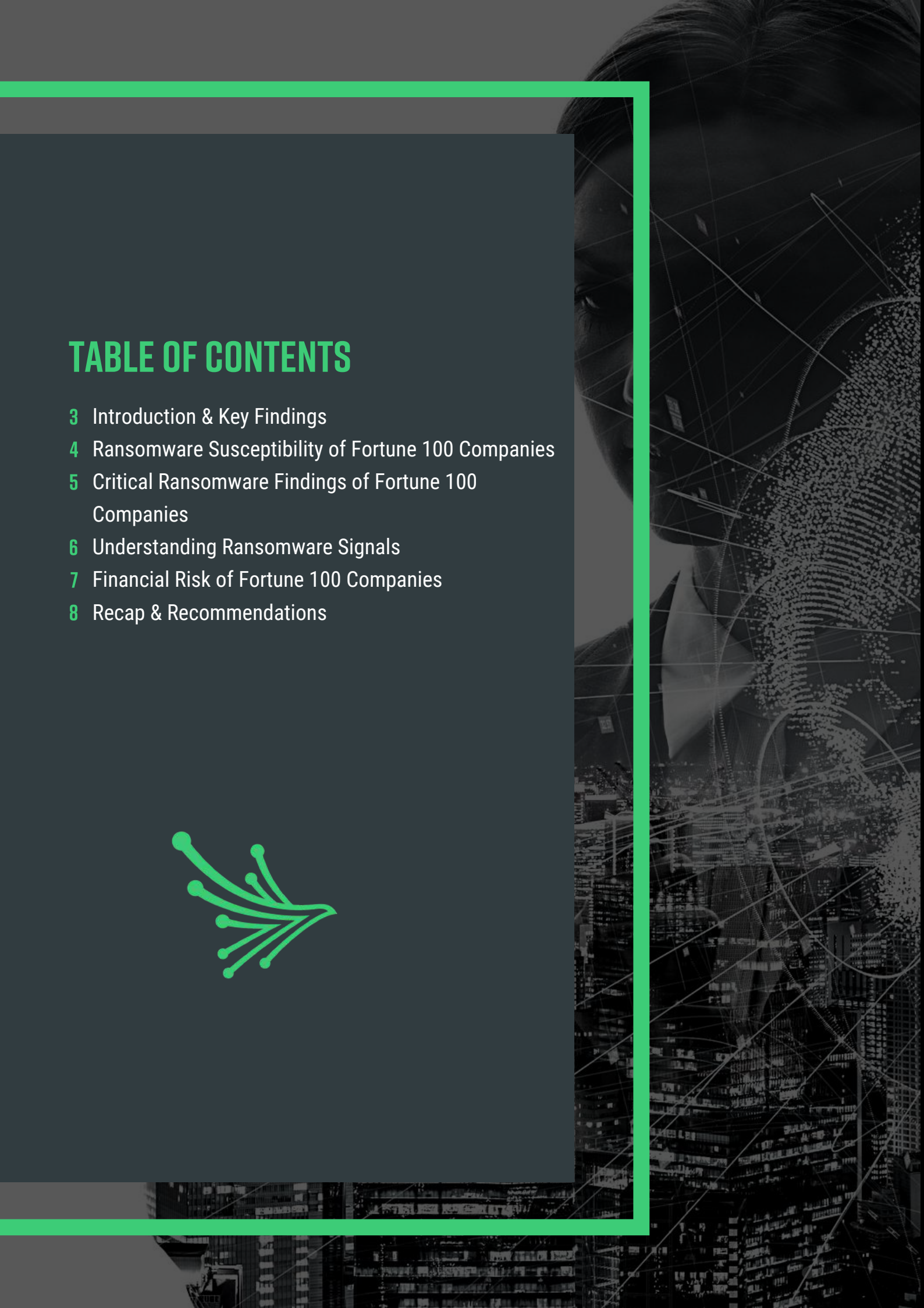
FORTUNE 100: RANSOMWARE RISK REVEALED

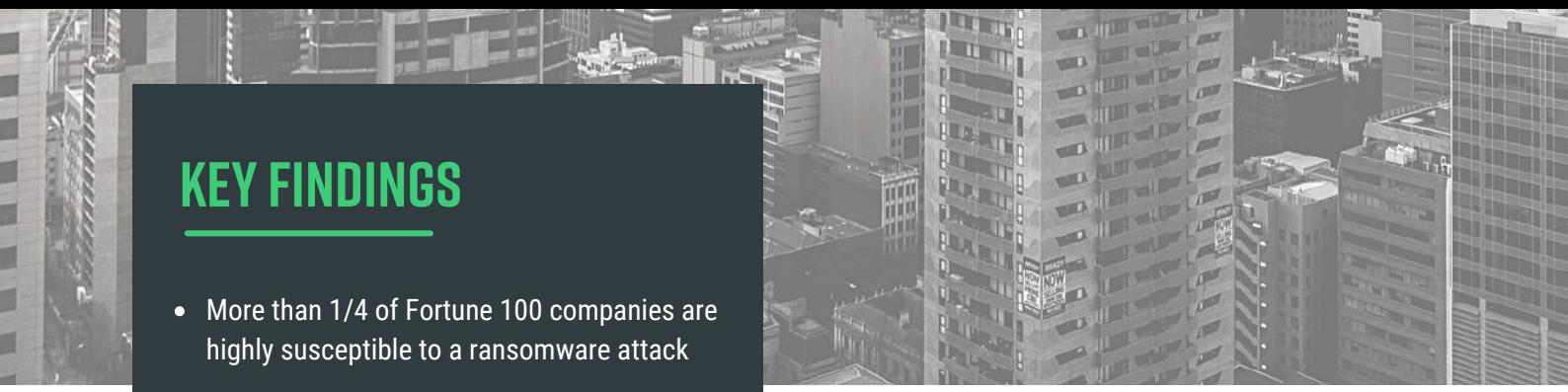
Cyber Risk Trends Among the Largest U.S. Public and Private Companies

BLACK KITE

TABLE OF CONTENTS

3 Introduction & Key Findings
4 Ransomware Susceptibility of Fortune 100 Companies
5 Critical Ransomware Findings of Fortune 100 Companies
6 Understanding Ransomware Signals
7 Financial Risk of Fortune 100 Companies
8 Recap & Recommendations





KEY FINDINGS

- More than 1/4 of Fortune 100 companies are highly susceptible to a ransomware attack
- 60% of Fortune 100 companies have experienced breach in the past
- More than 75% of Fortune 100 companies are likely to Incur a phishing attack
- Credential management is the most prevalent vulnerability for Fortune 100 companies, with 70% having "F" or "poor" ratings

INTRODUCTION

A collection of the most stable, famous, and simply put - richest organizations in America, Fortune 100 companies have built economic models to generate the highest reported revenue in the United States. While sales and capital continue to make these companies eye candy for investors, cybersecurity loopholes are also making these financial monopolies an appetizing target for hackers.

According to a recent report [1] on the digital risk of five hundred Fortune 100 company executives, social engineering (or phishing) based attacks are currently the primary threat to organizations, with an increase in frequency of 667% since January 2020. With individual footprints continuing to expand, corporate digital or social media use policies have not evolved to provide effective and actionable guidelines that properly protect organizations.

Susceptibility to phishing is one of the most common ransomware attack vectors. According to Black Kite's research, more than 1/4 of the Fortune 100 companies are highly likely to encounter a ransomware attack, with 88% of the organizations susceptible to a phishing attack.

Even companies with the largest security budgets and teams are exposed to ransomware risk due to:

- **Artificial intelligence automating PII collection:** Historical phishing attacks utilized manual methods. Modern technology is now making it possible for hackers to automate PII collection and prey on organizations at scale.
- **Historical breaches:** 60% of Fortune 100 organizations have experienced a breach In the past. Cybercriminals are notorious for targeting low-hanging fruit, and anticipate future opportunities for organizations that do not invest adequately in cybersecurity.
- **Expansive and valuable ecosystems:** Fortune 100 organizations have some of the largest supply chain networks, making these companies a prime target for island-hopping into other attack landscapes.

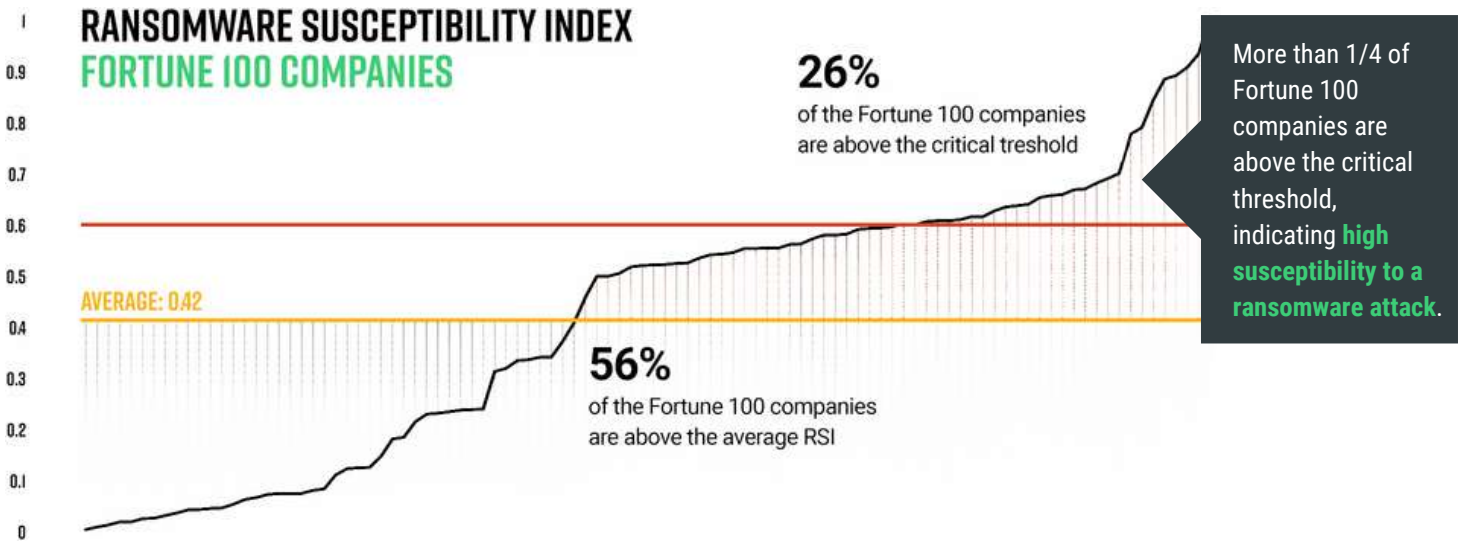
Recent ransomware attacks [2] show cybercriminals are shifting their focus to critical infrastructure, including Fortune 100 companies in the oil, energy and defense industries. These types of attacks can shut down entire supply chains, having a significant impacts on business and personal operations in the United States.

Because Fortune 100 organizations are known for their financial equity, they often do business with each other and overlap within cyber ecosystems. This interconnectivity poses an immense cybersecurity risk, opening doors to a domino effect of security issues throughout the most wealthy organizations In the country.

In this report, Black Kite researchers analyzed the cybersecurity posture and ransomware susceptibility for the Fortune 100 companies of 2021 [3]. Researchers also conducted a detailed study around common security issues in relation to the likelihood of a ransomware attack.

THE RANSOMWARE SUSCEPTIBILITY OF FORTUNE 100 COMPANIES

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.

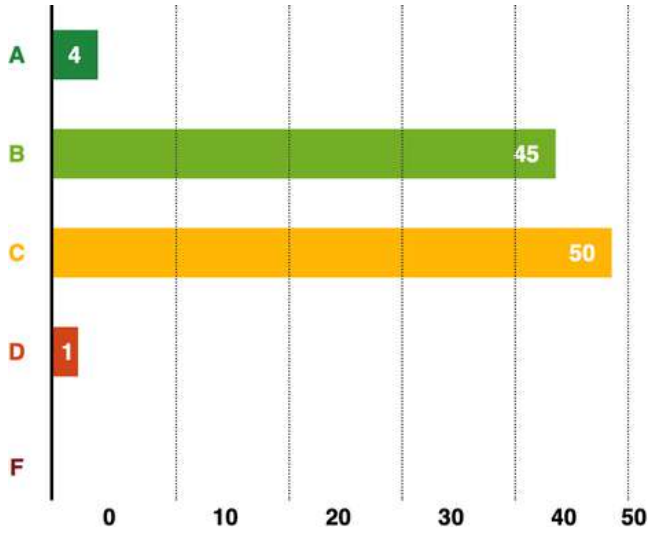
WANT TO UNCOVER TO UNDERSTAND YOUR RANSOMWARE RISK EXPOSURE?

REQUEST A FREE RSI™ RATING

CRITICAL RANSOMWARE FINDINGS OF FORTUNE 100 COMPANIES

AVERAGE TECHNICAL CYBER RISK SCORE

FORTUNE 100 COMPANIES



AT A GLANCE

On average, Fortune 100 companies reflect a “C+”, or “average”, overall cyber risk rating.

However, alarming security are prevalent including companies' susceptibility to phishing attacks, publicly visible ports, and credential management.

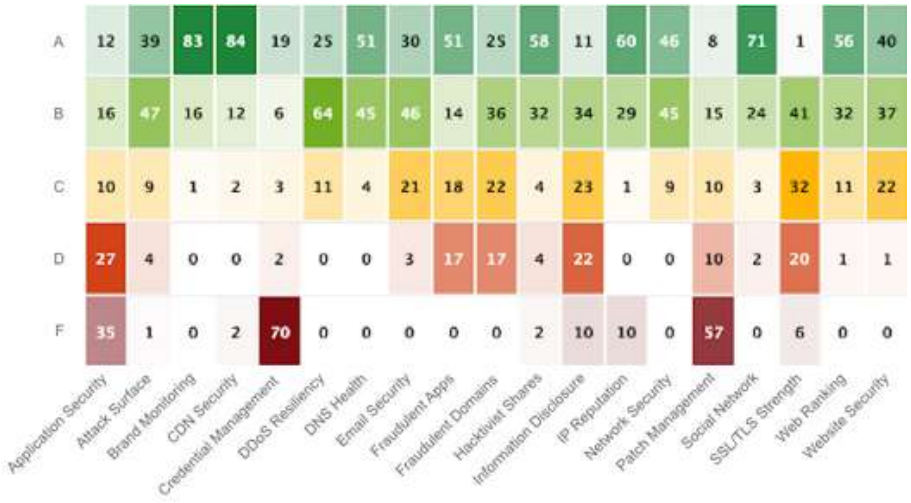
BENEATH THE SURFACE

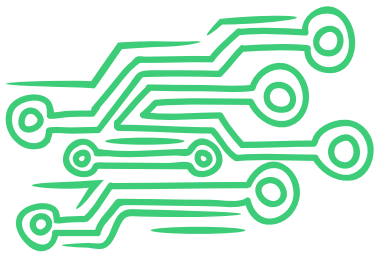
Credential management and **patch management** rank the lowest of the 19 cyber risk categories, with respective "F" ratings.

Based on Black Kite’s prioritized technical heat map, 70% of the 100 companies have "F" grades in credential management, and 57% have "F" grades patch management.

TECHNICAL GRADE HEAT MAP

FORTUNE 100 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 [4]. In fact, software vulnerabilities are common ransomware attack vectors, used one in five times over the last three years.

UNDERSTANDING RANSOMWARE SIGNALS

5 MOST IMPACTFUL RANSOMWARE ISSUES FOR FORTUNE 100 COMPANIES	RATE OF OCCURRENCE
At least one possible high-severity vulnerability due to out-of-date systems	88%
Susceptibility to phishing	88%
Publicly visible critical ports	85%
At least one leaked credential found in lists shared on deep web in the last 90 days	80%
Experienced data breach in the past	60%

CRITICAL RANSOMWARE ISSUES FOUND AMONG FORTUNE 100 COMPANIES

- **At least one possible high-severity vulnerability due to out-of-date systems:** Exploiting vulnerabilities that allow remote code execution is trending in the ransomware community. Although it's not as easy as using RDP ports, it's not as arduous as (spear) phishing.

- **Susceptibility to phishing:** Although the number of phishing incidents associated with ransomware attacks is declining, phishing is still a major attack vector for ransomware variants, such as Cont i v2. It's essential organizations 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 due to the fact that 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. The most recent popular method involves gaining access through credential-stuffing. The combo lists are shared on the dark web every day, and tools that automate the attacking process are helping to increase credential-stuffing attacks. Accessing networks using leaked credentials bypasses many cybersecurity countermeasures and poses a significant risk for ransomware incidents.

- **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. **60% of Fortune 100 companies have experienced breach in the past.**

FINANCIAL RISK FOR FORTUNE 100 COMPANIES

Most CFOs agree a real-time financial data model is critical to enable better business decisions, forecasting models and data accuracy.

Less than half of organizations conduct risk identification quarterly or more often.

Nearly one in 4 CFOs agree real-time insights are the highest priority for their finance function.

RISK IN FINANCIAL TERMS

Black Kite leverages the OpenFAIR™ methodology to transform cyber risk into financial terms. The FAIR calculation is an annual risk quantification that allows a company to estimate the cost of a cyber breach to the organization itself, or caused by a third party. Risk quantification does not include additional reputation loss and legal costs. The below numbers are average values for the 2021 Fortune 100 list, based on an estimate of 100,000 PII records shared.

ANNUAL RISK

MIN	MOST LIKELY	MAX
$25K	$537K	$2.6M

The average estimated annualized loss for an organization.

Based on Black Kite's research, some organizations' annual financial risk is more than $10M, with a projected cumulative risk for all 100 companies of $53.7M.

Ransomware events, which tripled in 2020 compared to the previous year, are estimated to reach $20 billion in 2021 [5]. Not only are these attacks multiplying in frequency, cybercriminals are raising the bar by threatening to publicly release stolen data if victims do not pay the ransom.

BLACK KITE'S TAKE

"The threats to your third-party ecosystem are evolving faster than ever before. Just look at how ransomware has become an epidemic. Any business can be a target of a ransomware gang, even another gang. While preparing to become a ransomware victim is an important business strategy, it is even more important to see your ecosystem the way the bad actors do, and take actions that preempt the attack.

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

RECAP & RECOMMENDATIONS

Cyber crime is a big business — and with a predicted attack rate of once every 11 seconds, ransomware has become the biggest cyber threat to organizations [5]. Whether it is a supplier, vendor, or the cybercriminals are after the organization itself, ransomware attackers are always in search of the weakest links.

KEY TAKEAWAYS

1. Many of the recent ransomware attacks were foreseeable. **Uncover your ransomware susceptibility** today for free with Black Kite's RSI™ here.
2. **Develop an effective course of action.** Companies cannot simply wait for the Federal Government or law enforcement to act. They must take responsibility and act themselves.
3. **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.
4. **Manage risk from a hacker's perspective.** An effective vendor risk management program should focus on what a bad actor would do, and look for indicators of attack (IOA) which could mitigate or reduce the damage of an attack in progress. Assets exposed on the Internet should be observed from the same perspective of a bad actor, which starts with looking for the easiest targets.
5. **Engage the company's board in cybersecurity risk.** Quantification is the key to board engagement and understanding in cybersecurity risk management.

REFERENCES

[1] *Fortune 100 Company Executive Digital Risk Report*
https://www.piiqmedia.com/resources/piiq-fortune-100-executive-risk-report
[2] *Ransomware Report: Latest Attacks And News*
https://www.ransomwarereport.com
[3] *Fortune 100 Companies*
https://fortune.com/best-companies/2021/
[4] *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
[5] *Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021*
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

CONTACT

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

www.blackkite.com