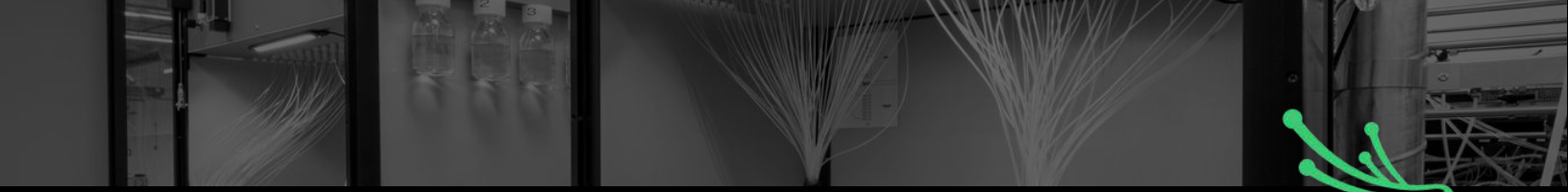


BIOTECHNOLOGY SUPPLY CHAIN RISK ANALYSIS

VULNERABILITIES IN THE THIRD PARTY ECOSYSTEM

October 2022

BLACK KITE

INTRODUCTION + SCOPE

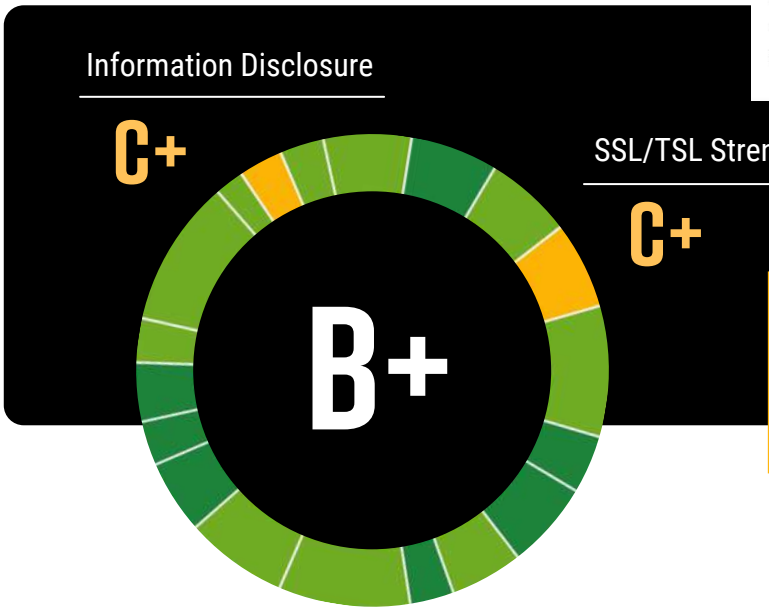
When the production of vital medicine, completion of essential research, and preservation of essential data is on the line, understanding relative third party risk is essential. It is a requirement and a responsibility.

For this analysis, Black Kite Research utilized the power and scale of the Black Kite platform to analyze the current cyber posture of 738 biotechnology companies across the globe. Black Kite operationalizes non-intrusive, powerful scans that tap a vast data lake, accessing information on 34+ million companies.

This technical rating is a weighted average of 20 risk categories mapping back to 290 controls with their proper MITRE classifications.

TECHNICAL CYBER RATING

Overall Average of Analyzed Biotech Entities



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

***10%** of biotech companies have a **C or lower** technical rating.*

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.

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.

MOST COMMON ISSUES AND VULNERABILITIES

Black Kite assesses cyber security through 20 technical categories where each category represents a different aspect of the holistic view of a true external assessment. The chart below summarizes the companies' performance for each category in a letter-grade format.

	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	289	476	239	416	507	560	418	177	737	345	735	135	269	614	272	737	38	93	341
B	279	201	499	89	102	177	295	379	1	133	3	254	267	70	168	1	322	290	293
C	53	35	0	225	28	1	25	160	0	114	0	173	98	54	76	0	269	322	100
D	51	20	0	8	10	0	0	22	0	145	0	148	72	0	40	0	100	32	4
F	66	6	0	0	91	0	0	0	0	1	0	28	32	0	182	0	9	1	0

For example, the category of Patch Management has a **grade of F** for 182 companies within the analyzed group of 738.

MOST CRITICAL ISSUES: A BREAKDOWN OF THE TOP 2

Overall, **3.4k** critical findings were discovered in this analysis across all 738 companies. The top two most critical issues found were **SMTP Open Relay** and **Cleartext Transmission of Sensitive Information.**

SMTP Open Relay is an SMTP server configured in such a way that it allows anyone on the Internet to send email through it, not just mail destined to or originating from known users. An open relay is the proliferation of its usage by spammers looking to obscure or even hide the source of the large-volume emails they send.

Cleartext Transmission of Sensitive Information is the failure to encrypt sensitive communications. An attacker who can sniff traffic from the network will be able to access the conversation, including any credentials or sensitive information transmitted.

Applications frequently fail to encrypt network traffic despite the necessity of protecting sensitive communications. Encryption (usually SSL) must be used for all authenticated connections, including Internet-accessible web pages and backend connections.

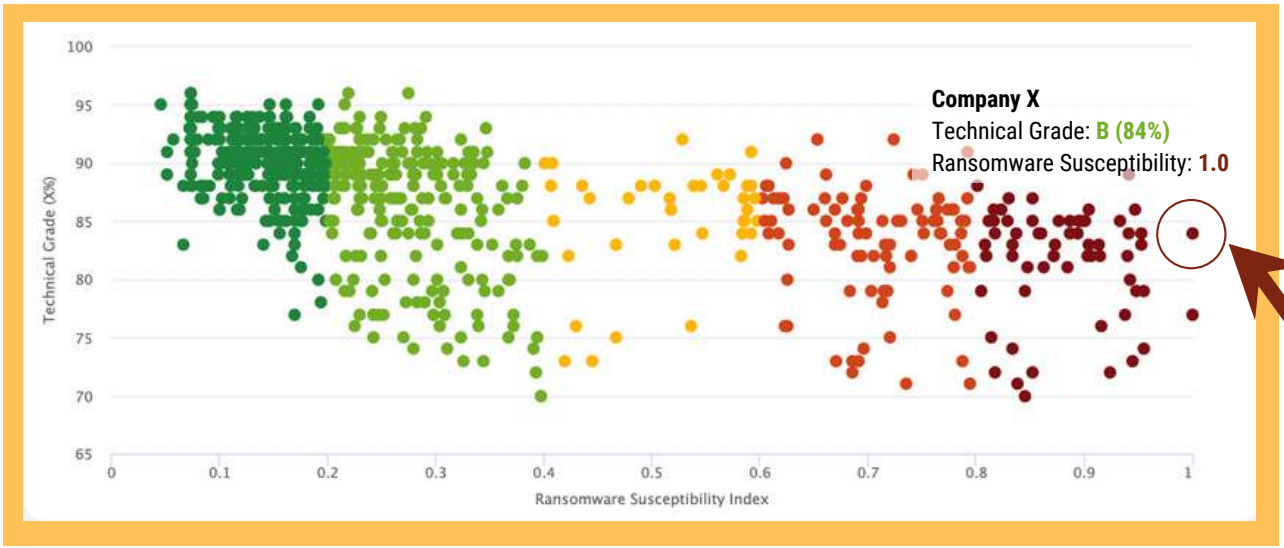
RANSOMWARE SUSCEPTIBILITY INDEX™

Black Kite is the only cyber ratings platform that can identify ransomware susceptibility for a company in advance of an attack. Using data and machine learning, Black Kite's RSI™ discovers the likelihood that an organization will experience a ransomware attack.

The Black Kite RSI™ follows a process of inspecting, transforming, and modeling data collected from 400+ OSINT sources (internet-wide scanners, hacker forums, the deep/dark web) as well as taking common indicators into account, including a third party's location, industry, and annual revenue. Using this data and machine learning, the correlation between control items is identified to provide approximations.

An RSI™ over 0.4 shows an evident risk of ransomware while an RSI™ over 0.6 shows a **significant** risk.

20% of the analyzed companies received an RSI™ above the critical threshold of 0.6, indicating a *high level of ransomware susceptibility*. It's important to note low susceptibility does not grant immunity to ransomware. Threats and vulnerabilities emerge every second, making continuous monitoring and proactive response time essential.



As Black Kite Research further examined the RSI™ vs. Technical Cyber Rating, high susceptibility to ransomware correlated to a lower rating and overall poor cyber health. The visual here is important.

The upper right side of this chart shows companies with higher technical ratings (A's and B's) and higher RSI™ ratings, showing that an organization's cyber posture should be examined from all angles. For example, one company highlighted in dark red has a 'B' rating, but an **RSI™ rating of 1.0** indicating a 100% susceptibility to a ransomware attack.

QUANTIFIED FINANCIAL RISK WITH THE OPEN FAIR™ MODEL

The Open FAIR™ model is used to calculate the probable financial impact if a third-party vendor, partner, or supplier experiences a breach. Not all vendors pose the same amount of risk to your organization. More privileged access inherently produces a higher price tag in the event of a data breach.

The average annual financial risk of Biotechnology companies, in the case of a cyber attack ->

WHAT IS OPEN FAIR™?

Factor Analysis of Risk (FAIR) is the only international standard Value-at-Risk model for information security and operational risk.

ANNUAL FINANCIAL RISK

$92K

$3.4K		$4.7M
Minimum	Most Likely	Maximum

The forecasted annualized loss based on the given parameters in the Open FAIR™ Model.

Black Kite is the world's only fully transparent, standards-based cyber ratings platform, ensuring all users know exactly how their findings are calculated, providing the confidence to take action.

EXPERIENCE THE CYBER RISK INTELLIGENCE

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 500+ 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.