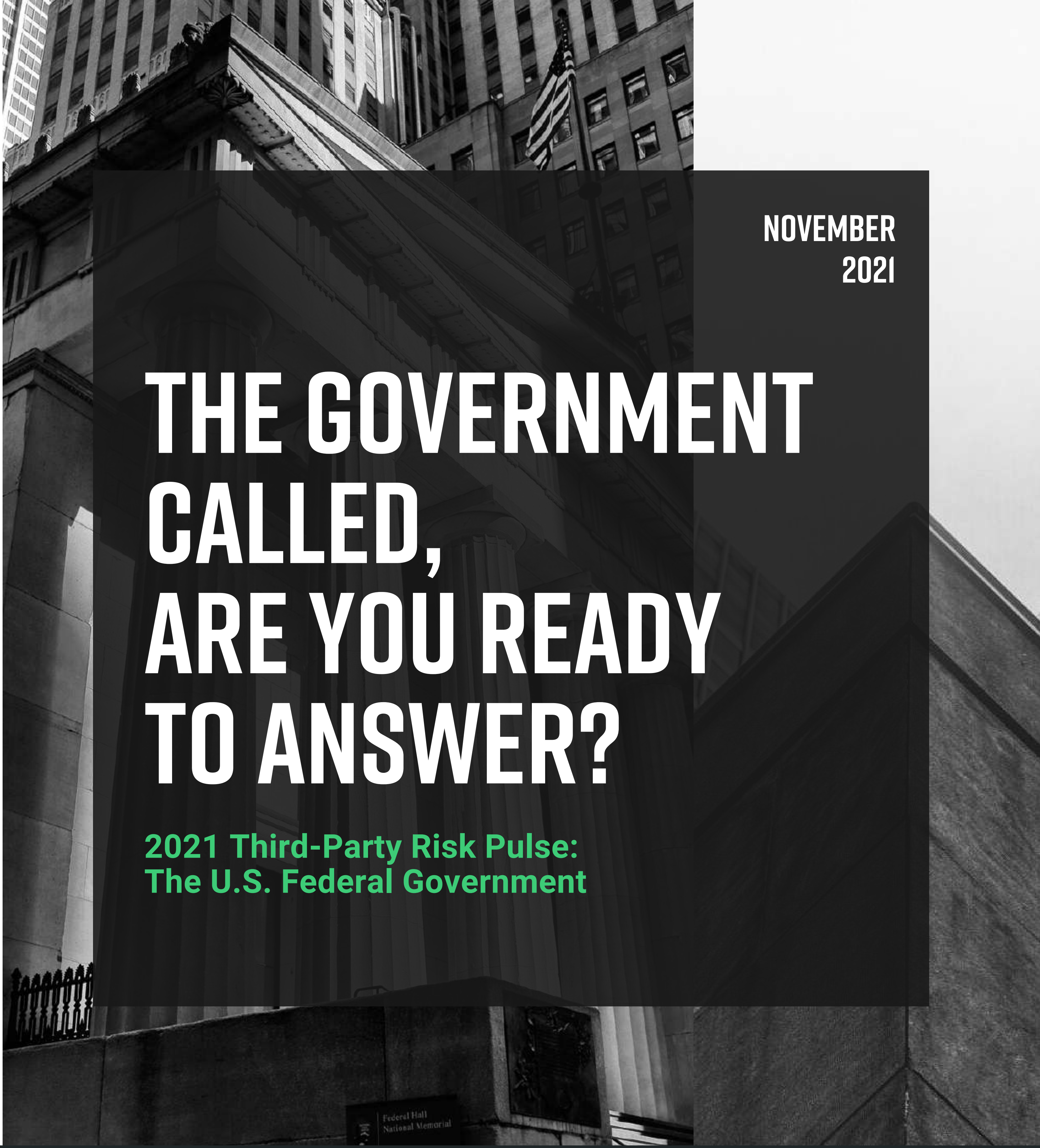


NOVEMBER
2021

THE GOVERNMENT CALLED, ARE YOU READY TO ANSWER?

2021 Third-Party Risk Pulse: The U.S. Federal Government

BLACK KITE

TABLE OF CONTENTS

KEY FINDINGS

- 20% of the top 100 defense contractors are highly susceptible to a ransomware attack
- 42% of defense contractors have had at least one leaked credential within the last 90 days
- Defense contractors are 96% compliant with publicly available CMMC controls
- Patch management is the most common vulnerability, with 43% of contractors rated as an "F" or "Poor"

INTRODUCTION

According to a recent survey around the data security of the federal government [1], 47% of respondents said they experienced a breach in the last 12 months. This year, Black Kite researchers analyzed data across organizations in financial services, healthcare, manufacturing, critical infrastructure, and business services. Each industry told a different story, but two common themes prevailed:

1. Key indicators for ransomware susceptibility remain consistent - email security issues, patch management, and credential management top the list
2. An organization’s true cyber posture can’t be determined with simply a technical rating

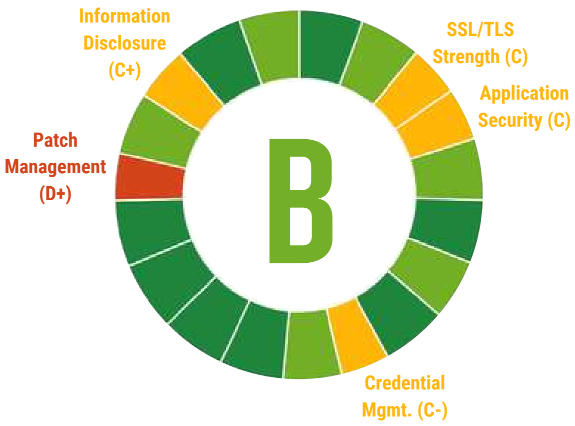
President Biden's Executive Order on *Improving the Nation’s Cybersecurity*, issued days after the Colonial Pipeline cyberattack, emphasizes transparency, demands that organizations work with secure vendors across their digital supply chain, and requires the federal government to partner with the private sector to foster a more secure cyberspace for all.

Since May, the U.S. State Department has announced plans for a bureau of cyberspace and digital policy. The time is now for the federal government to invest in technology advancements that will pinpoint areas of concentrated risk and support public and private sector organizations with proper governance.

Black Kite’s research team completed a detailed risk assessment on the 2020 top 100 defense contractors by contract value [2]. The study examined common security vulnerabilities indicating susceptibility to a ransomware attack, the overall risk landscape for the DoD, and compliance with the Cybersecurity Maturity Model Certification (CMMC).

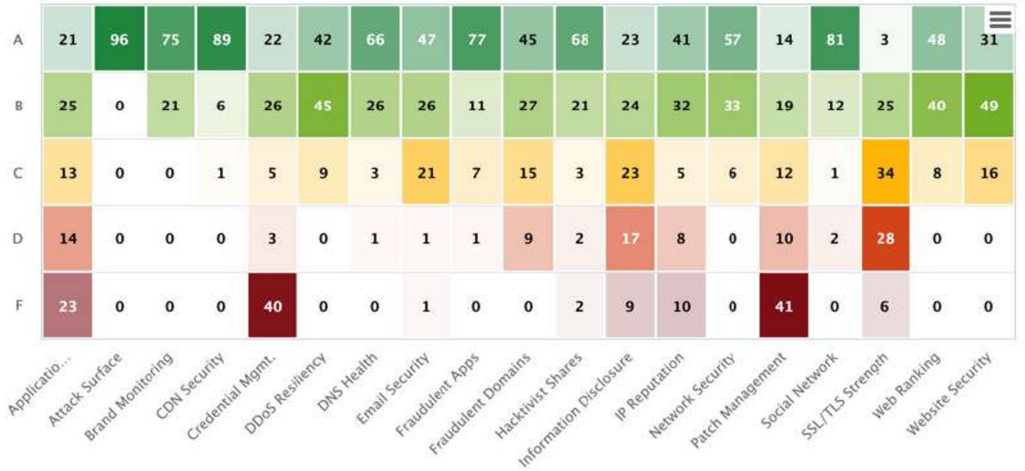
CYBER RISK POSTURE OF TOP DEFENSE CONTRACTORS

On the surface, defense contractors have a “Good” cyber posture, reflected as a “B” rating. However, Black Kite Research identified emerging threats causing the public sector to be a prime target for cyber attacks.



Patch management ranks lowest among the 20 technical categories in Black Kite’s platform, reflecting a “Poor” or “D+” rating. 41, or 43%, of the top defense contractors examined have “F” grades in patch management. Although the overall credential management rating is slightly higher at a “C-,” 40 companies have individual “F” ratings.

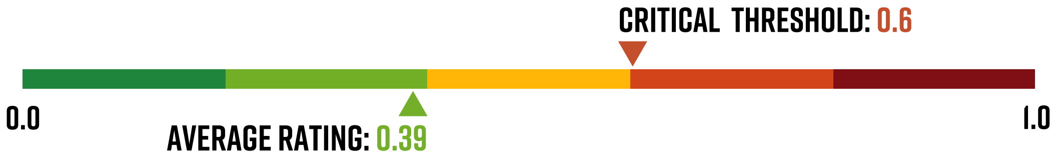
TECHNICAL GRADE HEAT MAP: DEFENSE CONTRACTORS



	Applicatio...	Attack Surface	Brand Monitoring	CDN Security	Credential Mgmt.	DDoS Resiliency	DNS Health	Email Security	Fraudulent Apps	Fraudulent Domains	Hacktivist Shares	Information Disclosure	IP Reputation	Network Security	Patch Management	Social Network	SSL/TLS Strength	Web Ranking	Website Security
A	21	96	75	89	22	42	66	47	77	45	68	23	41	57	14	81	3	48	31
B	25	0	21	6	26	45	26	26	11	27	21	24	32	33	19	12	25	40	49
C	13	0	0	1	5	9	3	21	7	15	3	23	5	6	12	1	34	8	16
D	14	0	0	0	3	0	1	1	1	9	2	17	8	0	10	2	28	0	0
F	23	0	0	0	40	0	0	1	0	0	2	9	10	0	41	0	6	0	0

Why is patch management so important? 42% of companies that experienced a data breach in 2020 blame their own patch failure for making a known vulnerability available to hackers [3]. Not only are security patches critical to reducing ransomware risk, fixing software and application vulnerabilities are a key part of diminishing an organization’s cyber risk.

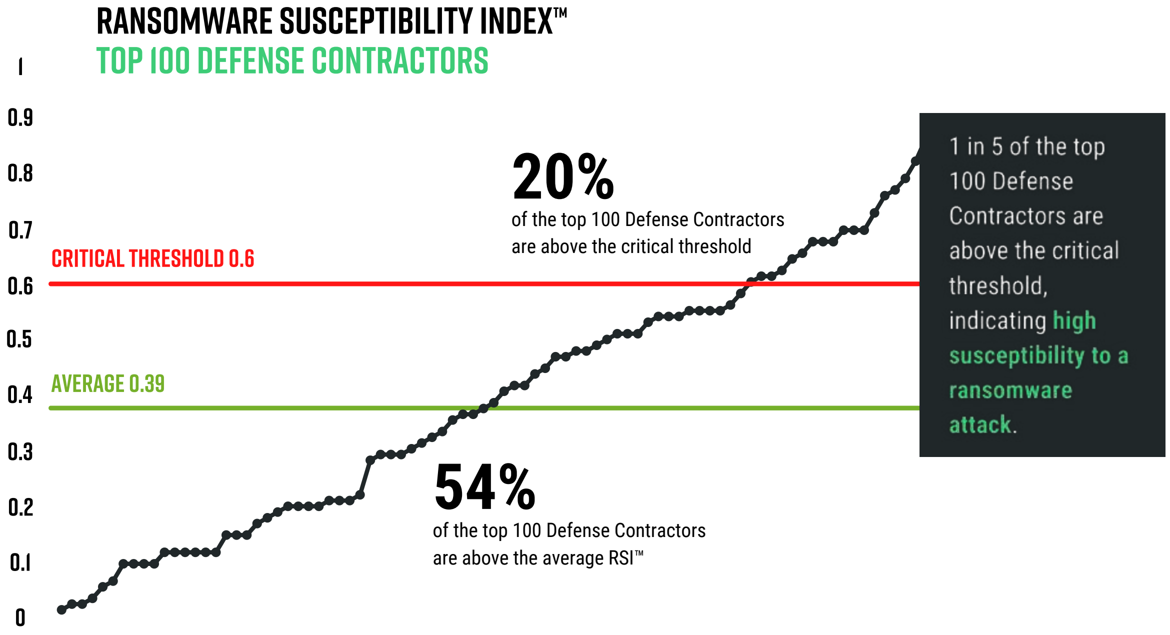
THE STATE OF RANSOMWARE: TOP 100 DEFENSE CONTRACTORS



Black Kite's Ransomware Susceptibility Index™ (RSI™) determines how susceptible a company and its third parties are to a ransomware attack. According to a 2021 survey of CISOs, ransomware is the #1 threat they face in their role [4].

The greatest concerns include:

1. Exposure of sensitive or proprietary data
2. Cost of recovering/restoring to normal operations
3. Loss of revenue due to operational disruptions



RANSOMWARE SUSCEPTIBILITY INDEX™
TOP 100 DEFENSE CONTRACTORS

20%
of the top 100 Defense Contractors are above the critical threshold

54%
of the top 100 Defense Contractors are above the average RSI™

1 in 5 of the top 100 Defense Contractors are above the critical threshold, indicating **high susceptibility to a ransomware attack**.

All defense contractors face susceptibility to ransomware, however some organizations are more vulnerable than others. It's important to note that a low RSI™ score does not guarantee immunity to ransomware attacks. Cybercriminals are opportunistic and may use zero-delay vulnerabilities for more sophisticated attacks, in which a security automation tool may not be able to predict.

RANSOMWARE SUSCEPTIBILITY ACROSS OTHER INDUSTRIES

PHARMACEUTICAL	AUTOMOTIVE
10%	49%
Companies above the critical RSI™ threshold, indicating high susceptibility to a ransomware attack	
86%	64%
At least one leaked credential found in lists shared on the deep web in the last 90 days	
89%	85%
Susceptibility to phising	

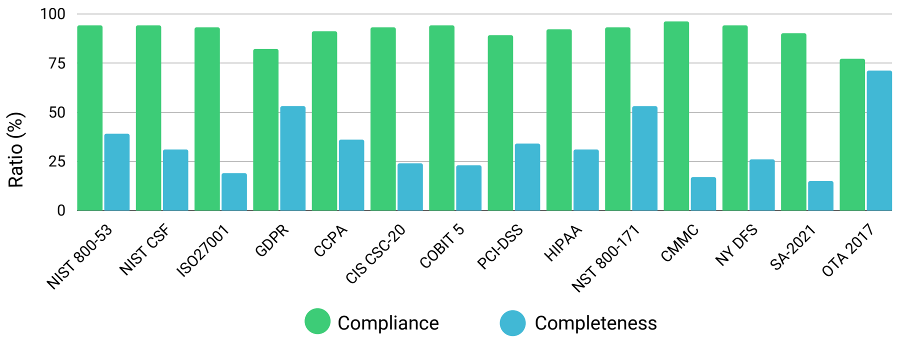
In the past three years, 36% of all cyberattacks significantly disrupted supply chain operations [4]. Ransomware threat actors have shifted their focus, becoming more likely to prey on small to medium-sized companies and their vendors. Certain industries experience more successful attacks than others, particularly the manufacturing sector, with an 81% attack success rate in 2021 [5]. This year, Black Kite Research published two industry reports assessing key ransomware signals for pharmaceutical and automotive manufacturing companies.

PRELIMINARY CMMC FINDINGS OF TOP 100 DEFENSE CONTRACTORS

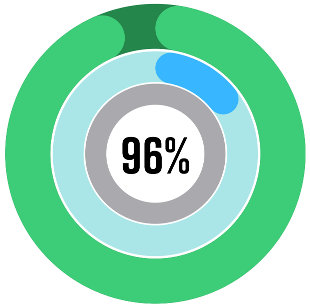
While the certification deadline continues to fluctuate, CMMC will be a leading indicator to better equip public and private organizations contracted with the DoD. Automation and continuous monitoring will be key to earning and maintaining higher CMMC levels.

CMMC is one of 14 global standards already available for compliance mapping in the Black Kite platform. The information is reported in terms of **"Compliance" (green ring)** and **"Completeness" (blue ring),** correlating directly how much of the global standard has been analyzed. For the 17% of CMMC controls we see in our external data collection process, Defense Contractors are 96% compliant.

COMPLIANCE OVERVIEW: DEFENSE CONTRACTORS



CMMC



Similar to how technical ratings fail to provide a comprehensive cyber risk posture, even highly compliant organizations are still susceptible to cyber attacks. Where external information isn't available, Black Kite's Universal Policy and Questionnaire Examiner (UniQuE Parser) consumes a wide variety of questionnaire and policy documentation to fill in the gaps.

Outside of the federal cybersecurity frameworks that comprise CMMC, defense contractors can get a head start today by looking at internal compliance, alongside the compliance levels of subcontractors across international standards such as ISO 27001, NIST 800-53, NIST CSF, and NIST-171.

RECAP & RECOMMENDATIONS

The federal government is at a crossroads. Both public and private sector companies are susceptible to cyber attacks, but with limited information sharing it's almost impossible to paint a comprehensive picture of the threat landscape. The government will be responsible for setting the precedence for collaboration, with support from cyber-focused organizations that understand the points of concentrated risk in today's digital supply chains.

Continuously Monitor Your Cyber Posture

Point-in-time assessments, such as penetration tests or questionnaires, do not provide an accurate picture of cyber risk or signal that a data breach might occur. Continuous monitoring is only possible with security automation, which provides alerts to emerging vulnerabilities as they arise. Continuous monitoring also helps prioritize and manage risks across the entirety of an organization's supply chain.

Understand Supply Chain Risk

A comprehensive risk management program monitors not only internal threats, but also those of third-parties. Seek to adopt a vendor risk management model that classifies organizations within the supply chain and identifies critical data sharing points for asset prioritization.

Develop a Course of Action - Begin the CMMC Process Today

Until CMMC becomes a formal requirement, start by learning its technical requirements and preparing internal resources for certification. Automate your overall compliance process with a standards-based tool that supports documentation upload to fill in any gaps.

REFERENCES

[1] **2021 Thales Data Threat Report - U.S. Federal**
https://cpl.thalesgroup.com/data-threat-report

[2] **Top 100 Defense Contractors 2020**
http://fi-aeroweb.com/Top-100-Defense-Contractors.html

[3] **Mitigate Vulnerability Challenges in the Cloud and On-Premises**
https://www.ibm.com/account/reg/us-en/signup?formid=urx-46992&_ga=2.38070435.1044506647.1626880624-1800770014.1626688714

[4] **The Business Costs of Supply Chain Disruption**
https://impact.economist.com/perspectives/sustainability/business-costs-supply-chain-disruption-1

[5] **Ransomware In Focus: CISO's Connect, Sponsored by Black Kite**
https://blackkite.com/whitepaper/ransomware-in-focus-new-research-from-a-cisos-perspective/

ABOUT BLACK KITE

One in four organizations suffered from a cyber attack in the last year, resulting in production, reputation and financial losses. The real problem is adversaries attack companies via third parties, island-hopping their way into target organizations. At Black Kite, we're redefining vendor risk management with the world's first global third-party cyber risk monitoring platform, built from a hacker's perspective.

With 300+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence. While other security ratings service (SRS) providers try to narrow the scope, Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: technical, financial and compliance.

CONTACT US

✉ info@blackkite.com

☎ +1 (571) 335-0222

📍 800 Boylston Street, Suite 2905
Boston, MA 02199