industry vendors are likely to incur a ransomware attack
- Almost half of all pharmaceutical companies have more than 1,000 leaked employee credentials exposed on the deep web
- Pharmaceutical companies' annual cyberattack risk averages $31.1 million
- Medium-sized pharmaceutical companies have the highest susceptibility to ransomware
- Data management vendors pose the most significant annual financial risk ($6.2 million) to pharmaceutical manufacturers
- Software vendors vary the most in terms of estimated financial risk, ranging from $331,000 to $46.1 million annually

INTRODUCTION

More than five billion [1] people rely on at least one product manufactured by the pharmaceutical industry. Whether it is an over-the-counter pain medication, a cutting-edge cancer drug, or the Covid-19 vaccine, well over half of the global population count on pharmaceutical manufacturers to heal, comfort and treat.

An interruption in manufacturing lifesaving drugs or therapies would be catastrophic for many. A cyberattack on a pharmaceutical company could mean life or death for consumers.

The pharmaceutical industry is the world's third-largest industry, following the finance and e-commerce sector [2]. With a predicted compound annual growth rate of 13.7% through 2027 [3], it's no secret that pharmaceutical organizations will become a more valuable target to cyber criminals.

Aside from size, there are several reasons why the pharmaceutical industry is a rich target for cyberattacks:

- **Digital transformation creates more gateways.** COVID-19 has removed many constraints and restrictions with virtual engagement, which allowed the pharmaceutical sector to accelerate digitization initiatives. In turn, more data is stored digitally and online than ever before.
- **Pharmaceutical companies have access to vast amounts of sensitive data.** Personal information, medicinal patents, and pharmaceutical technology are now stored online.
- **Medical technology is more widely adopted.** According to a recent Gartner report, "medical advances, such as messenger RNA and cell and gene therapy, have accelerated therapy development and approval, but require significant upgrades to existing development, regulatory and commercialization functions." This notion is reflected in the digital space and the pharmaceutical companies' digital assets.
- **Pharmaceutical supply chains are becoming more complex**. COVID-19 has altered the landscape, allowing acquisitions and new partnerships to bring in new security issues.

Data from pharmaceutical firms, including patented medication records, pharmaceutical developments, and technology data, are all valuable information. In the past year, we have seen how ransomware attackers can shut down entire manufacturing supply chains. Imagine if a ransomware attack halted a manufactured COVID-19 vaccine hostage, or stopped the production of vital chemotherapy drugs.

Losing control over that data can have dire consequences for a pharmaceutical company. The diminished trust of patients and consumers, lawsuits from customers who lose access to lifesaving therapies, intellectual property theft, and market delays due to cyber attacks all have real-world financial impacts.

Although most pharmaceutical firms are aware that a cyber attack could be detrimental to their business, the industry has not proactively deployed cybersecurity. Recent sophisticated attacks [4], aligning with COVID-19 vaccine studies against pharmaceutical firms, have served as a wake-up call for boards to take action.

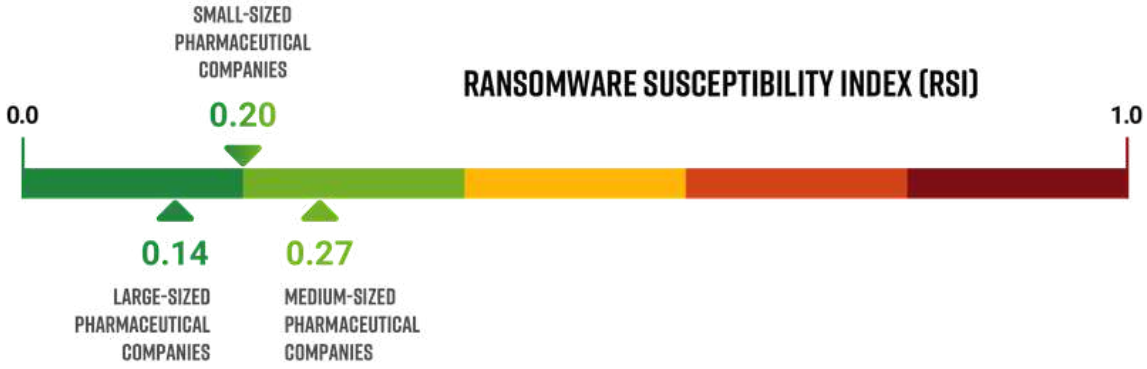
Among these attacks, ransomware continuously proves to be the most devastating type of cyber attack. In 2020, 92 ransomware attacks cost the U.S. healthcare and pharmaceutical industry $20.8 billion [5].

In this report, Black Kite researchers analyzed the cybersecurity posture and ransomware susceptibility for the top 200 pharmaceutical manufacturers and their commonly associated vendors. Pharmaceutical companies were tiered into three categories based on their market capitalization value:

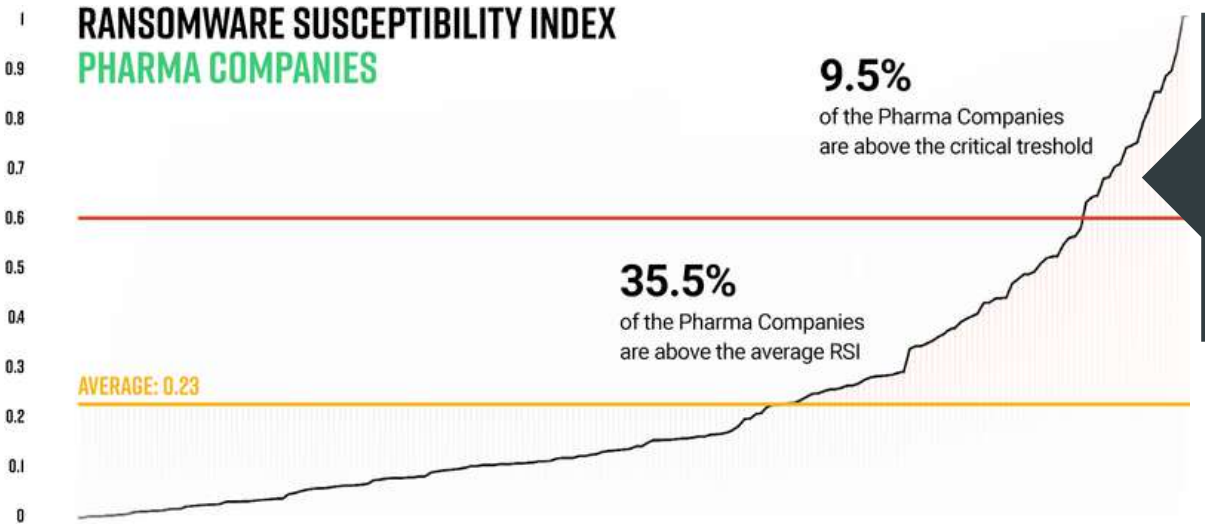
1. Small = $0 - $1B Market Capitalization Value
2. Small/Medium = $1B - $10B Market Capitalization Value
3. Medium = $10B - $50B Market Capitalization Value
4. Large = > $50B Market Capitalization Value

Researchers conducted a detailed study around the pharmaceutical supply chains to identify the most common security issues, as well as the estimated financial risk in the case of a ransomware attack.

THE RANSOMWARE SUSCEPTIBILITY OF PHARMACEUTICAL MANUFACTURERS



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).



Nearly 10% of pharmaceutical companies are above the critical threshold, indicating **high susceptibility to a ransomware attack**.

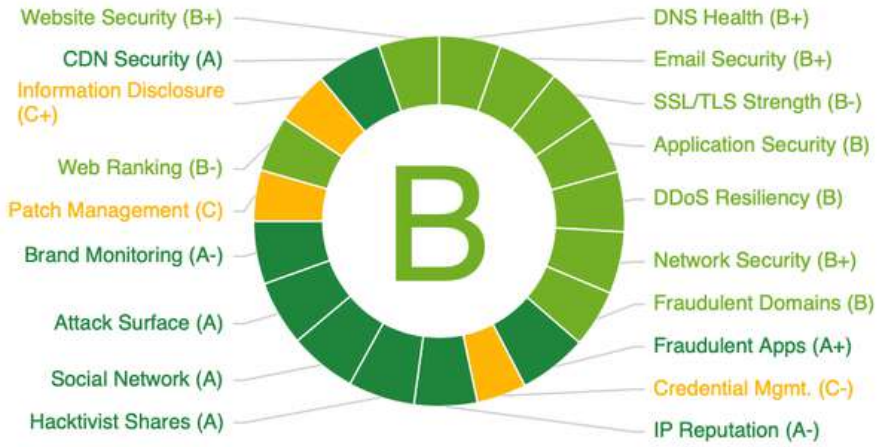
It's important to note a low RSI™ score does not necessarily mean a company is immune to a ransomware attack. Cybercriminals, especially state-backed actors, may use zero-day vulnerabilities and craft sophisticated attacks, which a security automation tool may not detect or predict.

Our researchers expected to see larger RSI™ values for small and medium-sized pharmaceutical companies, as larger enterprises tend to have more strict and mature cybersecurity controls. Our hypothesis proved accurate, as Black Kite's RSI™ findings indicate medium-sized pharmaceutical companies have the highest average ransomware susceptibility, followed by small-medium and small pharmaceutical companies.

These findings are consistent with recent reports that show ransomware threat actors target small and medium-sized companies more than large enterprises. A recent ransomware report [6] claims more than 73% of ransomware attacks target small and medium-sized companies.

CRITICAL RANSOMWARE FINDINGS OF THE TOP 200 PHARMACEUTICAL MANUFACTURERS

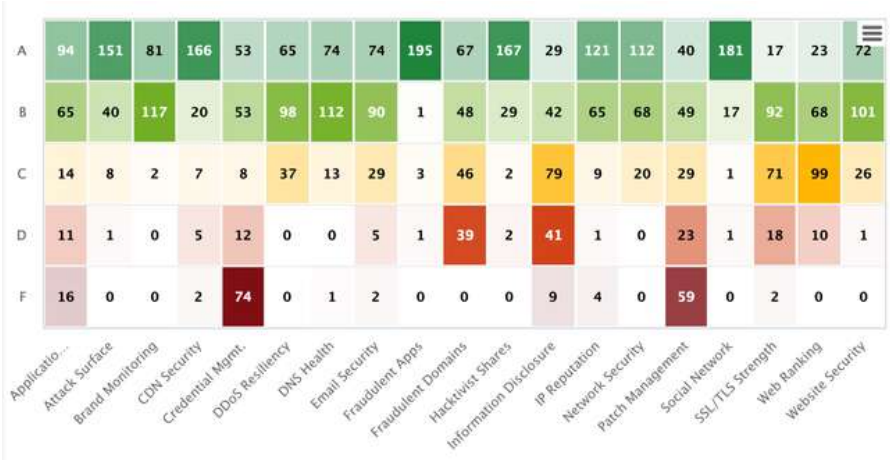
AVERAGE TECHNICAL CYBER RISK SCORE
PHARMACEUTICAL COMPANIES



On average, pharmaceutical manufacturing companies reflect a “B”, or “good”, 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.

TECHNICAL GRADE HEAT MAP
PHARMACEUTICAL COMPANIES



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

Based on Black Kite’s prioritized technical heat map, 37% of the 200 companies have "F" grades in credential management, and 30% have "F" grades patch management.

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. 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 PHARMA COMPANIES	RATE OF OCCURRENCE
At least one possible high-severity vulnerability due to out-of-date systems	98%
Susceptibility to phishing	89%
Publicly visible critical ports	73%
At least one leaked credential found in lists shared on deep web in the last 90 days	53%
Experienced data breach in the past	10%

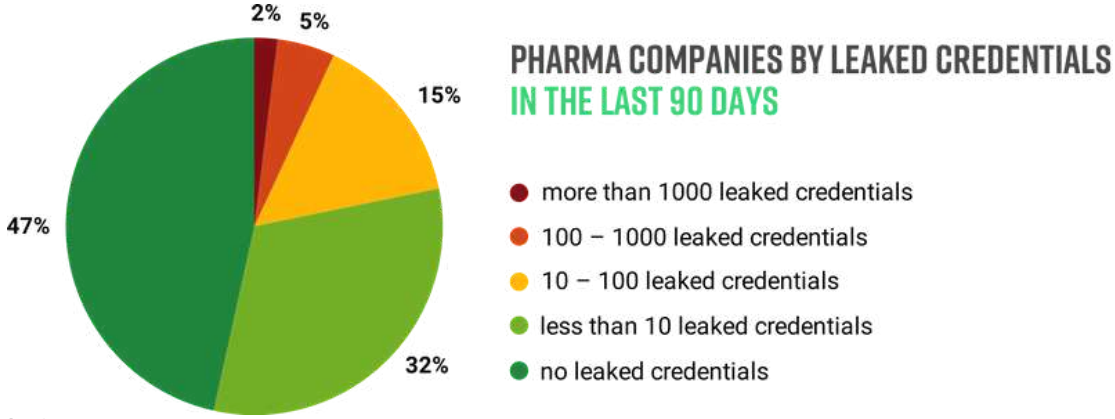
- **At least one possible high-severity vulnerability due to out-of-date systems:** 47% of pharmaceutical companies have more than 1,000 leaked credentials on the deep web, which opens the door for phishing campaigns. Exploiting the vulnerabilities that allow remote code execution is trending in the 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.

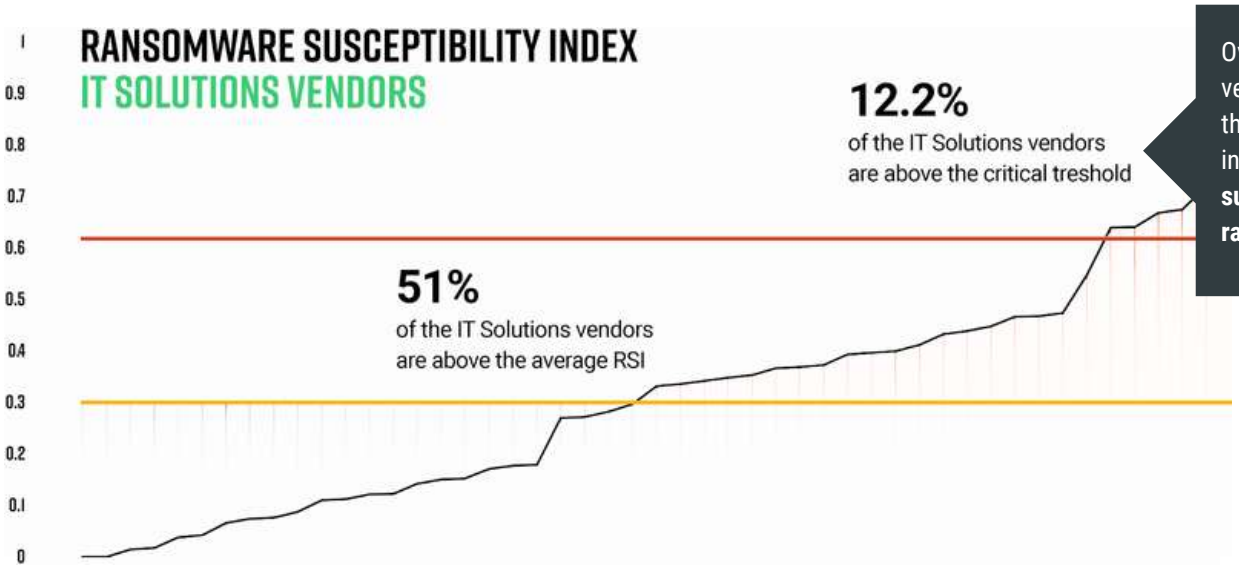
- **Experienced a data breach in the past:** History tends to repeat itself. Cybercriminals target organizations that do not consistently deploy due diligence and make cybersecurity a priority within the business. Cybercriminals anticipate security issues and vulnerabilities to remain present for exploitation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



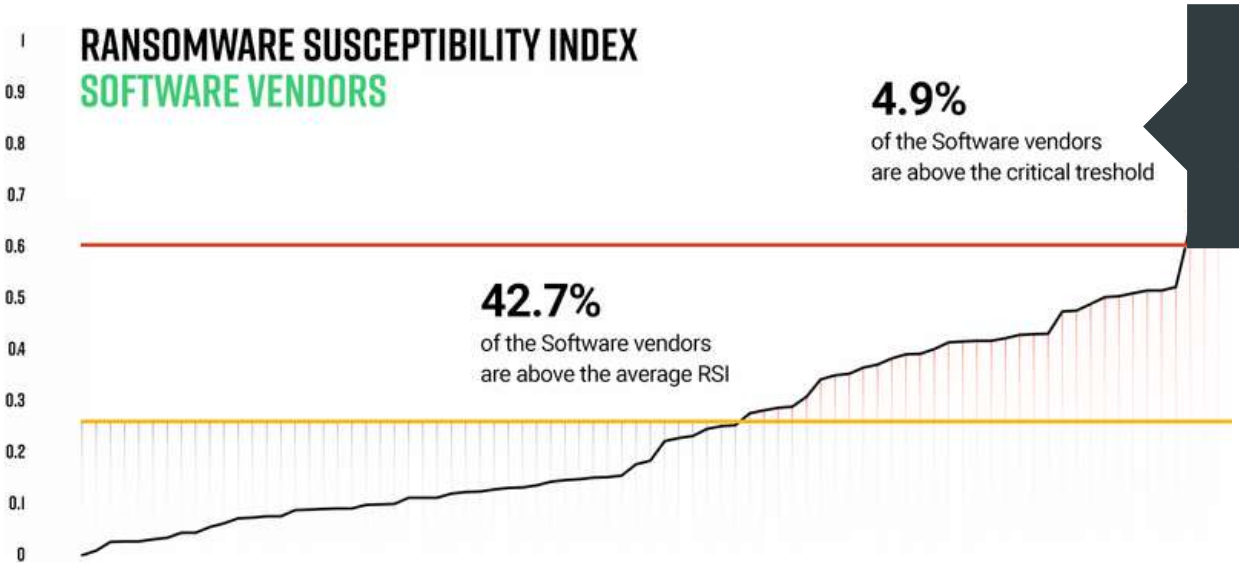
CRITICAL RANSOMWARE FINDINGS OF TOP PHARMACEUTICAL VENDORS

Ransomware threat actors have shifted their focus to vendors and supply chains in recent years, and are now more likely to prey on small companies and their vendors. Still, this does not mean that large enterprises are immune and should let their guard down in this threat landscape. Instead, they should focus on protecting their vendor ecosystems.

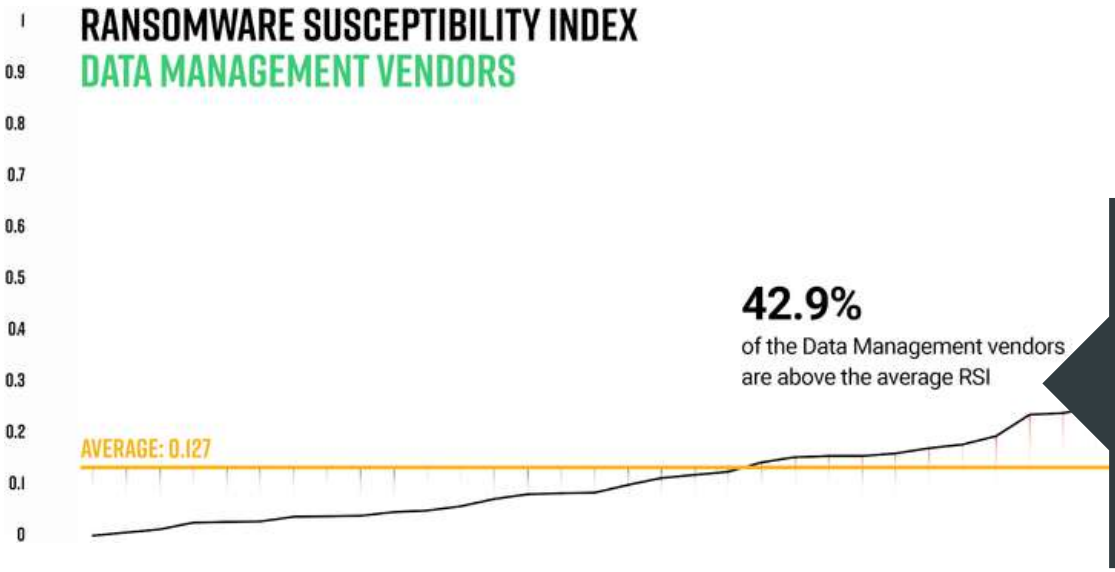
To better understand the current cyber posture of pharmaceutical manufacturers' third-party ecosystem, Black Kite researchers analyzed 166 vendors [7] in three different categories: data management, IT, and software.



Over 12% of IT vendors are above the critical threshold, indicating **high susceptibility to a ransomware attack**.



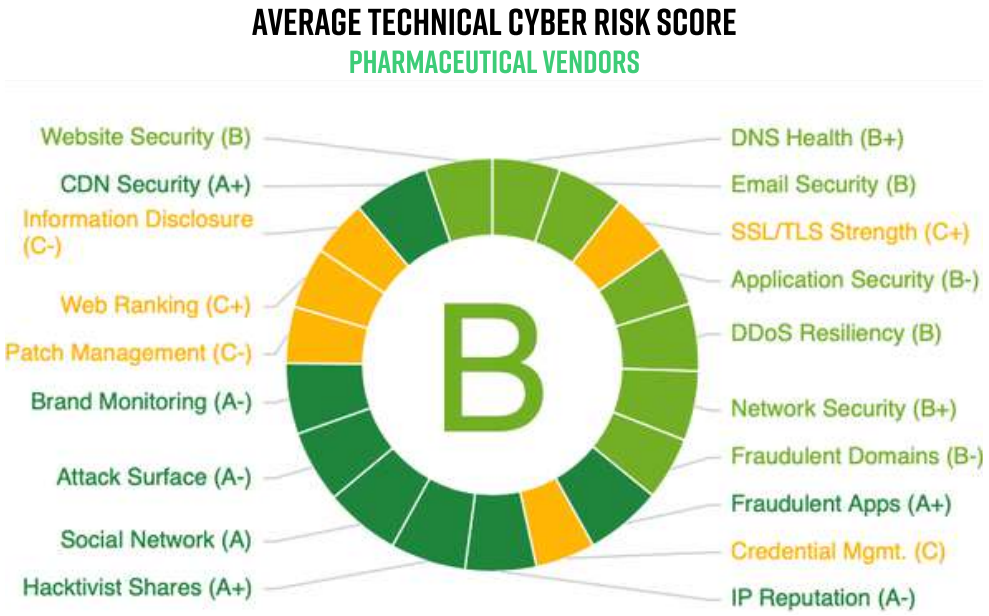
Nearly 5% of software vendors are **highly susceptible** to ransomware.



Nearly 43% of the data management vendors analyzed are highly susceptible to ransomware, making them the r**iskiest vendor category** for pharmaceuticals.

TECHNICAL ANALYSIS OF PHARMACEUTCAL VENDORS

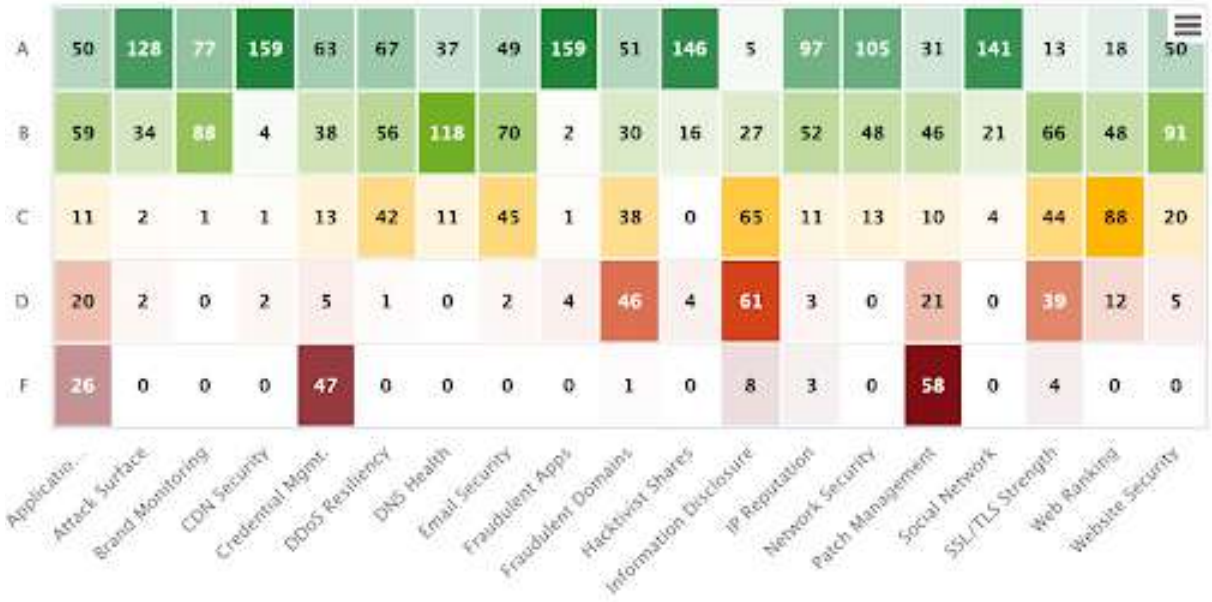
To uncover the factors leading to ransomware susceptibility, Black Kite researchers drilled down even further into the technical findings of each vendor group. The average pharmaceutical vendor reflects a “B” score or “good” rating, which is consistent with an average pharmaceutical company. However, critical security issues are also consistently present.



Credential management and **patch management** again ranked among the lowest-scored categories, receiving a "C" and "C-", respectively. Based on Black Kite’s prioritized technical heat map, 28% of the 166 vendors received an "F" grade in credential management, and 35% received "F" grades patch management.

TECHNICAL GRADE HEAT MAP

PHARMACEUTICAL VENDORS



As explained earlier in this report, fixing software and application vulnerabilities susceptible to a cyber attack is the key to reducing an organization's security risk.

Today most malware, and in particular ransomware, 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.

MOST IMPACTFUL RANSOMWARE ISSUES FOR PHARMA VENDORS	RATE OF OCCURRENCE
Susceptibility to phishing	89%
Publicly visible critical ports	73%
At least one possible high-severity vulnerability due to out-of-date systems	67%
At least one credential leaked in lists shared on deep web in the last 90 days	40%
Experienced a data breach in the past	5%

Susceptibility to phishing and publicly visible critical ports pose the most risk for ransomware to pharmaceutical vendors, with a rate of occurrence similar to pharmaceutical companies. At a 67% rate of occurrence, high-severity vulnerabilities allow threat actors to carry remote code executions on servers, making them highly susceptible to ransomware attacks.

RANSOMWARE ISSUES: PHARMACEUTICAL VENDOR CATEGORY BREAKDOWN

Black Kite Researchers also examined critical security issues for each of the three pharmaceutical vendor categories to see if certain problems are common among specific vendors.

5 MOST IMPACTFUL RANSOMWARE ISSUES FOR PHARMA VENDORS

RATE OF OCCURRENCE

	DATA MANAGEMENT VENDORS	IT SOLUTIONS VENDORS	SOFTWARE VENDORS
Susceptibility to phishing	89%	90%	88%
Publicly visible critical ports	80%	67%	74%
At least one possible high-severity vulnerability due to out-of-date systems	74%	63%	66%
At least one leaked credential found in lists shared on deep web in the last 90 days	57%	37%	34%
Experienced data breach in the past	6%	4%	5%

The analysis revealed data management vendors had slightly more credential-related issues, vulnerabilities due to out-of-date systems, and publicly visible critical ports. This increase in risk is due to statistically restricted IT security budgets and resources for data management companies.

BLACK KITE'S TAKE

"The people you do business with matters, more-so now than ever. Supply chain continuity is *everyone's* responsibility, especially amidst today's evolving cyber landscape. That said, your risk management obligations are never entirely fulfilled, not even after you've achieved a 'good' cyber rating. Your suppliers, partners, vendors and third parties all open other gateways to your network.

Common vulnerabilities leveraged in ransomware attacks aren't a coincidence. Hackers know exactly what to look for—visible ports, outdated systems, phishing opportunities and other attack vectors that don't necessarily reflect a poor cyber hygiene. As security professionals, it's critical that we view our world the way bad actors see it. It's the only way to stay left-of-bang."

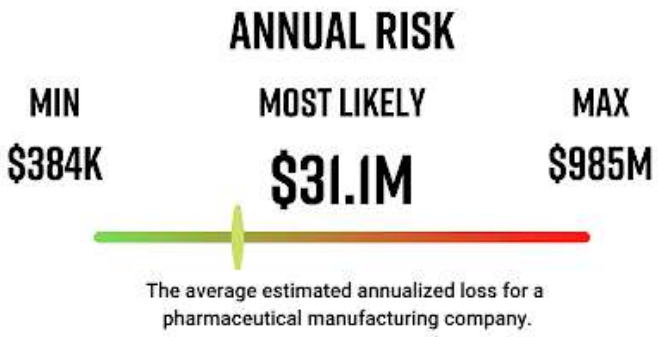
Bob Maley, CTPRP, CRISC, Open FAIR™
Chief Security Officer

RANSOMWARE FINANCIAL RISK: PHARMACEUTICAL MANUFACTURERS & THIRD-PARTY VENDORS

When we recall NotPetya on Merck, the aftermath was devastating, even weeks later. Overall, the attack crippled more than 30,000 laptop and desktop computers at the global drugmaker, as well as 7,500 servers. Many departments, including sales, manufacturing, and research units, were hit. Some employees reported that they lost 15 years of work. More importantly, the breach halted Merck's production facilities for the leading vaccine against human papillomavirus.

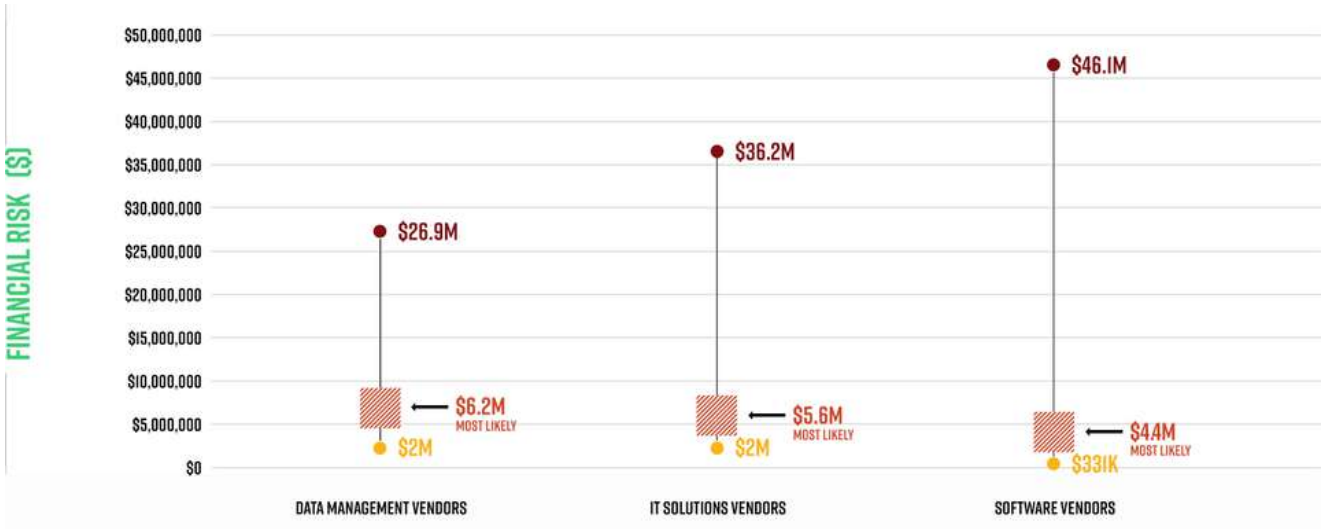
Regarding a ransomware attack, the costs go far beyond the ransom payments themselves, such as replacement costs, i.e., halting business operations, productivity losses, forensic costs, legal costs, and lost business as a result of eroded patient trust. Merck's insurance claims were eventually $1.3 billion.

In light of this information and many cyberattacks on numerous pharmaceutical companies, we derived a formula for the "Cost of a Ransomware Attack" based on the correlation with a pharmaceutical company's revenue. Considering the above parameters, Black Kite researchers calculated the probable financial impact (risk) for each pharmaceutical company. First, researchers derived a "Loss Event Frequency," which is the cyber event frequency a company is likely to have within a year. Upon multiplying the LEF value with the probable cost of a ransomware attack, we could derive the 'Financial Impact Rating' a.k.a the risk.



Risk is not bound to the perimeter of a company. It is inherent across the entire supply chain and third-party ecosystem. Therefore, the risk a vendor brings into the company becomes critical. For the pharmaceutical sector, Black Kite researchers classified the vendors into three categories (data management, software, and IT solutions vendors) to measure the cyber risk in dollars based on the Open FAIR™ methodology.

For the pharmaceutical vendors, the average risk is quite similar across each category. However, the range of probability spans the widest for software vendors due to the variation of vendor company sizes in this data set. On average, data management vendors exhibit the highest financial risk to pharmaceutical companies, approximating $6 million annually.



RECAP & RECOMMENDATIONS

While the daily barrage of ransomware attacks can seem like a daunting challenge, there are proactive measures that pharmaceutical 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 is now a top threat 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 can be complex. 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.

GLOSSARY

Market Capitalization Value: The market value of a publicly-traded company's outstanding shares.

OpenFAIR™: Factor Analysis of Information Risk (FAIR) calculates the estimated financial impact In the case of a cyber breach.

Risk: Probable frequency and probable magnitude of future financial loss.

REFERENCES

[1] *Access to Medicine Foundation* from https://accesstomedicinefoundation.org/
[2] *The Pharma 100: Top Global Pharmaceutical Company Report* from https://torreya.com/publications/pharma1000-intro-presentation-sep2020.pdf
[3] *Pharmaceutical Manufacturing Market Size, Share & Trends Report* from www.grandviewresearch.com
[4] ***Hackers steal Pfizer/BioNTech COVID-19 vaccine data*** **from** https://www.reuters.com/article/us-ema-cyber/hackers-steal-pfizer-biontech-covid-19-vaccine-data-in-europe-companies-say-idUSKBN28J2Q7
[5] *Ransomware attacks on US healthcare organizations* from https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
[6] *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound* from https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
[7] *Vendor Categories* from https://www.pharmamanufacturingdirectory.com/category/technology/it-solutions https://www.pharmamanufacturingdirectory.com/category/technology/software https://www.pharmamanufacturingdirectory.com/category/technology/data-collection-and-handling

CONTACT

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

www.blackkitetech.com