BLACK KITE

CENTRALIZING SUPPLY CHAIN CYBERSECURITY

U.S. FEDERAL GOVERNMENT RISK IN 2022

TABLE OF CONTENTS

KEY FINDINGS

- 72% of the top 100 defense contractors have at least one leaked credential in the last 90 days *(compared to 42% in November 2021)*
- 20% of the top 100 defense contractors are still highly susceptible to a ransomware attack after our follow-up analysis 6 months later
- 17% of the top 100 defense contractors have at least one possible critical vulnerability due to out-of-date systems
- 46% of the top 100 defense contractors are 3x more likely to experience a cyber breach than those with "A" technical ratings

INTRODUCTION

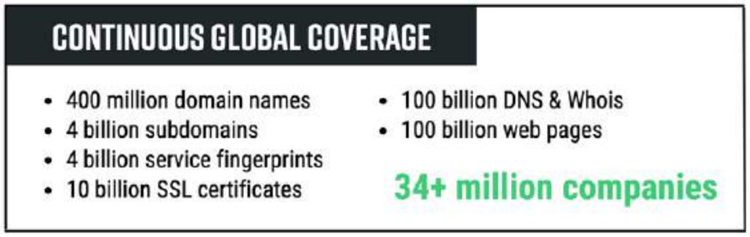
Over the last 12 months, the federal government has spearheaded a sense of urgency to protect critical infrastructure and the nation from increasing cyber threats. With the establishment of the National Cyber Director's office in January 2021, a comprehensive Executive Order in May, and new guidelines for cyber incident reporting, a desired cohesive strategy has emerged.

Cybercriminals are unyielding, and many cyber attacks are still flying under the radar. The devastating attacks capturing news headlines demonstrate critical ongoing cybersecurity weaknesses in the supply chain, furthering the need for continuous monitoring of high-risk vulnerabilities. Black Kite's platform has the power to provide visibility into the cyber architecture of the supply chain, and address issues that must be resolved to ensure resiliency.

Black Kite Research released 'The Government Called, Are You Ready to Answer? [1]' in November 2021, which examined the third-party cyber risk posture of the U.S. federal government. In that report, the team conducted an analysis on the top 100 defense contractors by contract value in 2020 [2].

Black Kite operationalizes non-intrusive, powerful scans that tap a vast data lake, accessing information on 34 million companies — 4x that of our competitors. Proactive behavior requires cyber intelligence that prompts the operationalization of threat data. This behavior also requires data that is trustworthy and standards-based.

By using the same level of data and intelligence, our team was able to research the current cyber posture of the public sector and provide an update into the issues that federal organizations are facing in their cybersecurity efforts.



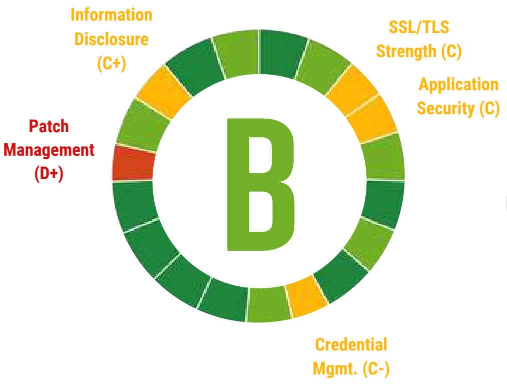
CONTINUOUS GLOBAL COVERAGE

- 400 million domain names
- 4 billion subdomains
- 4 billion service fingerprints
- 10 billion SSL certificates
- 100 billion DNS & Whois
- 100 billion web pages

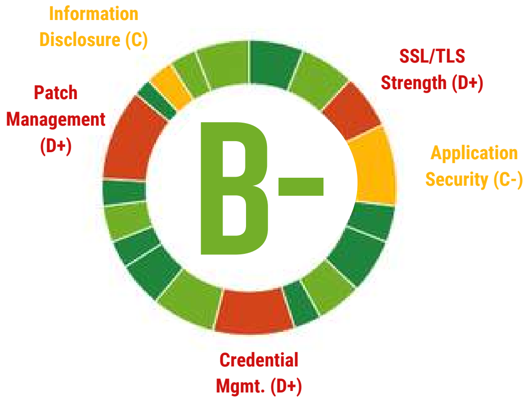
34+ million companies

THIRD PARTY INTELLIGENCE TO STAY LEFT OF BOOM U.S. DEFENSE CONTRACTORS

In an effort to provide consistent and updated market analyses, Black Kite Research conducted a follow-up investigation of the same top 100 defense contractors, six months later.



TOP 100 DEF CONTRACTORS - NOVEMBER 2021



TOP 100 DEF CONTRACTORS - MAY 2022

Since the release of our first report, the cyber posture of defense contractors decreased from a “B” rating to a “B-.” While both are classified with a relatively “Good” standing, we see decreases in a number of critical technical categories:

- **Credential Management: D+**
- **Attack Surface: B-**
- **SSL/TLS Strength: D+**
- **Application Security: C-**

Credential Management continues to be a key concern for defense contractors. **72% of analyzed contractors had at least one leaked credential available on the dark web in the last 90 days.** Maintaining widespread visibility of credential leaks is imperative, but difficult, especially within the realm of third, fourth and nth parties.

In the 2021 Data Breach Investigations Report by Verizon [3], 61% of the 5,250 confirmed breaches analyzed can be attributed to leveraged credentials. These logins are often a threat actor’s primary means of entry to an organization, and an even larger issue if the credentials lead to privileged information.

Black Kite’s findings tell the full story, providing a multidimensional view of your entire global attack surface from a technical, financial impact, and compliance perspective. The platform is scalable to any number of companies in need of analysis and monitoring. Findings are derived from 20 technical categories graded according to MITRE Cyber Threat Susceptibility Assessment (CTSA) and NIST. Black Kite has over 500 control points corresponding to MITRE's TTPs. These standard scoring models eliminate false positives, creating trustworthy, defensible metrics.

MOST CRITICAL ISSUES

This research uncovered an alarming increase in federal organizations with an “F” rating in both Information Disclosure and SSL/TLS Strength. Any weakness in these categories can create an extremely risky situation, putting the privacy of U.S. citizens, and security of critical infrastructure at risk. Why? Let’s dive in.

INFORMATION DISCLOSURE

Misconfigured services or other public assets may disclose local IPs, email addresses, version numbers, WHOIS privacy records, and other sensitive information.

Information disclosure occurs when a system fails to properly protect sensitive information from parties that are unqualified to have access to such information in normal circumstances. In most cases, these types of issues are not exploitable. However, they are considered security issues because they allow attackers to gather information that can be used later in the attack lifecycle to steal additional information.

For example, during the completion of the 2020 follow-up bipartisan subcommittee report [4], the Department of Education’s security was actively tested. The Inspector General was successfully able to extract hundreds of PII files, including sensitive data and 200 credit card numbers — *all without the agency detecting or blocking the action.*

SSL/TLS STRENGTH

SSL refers to Secure Socket Layer whereas TLS refers to Transport Layer Security. They both refer to cryptographic protocols that encrypt and authenticate data between the user and a web server. SSL/TLS and SSH prevent intruders from tampering with communication, as well as listening to the communication that passes between the server and the user. This is especially important when sensitive data, such as personal information, payment details, etc. is disseminated.

EQUIFAX BREACH: WHAT HAPPENED?

One of the most significant data breaches in the last decade was Equifax [5]. The 2017 breach resulted in more than 140 million individuals’ PII leaked, due to the attacker gaining network access and extracting database intel. At the time, the IRS, the SSA, and the USPS relied on Equifax as their identity verification service. According to the congressional report [6] on the breach, Equifax allowed, at minimum, 324 of its SSL certificates to expire. 79 of these certificates were connected to devices monitoring critical domains.

In a statement within the 2018 congressional report, they found, “Equifax did not see the data exfiltration because the device used to monitor ACIS network traffic had been inactive for 19 months due to an expired security certificate. On July 29, 2017, Equifax updated the expired certificate and immediately noticed suspicious web traffic.”

Long story short, Equifax did not realize they had this vulnerability until it was too late. Poor SSL/TLS strength puts the critical data of the United States at risk, not to mention the ripple effect of damages that the economy could incur.

DEPARTMENT OF DEFENSE BUG BOUNTY PROGRAM

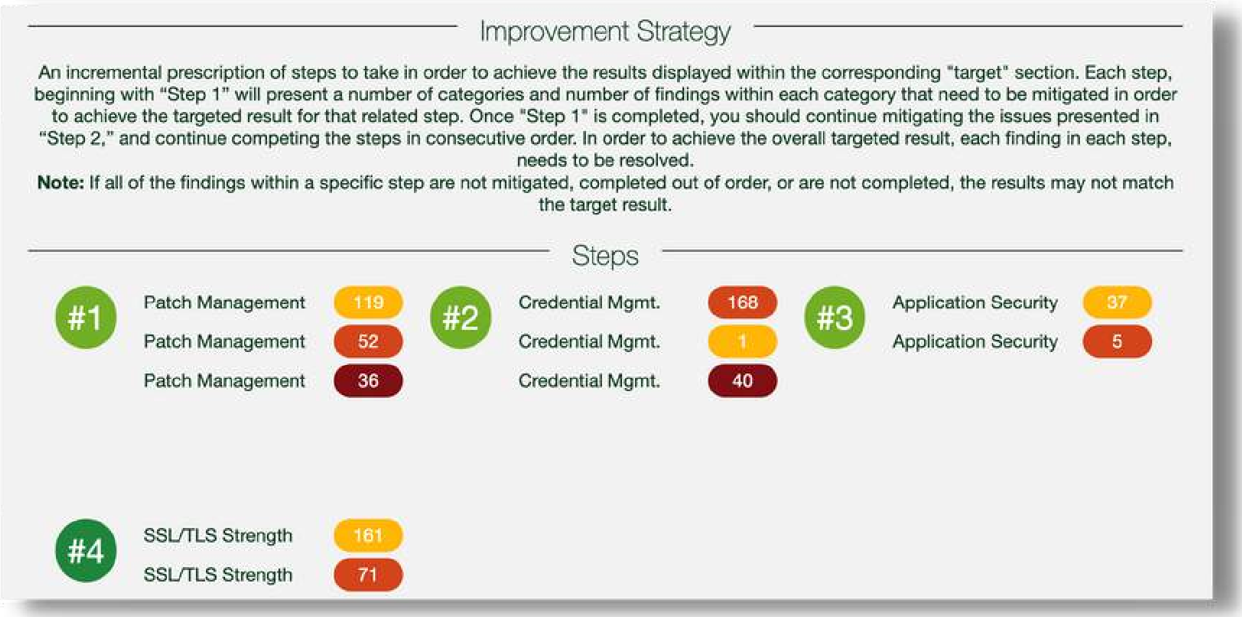
A U.S. Department of Defense pilot program, [7] designed to root out digital vulnerabilities among contractors and companies that work for the department, identified hundreds of flaws over the course of one year.

Starting in April 2021, 400 issues across dozens of organizations were found, putting ethical hackers and crowdsourced information to work. The pilot program was “intended to identify whether similar critical and high-severity vulnerabilities existed for small-to-medium-cleared and non-cleared DIB companies with potential risks for critical infrastructure and the U.S. supply chain.”

Fourteen companies participated, with 141 examinable assets, but the group grew to 41 companies and 350 assets by the end.This approach to cyber risk is extremely powerful, and Black Kite’s platform has the capacity to auto-discover and analyze thousands of companies and assets - in minutes. With standards-based methodology and the utilization of open-source intelligence, vulnerabilities can be found in near real-time, scalable to any number of companies or vendors.

The Department of Defense has over 200,000 companies within their contracting ecosystem, hinting at hundreds, if not thousands, of vulnerabilities that need to be found and flagged. This is especially imperative for a department that is under attack or experiencing threats on a regular basis.

By providing continuous monitoring, Black Kite has the power to revolutionize that communication process between departments and agencies and the vendors who serve them that are affected by high-profile cyber events.



Improvement Strategy

An incremental prescription of steps to take in order to achieve the results displayed within the corresponding "target" section. Each step, beginning with “Step 1” will present a number of categories and number of findings within each category that need to be mitigated in order to achieve the targeted result for that related step. Once "Step 1" is completed, you should continue mitigating the issues presented in “Step 2,” and continue competing the steps in consecutive order. In order to achieve the overall targeted result, each finding in each step, needs to be resolved.

Note: If all of the findings within a specific step are not mitigated, completed out of order, or are not completed, the results may not match the target result.

Steps

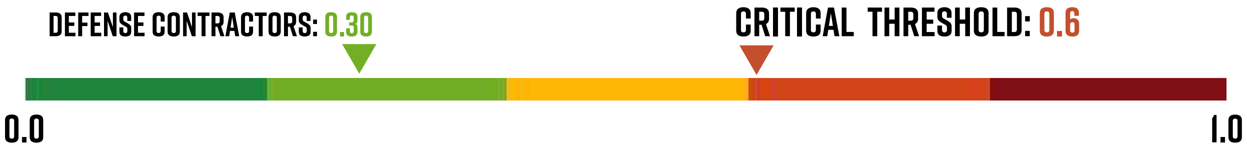
#1	Patch Management	119
	Patch Management	52
	Patch Management	36
#2	Credential Mgmt.	168
	Credential Mgmt.	1
	Credential Mgmt.	40
#3	Application Security	37
	Application Security	5
#4	SSL/TLS Strength	161
	SSL/TLS Strength	71

RANSOMWARE POSTURE

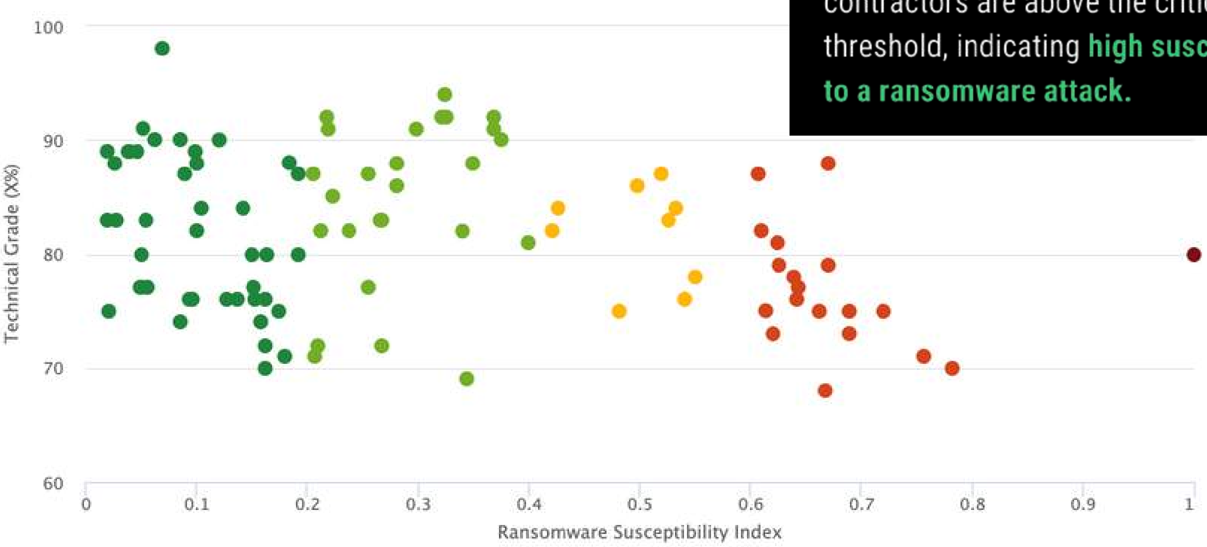
According to a survey of government organizations around the world conducted by Sophos [8], 40% of central government and 34% of local government organizations were hit by ransomware within the last year.

This report calls the government ransomware problem a 'national emergency,' with even more survey respondents reporting they expect to be hit by an attack in the future. This is particularly concerning given that the U.S. Government is one of the largest holders of personal identifying information (PII).

Black Kite is the only cyber risk intelligence platform that analyzes an organization's susceptibility to ransomware. The Ransomware Susceptibility Index™ uses AI and machine learning to discover the likelihood that you or one of your vendors will experience an attack.



The average RSI™ for defense contractors is **0.3**, however, **of the 100 organizations analyzed, 20% received an RSI™ rating above the critical threshold of 0.6.** These ratings indicate a **high** level of susceptibility to a ransomware attack, but lower ratings do not guarantee that an organization is fully protected. Continuous monitoring for changes is still imperative.

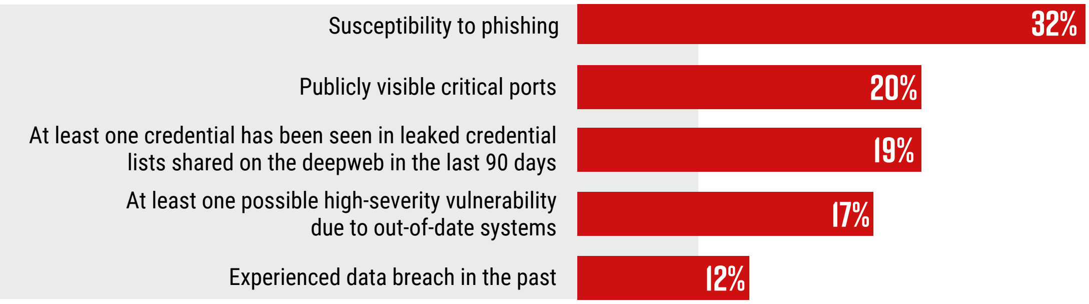


1 in 5 of the top 100 defense contractors are above the critical threshold, indicating **high susceptibility to a ransomware attack.**

As Black Kite Research further examined the RSI™ vs. Technical Cyber Rating, high susceptibility to ransomware correlated to a lower rating and overall poorer cyber health rating.

RANSOMWARE POSTURE: CRITICAL ISSUES

Of the most impactful ransomware-related security issues for the top 100 defense contractors studied, susceptibility to phishing is the most common. **32% of the companies studied are vulnerable,** so it is important to discuss why phishing still creates significant opportunity for threat actors. Phishing is known to be extremely low risk for threat actors, but if successful, can be a source of high gains.



CISCO's 2021 Cybersecurity Report [9] suggests that 86% of organizations had at least one person click a phishing link last year. Furthermore, the data suggests that phishing accounts for around 90% of data breaches.

LOCAL GOVERNMENT: MORE VULNERABLE?

Threat actors succeeded in encrypting the data of 69% of targeted local government organizations.

According to the Sophos report mentioned above, 69% of local government organizations hit by ransomware said the cybercriminals succeeded in encrypting their data — a full 20 percentage points higher than central government organizations. Cybercriminals are pivoting their tactics to target smaller, seemingly more vulnerable organizations that might offer entry into larger organizations with more financial resources.

Local governments often deal with smaller IT teams, higher counts of outdated systems, and limited cybersecurity budgets — facing pressure to divert those funds to public services. Even if the ransom is paid by these organizations, critical systems like utilities and public safety may be compromised long-term.

The most common requests include revealing a credential, sharing personal information, or giving access to a platform. Even something as simple as a credential can be all a bad actor needs to gain access to PII.

With the government being the one of the largest holders of PII, these access issues quickly cause big problems. This leads to another pressing issue: Leaked credentials. Once a credential is secured, leaking it on the deep web is a second step that can lead to a domino effect of risk, giving access to not only the original cyber criminal, but anyone who finds the credential.

17% of the top 100 defense contractors studied have at least one possible critical vulnerability due to out-of-date systems. Out-of-date systems, and systems that are no longer receiving security updates are an obvious, but often ignored issue, that facilitate access points for hackers to exploit. Often these imperative system updates are ignored due to systems still being capable of completing daily work tasks.

THE STATE OF CYBER ESPIONAGE

As incidents have increased across the board, and across industries, federal agencies have experienced some of the most damaging attacks in the last decade. In 2020, 30,819 information security incidents were reported across the Federal Government, rising 8% from 2019.

30,819 **INFORMATION SECURITY INCIDENTS REPORTED ACROSS THE FEDERAL GOVERNMENT IN 2020.**

In the staff report referenced earlier on federal cybersecurity, eight key federal agencies [DHS, State, DOT, HUD, USDA, HHS, ED, and SSA] were analyzed and inspected to fully understand the state of their cybersecurity posture, on the assumption that the United State's data was at risk.

The results were astounding, including documentation that as of 2019, zero of the eight agencies met basic cybersecurity protocols expected of them. One of the most alarming findings was that all eight of the agencies were actively using out-of-date systems and applications — systems that were no longer receiving security updates or patches from the vendor, creating endless cyber vulnerabilities.

When revisited in 2020, nearly none of the recommended changes were made, effectively putting the stored sensitive data at risk. By continuing to delay these needed changes, PII and national security secrets are remaining vulnerable to talented and determined threat actors targeting the U.S. Government.

Data, PII, and national secrets are not the only component at risk. Targeted and malicious cyber activity costs the United States billions of dollars in damages every year.

Malicious Activity: *as defined by the CEA,* is an activity, other than one authorized by or in accordance with U.S. law, that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident thereon.

In fact, according to the 2018 CEA Report on Malicious Cyber Actors on the U.S. Economy [10], in 2016 alone, this activity cost the U.S. economy over 57 billion dollars.

Damage cascaded past the initial target as well, hitting interconnected firms. What sector poses the highest risk to the economy if impacted? **Critical infrastructure.**

Critical Infrastructure

According to CISA [11], "the assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

EXPERT INSIGHTS

MIKE BROWN

RADM, USN, (Ret.) & Founder/President, Spinnaker Security LLC

How is the cyber perspective changing in the federal world? What regulations do we anticipate for the future?

In both my public and private sector experience, I've found that most cybersecurity issues lead to the road of cyber hygiene. I believe we will never get ahead of the wave if we don't have visibility into potential vulnerabilities and activities on an ongoing basis, prioritize them, and make genuine efforts to fix them.

In recent years, the government has put forth a number of time-consuming policies, regulations and best practices that attempt to change the cybersecurity culture and hold people and organizations accountable, but we still don't quite hit the mark.

Recently, the government is starting to look at how to develop comprehensive federal regulations that account for well known cyber risks within the supply chain and the potential for its impact in critical infrastructure, specifically. The past 20 years have seen many legislative and regulatory attempts to increase the security posture of the public and private sectors, starting with the Federal Information Security Management Act of 2002, which is in the process of seeing another update.

My hope for the future is that the government puts forth a strategy that synergizes various frameworks and cybersecurity policies into an easy-to-understand architecture that allows public and private sector organizations to not only comply, but feel confident in making decisions that will improve their cyber hygiene while addressing their specific risks.

We are moving in the right direction, but priority should continue to be placed on using cloud and SaaS systems with built-in security and tools to help automate crucial processes. The government must move away from offering tools and processes and create executable rules and regulations that deliver capability for all organizations.

EXPERT INSIGHTS

BOB MALEY

Chief Security Officer, Black Kite

Is the government doing enough?

The government is *doing a lot,* but I don’t think they are *doing enough of the right thing*.

Lately, we’ve seen a handful of proposals come out of the government. We saw the executive order on Zero Trust in 2022, as well as the upgrade from CMMC Level 1 to Level 2 which applies to the defense industrial base. There’s no shortage of things happening and moving pieces to observe.

But what question should we be asking? How agile are those things that the government is doing to reduce the risk to our government systems? Is it enough particularly for our 16 sectors of critical infrastructure? Many of the companies in the critical sector are actually private companies that receive checklists, plans, “should do’s” and “should haves.”

But guess what? Threat actors look right over all the imposed regulations. They see the attack surface and they say **“how do we get in and how do we complete the objective?”** That is where the government is lacking - understanding of where threat actors gain access, get in and do the most damage.

In today’s current environment, critical infrastructure seems to be caught in the crosshairs. This has a lot to do with tensions around the world, as well as bad actor groups taking sides within these wars and attacking with political motivation. At the end of the day, these groups operate as a business and must keep the bottom line in mind, often monetizing the weakest link.

The biggest frustration is seeing the government recommend the same practices and warnings for decades: patch management, passwords, etc. Groups are just choosing not to implement said repetitive recommendations. Potential solution? Encourage and entice people to want to do the right thing, to embrace agile thinking, without merely adding more regulations to their “never-ending” list.

EXPERT INSIGHTS
JEFFREY WHEATMAN

Senior VP, Cyber Risk Evangelist, Black Kite

Is the government overstepping?

In reality, this question is asking two separate things – Is what the government doing effectively supporting national cybersecurity goals? And is the government getting too involved?

Regarding whether the guidance is useful or not, I think the challenge has been that the people creating policy do not fully understand the implication of what they are suggesting or requiring. Lawmakers frequently lack the technical background necessary to create effective guidance.

This leads to checkbox compliance efforts that do not address the true underlying risk(s). We have a long history of the government stepping in to regulate or fix things, and often making things worse. It isn't uncommon for requirements to have outsized impacts on business objectives. Companies subject to onerous requirements may end up secure and compliant but could be forced out of business due to the cost of compliance.

As far as overstepping — I think we have seen repeatedly that, left to their own devices, most organizations will sideline security to hit financial targets. This includes critical infrastructure providers that act as the underpinnings for our entire nation.

Without oversight and regulation, we would be exposed to bad actors in grossly unacceptable ways.

So is the government overstepping? I would not go as far as to say that. Until we see evidence that critical infrastructure is focusing on reasonable cybersecurity investment, oversight will always be needed. However, we need balance, perspective, relevancy, consistency, and an understanding that you cannot legislate away risk.

Get experts involved, bring industry expertise, and find a balance between the need to run the organization and the need to protect the organization.

OPERATIONALIZING BLACK KITE INTELLIGENCE

TOP GLOBAL DEFENSE INDUSTRIAL BASE VENDOR

The Black Kite platform is built from a hacker's perspective, leveraging MITRE frameworks to communicate cyber risk in a common language. After aggregating hundreds of data sources from open-source intelligence (OSINT), MITRE CTSA is the foundational scoring matrix to map vendors in our system using a well-known industry standard.

Black Kite provides an automated remediation plan for each one of your vendors. In our Strategy Report, we highlight the vendor's current posture and outline a set of prescriptive steps that are designed to advise them on increasing their cyber risk and reducing financial risk.

A top 10 global defense contractor transformed their cyber security posture in less than two weeks, based on the defensible data provided to them within the platform.

There were visible decreases in patch management vulnerabilities (improving from an F to a D), as well as an SSL/TLS strength improvement from a C to a D. A significant increase in CDN Security moved the grade from a D to an A.

However, while the overall rating improved, our ransomware indicator found an increase in critical software vulnerabilities. Our ransomware susceptibility index follows a process of inspecting, transforming, and modeling data with the goal of discovering the likelihood of a ransomware incident. Black Kite's data is collected from a variety of OSINT sources such as internet-wide scanners, hacker forums, the deep/dark web, and more.

These vulnerabilities rose to 37 findings, up from 25 when first assessed. 36/37 of the findings are critical patch management issues and they are all PATCH-001 findings with CWSS scores of 7.8-9.8. Each finding maps back to MITRE standards and verifiable scoring.

In the original assessment, 10 critical misconfiguration findings were a second strong indicator of ransomware susceptibility, including missing DKIM records, DMARC vulnerabilities, and poor email security. According to DMARC.com [12] "The DMARC check reveals that your domain is not secured and is subject to spoofing attacks. Any spoofing attacker can send malicious emails using your domain, which potentially incurs damage to your brand after landing in your customers' mailboxes."

This speaks to the need for continuous monitoring - Black Kite's federal solution can help preserve critical national security functions.

MOVING FORWARD

TONY MONELL **VP of Public Sector**

Throughout the course of my 30 year career in government, it wasn't uncommon to feel conflicted when trying to solve large problems affecting ordinary Americans in a technology-driven world. How do we strike the balance between putting the right bureaucratic guardrails in place to protect our everyday way of life, while keeping up with cyber threat actors that shift tactics faster than the government can react?

Instead of finding this balance, policymakers default to layering more regulation on top of already onerous regulations. Lawmakers continue to lobby for legal action against companies that serve the government for failure to report breaches or attacks. The decision to "fix" private industry is to use "more stick and less carrot", forcing small to mid-tier suppliers, which comprise the largest demographic of vendors to the federal government, to weigh the cost/benefit analysis of continuing to do business with the public sector.

As the largest consumer in the world, the U.S. Government spends over $650 billion on products and services each year through the private sector [13], leaving both inextricably linked.

The public sector relies heavily on the private sector for innovation, investing heavily in more digital capabilities, from cloud-based management platforms to IoT-enabled factories to remote technology.

The same pace of technological advancement and digital connectivity that contributes to America's global edge is also challenging us in cyberspace [14]. And that trend is not likely to abate anytime soon.

A 2020 CSIS-McAfee report [15] estimated that global losses from cybercrime now total over $1 trillion annually, coupled with the pacing challenge of ceding economic/national security competitive advantage through the loss of intellectual property by state-sponsored attacks.

A free and open internet has created a permissive environment where threat actors can launch disruptive and destabilizing attacks against U.S. critical infrastructure and the entire U.S. economy.

Fortunately, last May, the Administration tossed out a lifeline, requesting the private sector work closely with the federal government to protect the Nation from malicious cyber actors, outlined in the Executive Order on Improving the Nation's Cybersecurity.

The release of that E.O., however, has now created another concern for government buyers in the market: how to sort through the thousands of cybersecurity vendors vying for billions of federally funded contracts up for land grab.

MOVING FORWARD

TONY MONELL VP of Public Sector

In most cases, when the federal government establishes any requirement, trends are instantly born overnight. More recently, the movement is towards developing AI/machine learning and analytic regimes to be more disruptive to threat actors. Here are some of my recommendations to help navigate evaluating any service provider to defend your ecosystem :

- **Start with a service that incorporates ALL of vendor data into one analytical tool, using a standards-based framework commonly benchmarked in the world of cybersecurity, such as MITRE or NIST.**

- **Ensure this platform is able to scale deeply into your vendor base, all the way down to your nth parties, with the ability to reflect real world cyber events within 48-72 hours on every vendor in your supply chain. This opens communication between the federal government and affected vendors, where remediation becomes a priority.**

- **Next, ensure any service you procure includes step-by-step remediation tools that small to mid-sized companies with less seasoned cybersecurity professionals can understand and implement. If the remediation is assessed against benchmarked cybersecurity standards, the results are easily defensible for smaller vendors.**

- **Finally, ensure a service provider is able to establish a historical record of data breaches, and a ransomware indicator to determine the most at risk vendors in your ecosystem. If you don't have a sense of a vendor's health, you place your whole supply chain at risk of attack.**

Asking these tough questions of prospective service providers will help save time from having to recompete vendors year after year. Moreover, your organization will minimize costs, build resilience into your supply chains, and preserve the unique capabilities suppliers' offer to the federal government, regardless of their size. That's how you use more carrot and less stick.

REFERENCES

1. The Government Called, Are You Ready to Answer? 2021 Risk Pulse: US Federal Government - Black Kite
2. Top-100 US Defense Contractors FY 2020 | FI AeroWeb
3. 2021 Data Breach Investigations Report | Verizon
4. HSGAC Senate.gov
5. Equifax Data Breach Due to Unknown Certificate Expiration | Sectigo® Official
6. https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf
7. Pentagon finds hundreds of cyber vulnerabilities among contractors
8. The State of Ransomware in Government 2021
9. Cybersecurity threat trends: Cisco Umbrella
10. https://www.hsdl.org/?view&did=808776
11. Critical Infrastructure Sectors | CISA
12.How to fix "No DMARC Record Found"
13. Selling Greener Products and Services to the Federal Government | US EPA
14. Mr. Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy, Before the Senate Armed Services Committee Subcommittee on Cybersecurity
15. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
16. Compromised Passwords Responsible for Hacking Breaches
17. https://www.gao.gov/assets/gao-18-559.pdf

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 350+ 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