BLACK KITE

THE COST OF A DATA BREACH REPORT

A New Perspective

A data-driven study of the financial impact of global data breaches in the last five years.

2022

TABLE OF CONTENTS

KEY FINDINGS

- Overall average cost of a data breach (including outliers) - **$75.21 million**
- Overall average cost of a data breach (outliers removed) - **$15.01 million**
- Most financially devastating threat actor: **Conti**, with 10 attacks averaging **$84.98 million per incident**
- **79%** of the 1,700 analyzed breached companies are **highly susceptible to a phishing attempt**
- The **finance and insurance** sectors experienced the *most incidents* (445), with an average cost of **$35.34 million per incident**
- **17%** of the 1,700 analyzed breached companies are **highly susceptible to a ransomware attack**

INTRODUCTION

What does a data breach truly cost a company? What about a ransomware incident?

In the last decade, the financial impact of data breaches has increased dramatically, approximately ten percent each year according to the 2021 CyberSecurity Ventures report [1].

At this rate, the global cost of cybercrime could reach upwards of $10 trillion in the next three years, up $7 trillion from 2015. According to the 2022 IBM Cost of a Data Breach report [2], individual incidents are already averaging $4.35 million (an all-time high).

Coincidentally, the shift from in-office to remote work over the last three years has added to this drastic increase, with the average cost per breach of remote workers coming in at approximately $1 million higher than company breaches without remote workers.

Most current data breach cost studies are either survey-based or done through conducted interviews. For example, the annual IBM Cost of a Data Breach Report interviews thousands of security professionals to approximate the total cost per breach for an organization.

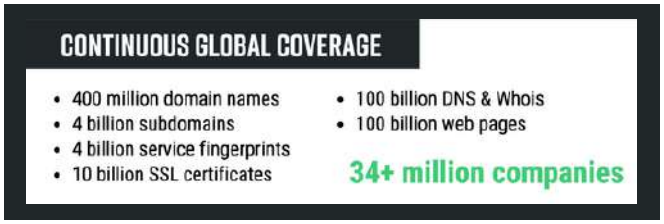
For this report, Black Kite Research decided to approach the cost of a data breach from a new angle, to build upon survey-based data in a comprehensive way. A team of 14 researchers conducted a global data breach cost analysis curated with OSINT techniques, encapsulating 2,400 data breach incidents from 2017-2022. The thorough cost analysis includes information on regulatory fines, court settlements, paid ransom, victim notification, business loss, and more.

INTRODUCTION CONT.

With this research in hand, the team utilized the power and scale of the Black Kite platform to analyze the current cyber posture of the 2,400 affected organizations, finding that only 1,700 still had a digital presence that could be monitored.

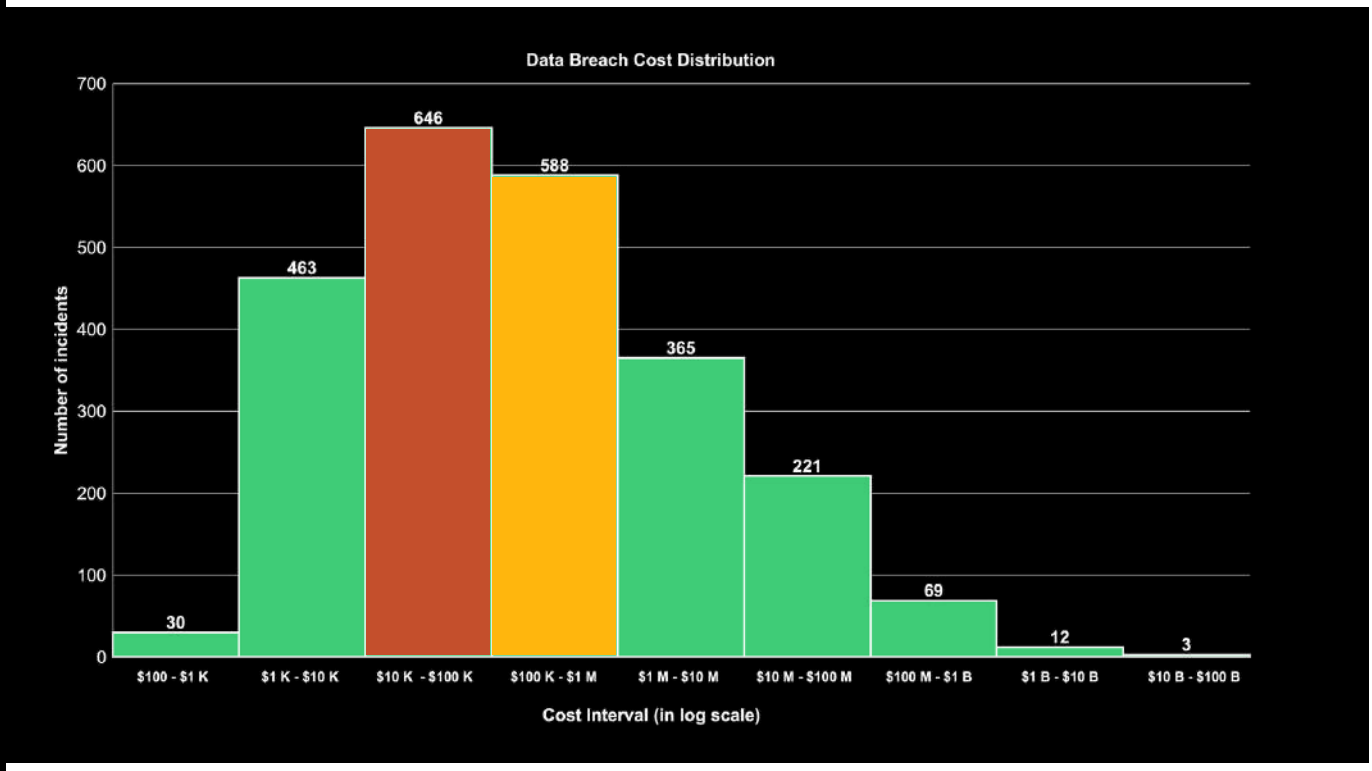
- **The first half of this report provides insight into the 2,400 analyzed data breaches**
- **The second half, the cyber risk posture deep dive, covers a thorough analysis of the 1,700 organizations that are still online and in business today**

Black Kite operationalizes non-intrusive, powerful scans that tap a vast data lake, accessing information on 34 million companies — 4x that of our competitors.



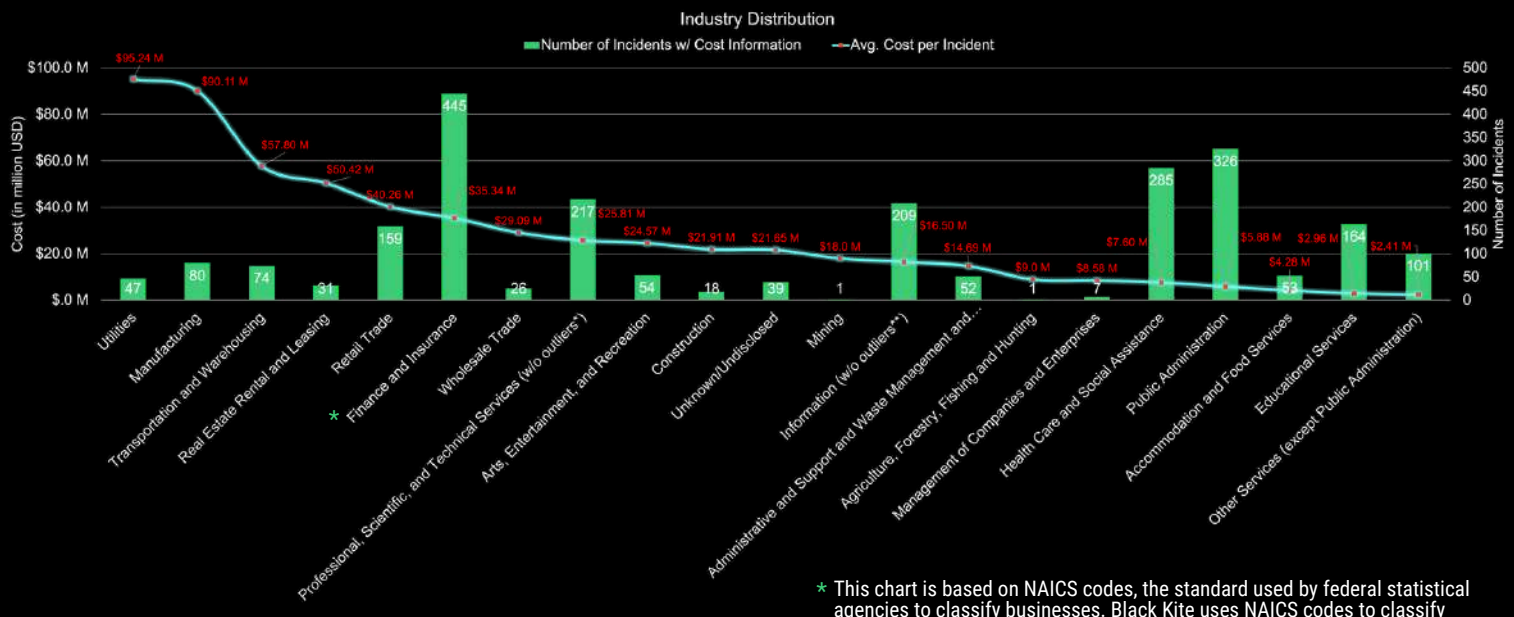
Proactive behavior requires cyber intelligence that prompts the operationalization of threat data. This behavior also requires data that is trustworthy and standards-based.

OVERALL COST DISTRIBUTION



The overall cost of a data breach is widely distributed, but **more than half (51%) fall between a cost of $10,000 and $1 million.** Another 15% of analyzed breaches cost between $1 million and $10 million, following the predictions that cybercrime could be a trillion dollar industry in the near future.

OVERALL COST PER INDUSTRY



* This chart is based on NAICS codes, the standard used by federal statistical agencies to classify businesses. Black Kite uses NAICS codes to classify companies by industry for benchmarking and other comparison purposes.

FINANCE AND INSURANCE

Within our research, the average incident cost per industry revealed that the finance and insurance sectors experienced the highest number of breaches with a combined total of 445 (19%) incidents and an average cost of $35.34 million per incident.

Finance and insurance companies hold significant amounts of sensitive data and, simply put, hackers are looking for sensitive information to gain a financial advantage. Both industries are also subject to the growing Internet of Things (IoT) challenge, where new technologies like mobile banking, chatbots, and online claims processing mean more interconnectivity than ever. Many of these organizations use email to conduct financial transactions [3], presenting an opportunity for adversaries to insert themselves into the process.

PUBLIC ADMINISTRATION

Public administration emerged as the next sector with the highest incident count, with 326 (14%) incidents and an average cost of $5.88 million per incident.

State and local governments are attractive targets for adversaries. Often not because of the financial opportunity, but for the ability to disrupt society at the local level.

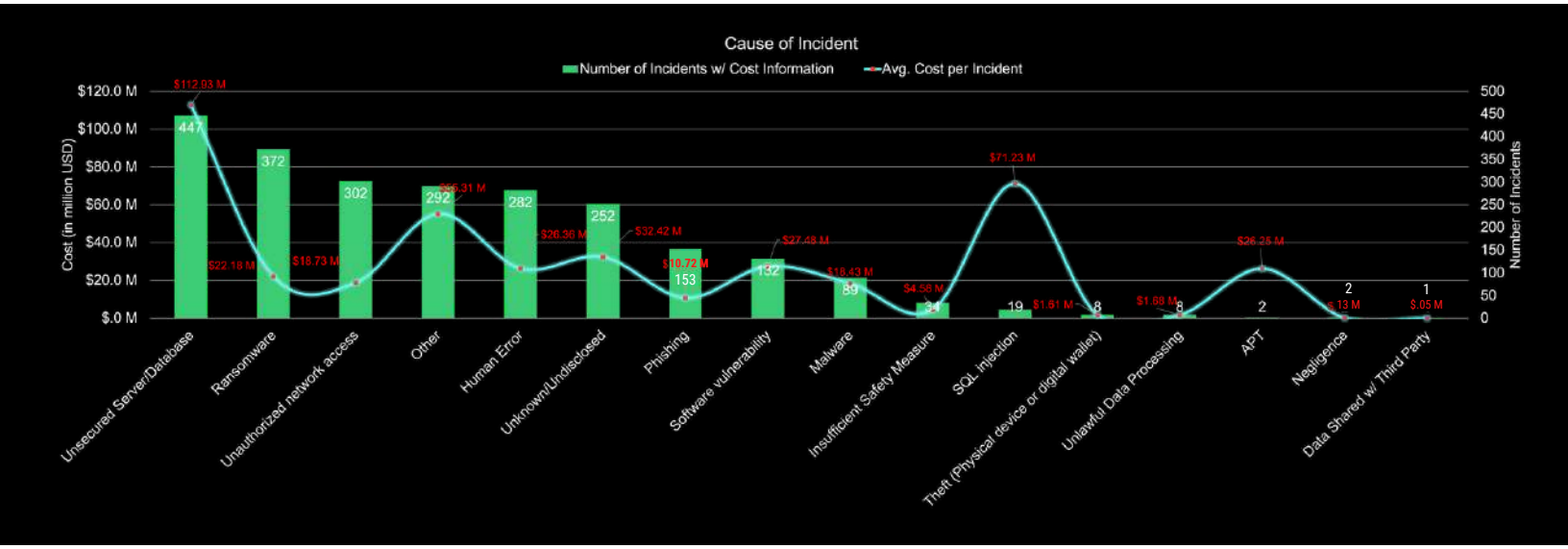
Financial impact is important, but typically overlooked are the people and process disruptions that may shake the confidence of local citizens or hurt the reputation of community business owners. With limited resources, smaller organizations may have to take a reactive approach instead of a proactive one, leaving them more vulnerable.

For example take Click2Gov, a software product designed to provide cities with interactive self-service bill-pay options for utilities, community development and finance. Reported breaches in 2017 and 2018 [4] appear to have come from patching issues in Oracle's WebLogic platform, a third-party of Click2Gov. Although patches were made, some organizations still chose to trust the platform, only to fall victim again in 2019. Six of the eight cities breached were compromised in the 2018 breach as well.

**For the cost per industry results, we remove the outliers in two categories, (1) Professional, Scientific, and Technical Services and (2) Information. These companies' incidents cost billions of dollars and therefore they were removed from the stats.

CAUSE OF INCIDENT

When analyzing the full cost of a data breach, it is imperative to dive into causation and costs related to particular attack methods used.



UNSECURED SERVERS AND DATABASES

The most frequent incident cause is **unsecured servers and databases,** accounting for **19% of all incidents,** with an average cost per incident of **$112.93 million.**

As one of the most frequent causes of these incidents, unsecured external facing assets, such as databases and servers, pose a major risk to companies. The risk grows much larger when a third party manages PII on behalf of a company or within a shared responsibility agreement.

Our studies confirm that the boundaries are blurred when a third party manages that data. In some cases, the companies who are served by the database/server vendor take the idea of security for granted, and do not monitor these vendors until it's too late.

RANSOMWARE

69% of CISOs expect to face at least one ransomware attack in 2022 [5].

The second most frequent incident cause is **ransomware**, which aligns with the exponential growth of ransomware in the last three years. In a Black Kite-sponsored report [5] that collected feedback from 250 CISOs in 2021, 53% claimed they were hit at least once by a ransomware attack last year, with 69% expecting to face at least one ransomware attack in 2022.

Ransomware accounted for **16% of incidents**, with an average cost per incident of **$22.18 million.** The incident frequency was similar to unsecured servers and databases, but the cost per event was significantly lower overall.

CAUSE OF INCIDENT CONT.

SQL INJECTION

One observation worth highlighting is the cause of SQL injection. While only accounting for 19 of more than 2,400 incidents, the average cost per incident was the second-highest, at **$71.23 million**. According to MalwareBytes, an SQL injection [6], or SQLI, is a type of attack vector where threat actors exploit software vulnerabilities in web applications in order to steal, delete, or modify sensitive company data. They may also gain administrative control over any system running the affected applications.

According to a report by the Ponemon Institute [7] on national retail organizations, concerns regarding SQL injection threats remain high, while action steps to mitigate that risk remain low. 65% of organizations represented had an SQL injection attack in the last year that successfully broke through any security defenses enacted.

In fact, 36% of respondents (IT and security professionals) within the study claimed that there was a 51-75% likelihood that recent attacks against national retail organizations involved SQL injection as an attack component. Furthermore, 52% of the Ponemon Institute report respondents do not take fundamental precautions, such as testing and validating third-party software, to ensure it is not vulnerable to SQL injection threats.

SQL INJECTION AWARENESS IN THE BLACK KITE PLATFORM

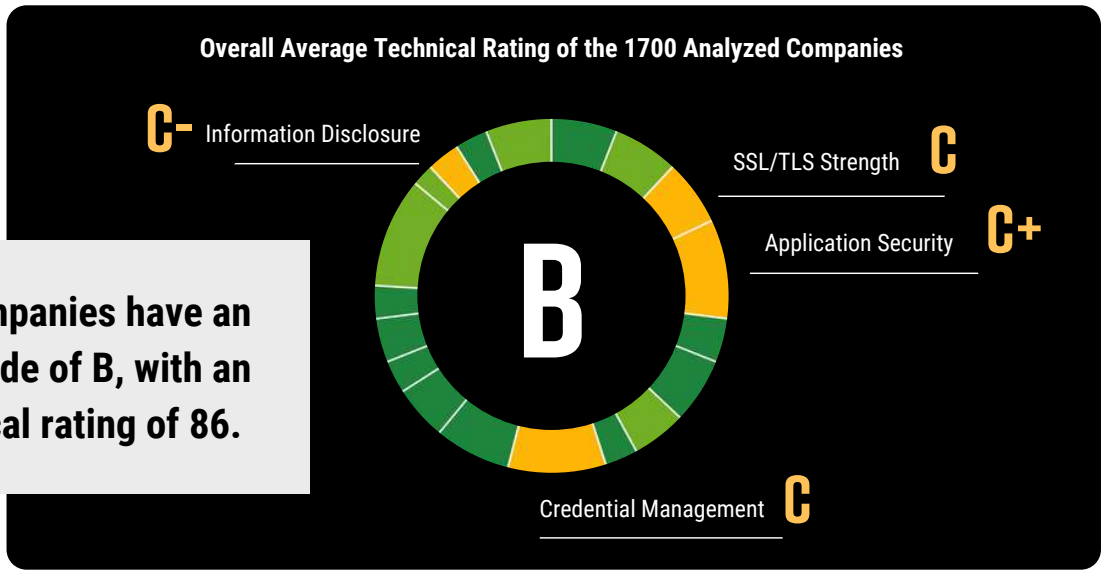
Black Kite's Technical Cyber Rating uses standard scoring models from MITRE's Common Weakness Scoring System (CWSS™) to prioritize software vulnerabilities. One of 20 technical categories, Application Security is one of the most heavily-weighted at 9% of the overall rating. Where vendors have application weaknesses or encryption issues, a list of findings with remediation recommendations is provided.

Common critical issues include:

- **APPSEC-013: SSL Certificate Invalid, Incorrect, Expired or Self-Signed** - SSL protocol ensures information travels safely across the internet and helps prevent adversaries from sniffing the network to steal information
- **APPSEC-014: Cleartext Transmission of Sensitive Information** - Some applications transmit passwords over an unencrypted connection, making them vulnerable to interception

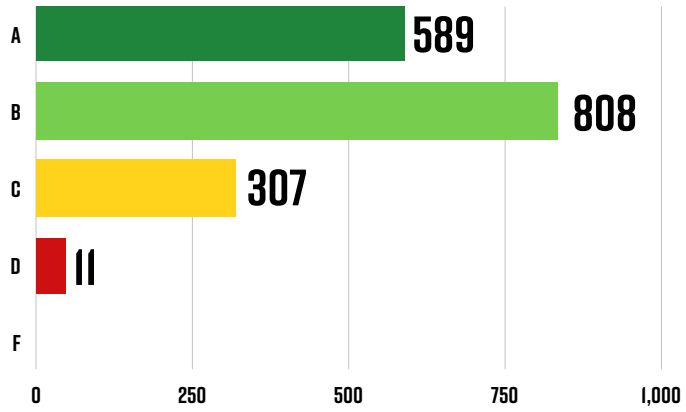
CYBER RISK POSTURE

1,700 of the 2,400 companies within the incident list analyzed still have active or known websites accessible with OSINT data. Black Kite Research scanned these 1,700 companies to provide an in-depth analysis of the current cyber security posture and ransomware susceptibility of these organizations. This section provides a look into the health and common vulnerabilities of companies hit by impactful cyber attacks in the last five years, allowing for additional insight and visibility.



Overall, the 1,700 companies have an average, or "Good" grade of B, with an average technical rating of 86.

ANALYZED COMPANIES' GRADE DISTRIBUTION



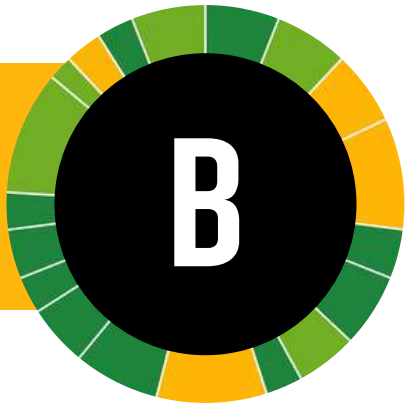
Black Kite follows and applies MITRE frameworks to determine the overall company rating, converting highly technical terms into simple letter grades. The cyber rating, an aggregation of open-source intelligence, provides a snapshot of the overall health of a company.

The total rating is a weighted average of 20 defined categories, providing unmatched breadth and insight into detected vulnerabilities. Each category, as well as each control point, has a different weight in the overall grade.

Black Kite has 290 control points with various weights corresponding to MITRE's TTPs, eliminating false positives. In this case, with a "B" rating, a company is 3x as likely to experience a data breach than a company that achieves an "A" rating.

BREAKDOWN OF TOP THREE CRITICAL ISSUES

1. CREDENTIAL MANAGEMENT: C
2. INFORMATION DISCLOSURE: C-
3. SSL/TLS STRENGTH: C



Credentials remain one of the most sought-after pieces of information for adversaries, with compromised passwords accounting for 63% of breaches in 2022 [8]. To combat this susceptibility, many organizations turn to protection measures like two-factor authentication. That way, if a credential is compromised, there is an extra layer of security between the attacker and their target.

Third-party companies may have their own password rules, but even the most sophisticated policies are not foolproof. It's imperative to monitor for third-party credential leaks on a continuous basis in order to identify and take action with that vendor right away.

Information Disclosure is a broad category of potentially serious vulnerabilities. Misconfigured services or other public assets may disclose local IPs, email addresses, version numbers, whois privacy records or other sensitive information on the internet. However, in some cases it may not be that obvious. Sometimes it is about what isn't disclosed.

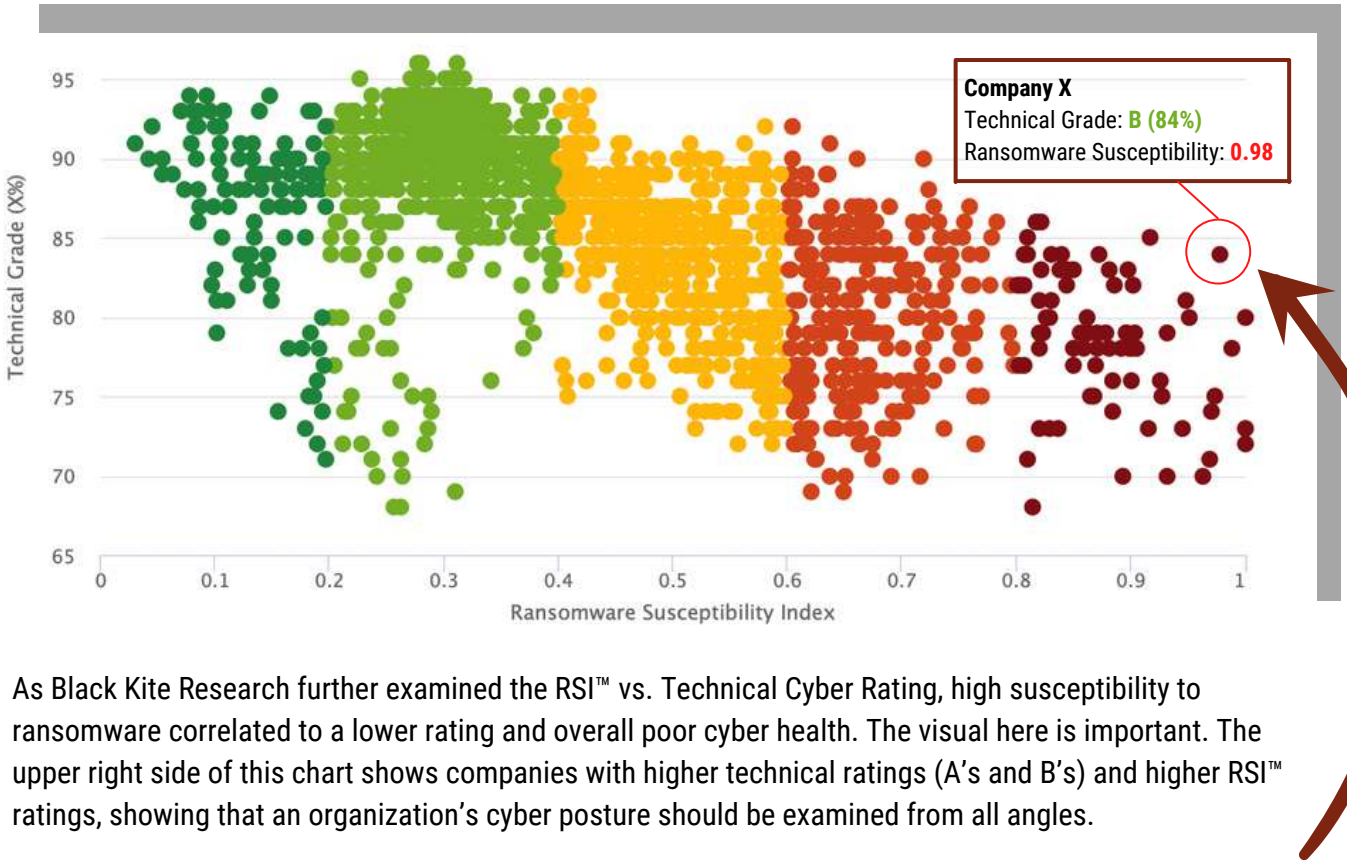
Common vulnerabilities discovered by Black Kite's non-intrusive scans often have to do with missing information in company privacy policies. For example, GDPR [9] grants individuals rights over their personal data. Subject to certain conditions, companies are required to facilitate these rights, i.e. the right to be informed, the right of access, the right to be forgotten, etc. and privacy policies must reflect specifics around data rights.

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.

RANSOMWARE SUSCEPTIBILITY INDEX™

Black Kite is the only cyber ratings platform that can identify ransomware susceptibility for a company in advance of an attack. The average Ransomware Susceptibility Index™ rating for the 1,700 analyzed breached companies reflects a **0.42** - mid-level risk index rating on a 0.0 to 1.0 scale of susceptibility.

However, **17% 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.

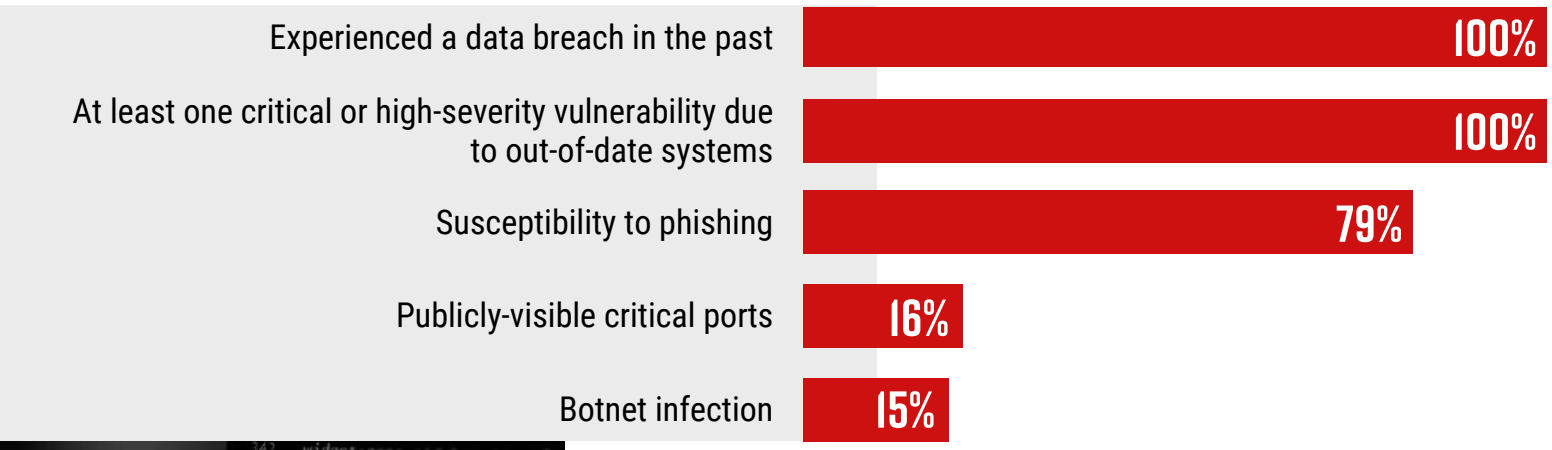


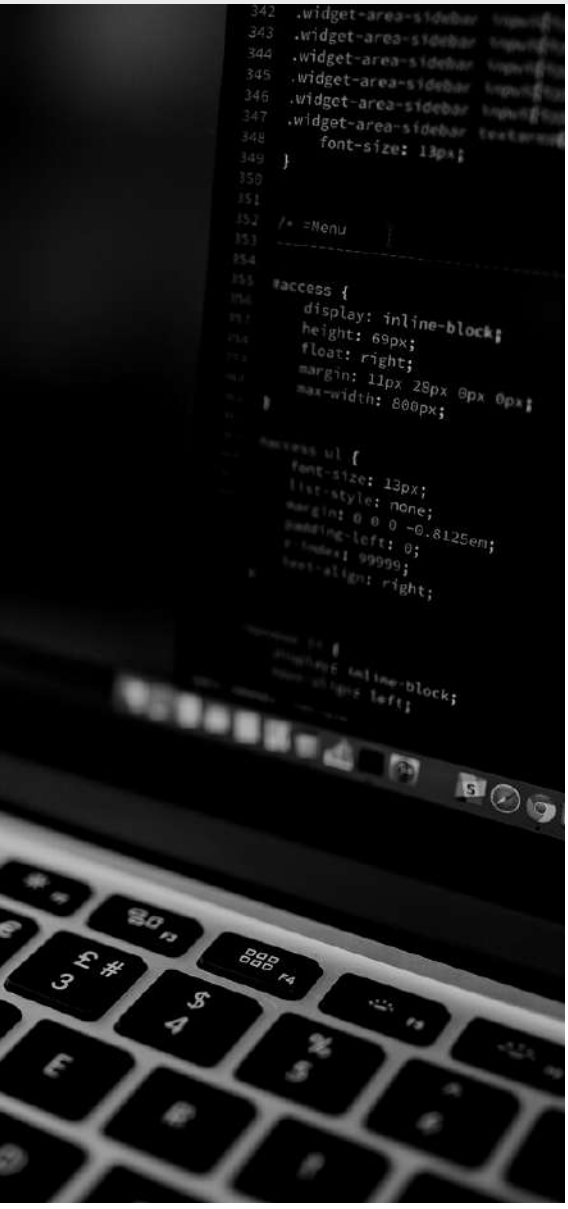
As Black Kite Research further examined the RSI™ vs. Technical Cyber Rating, high susceptibility to ransomware correlated to a lower rating and overall poor cyber health. The visual here is important. The upper right side of this chart shows companies with higher technical ratings (A's and B's) and higher RSI™ ratings, showing that an organization's cyber posture should be examined from all angles.

One company **highlighted in dark red has a 'B' rating, but an RSI™ rating of 0.98,** indicating almost *100% susceptibility to a ransomware attack.* Black Kite shows 28 ransomware findings for this company, 24 of which are noted as 'Critical' or 'High' by MITRE's CWSS standard.

Remember that all 1,700 of these companies have confirmed data breaches analyzed by Black Kite Research, so *companies with high RSI™ ratings must take note to reduce ransomware risk.*

RANSOMWARE POSTURE: CRITICAL ISSUES





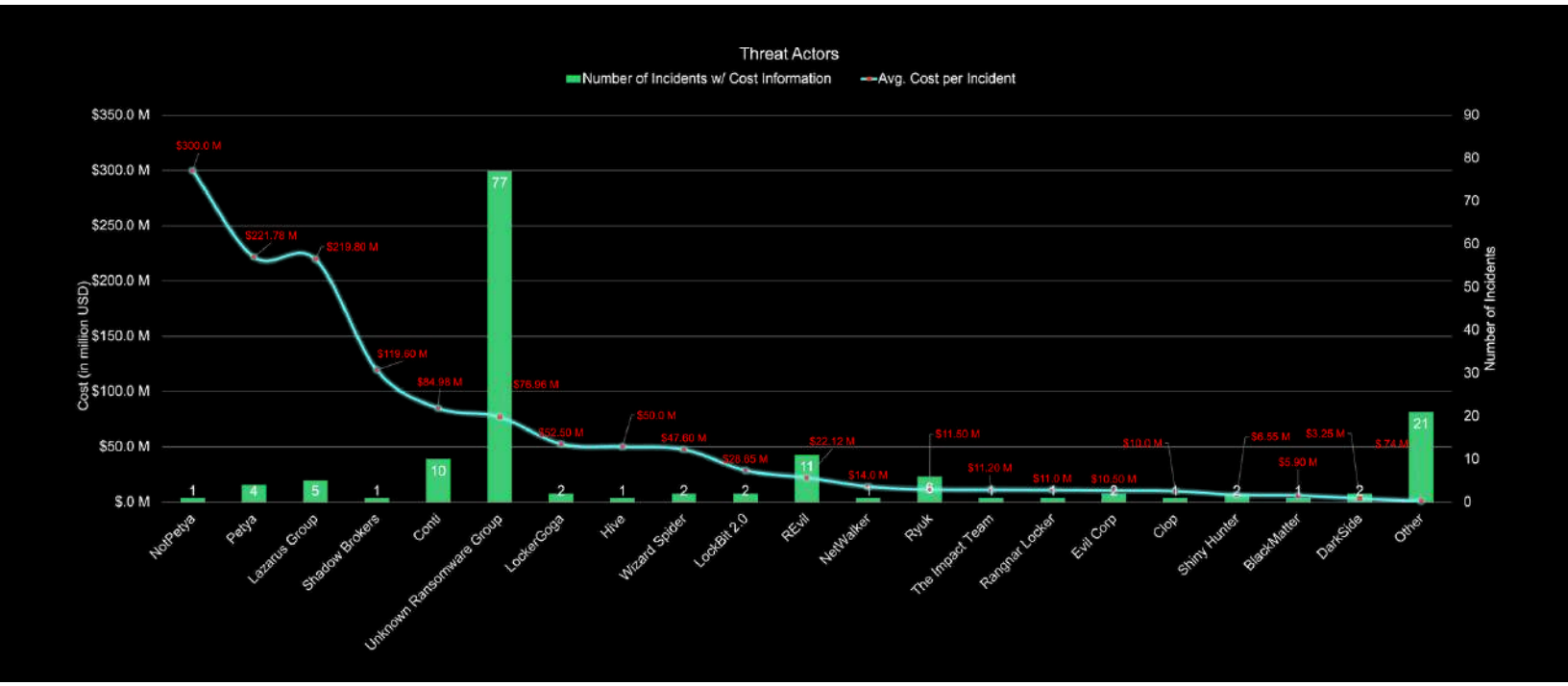
1. Unsurprisingly, **organizations that have experienced a data breach are more susceptible to future breaches, and more specifically, ransomware attacks.** Most organizations immediately jump to fix the vulnerability that caused the breach, but they often stop there. Once an adversary has found a vulnerability to exploit, they become more confident and may escalate to more severe attack methods.

2. Another alarming statistic is that **100% of the breached companies analyzed have at least one critical or high-severity vulnerability due to out of date systems.** When a software application no longer has updates to sustain it, it becomes outdated and unmaintained, leaving it open to more advanced cyber attacks. Organizations that rely heavily on an outdated application may find more reasons to keep using the software than to replace it or evaluate a new solution.

3. Software that allows remote administration is becoming more common as it becomes more difficult to physically be near a system to use it. Open ports are not dangerous by default, but **publicly-visible open critical ports** that are misconfigured, unpatched or have poor network security rules increase attack surface.

TOP THREAT ACTORS

Of the 2,400 incidents, Black Kite Research analyzed the top threat actors responsible for both the highest count of incidents, plus the highest average cost per incident. Setting aside the grouping of unknown ransomware groups, **REvil** registers as the most frequent threat actor, accounting for 11 incidents, with an average cost per incident of **$22.12 million**.



REvil is an advanced ransomware group that first appeared in April 2019, and is tied to headline attacks such as Colonial Pipeline. It operates through the RAAS (ransomware-as-a-service) model. In this model, after each attack, acquired revenue is split among the affiliates.

In early 2022, the Russian Federal Security Bureau's intelligence agency (FSB) seized 14 members of the long-sought REvil gang along with their stashes, halting operations. However, in recent months, REvil has re-emerged as active. According to Black Kite research, the often high-profile **REvil attacks accounted for 3% of the total ransomware attacks in 2021.**

The next most frequent threat actor was **Conti,** accounting for ten incidents with an **average cost per incident of $84.98 million,** nearly *4x the amount of REvil attacks.*

Conti is perhaps one of the most ruthless and greediest ransomware groups of all time, with its ransomware demands surging as high as $25 million. Its 2021 revenue reached as high as $180 million. Conti, most recently, has been active siding with Russia in the Russia-Ukraine conflict over the past several months.

Both Conti and REvil are known for their ransomware, or RaaS, attacks. 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 **Lazarus Group** was responsible for a much lower number of incidents, but the average cost per incident was significantly higher than the rest, coming in at **$220 million.** Lazarus Group has been active since 2009 and is based in North Korea.

EXPERT INSIGHTS

FERHAT DIKBIYIK, PH.D.

Head of Research, Black Kite

Research Perspective: Why is this research so important for the cybersecurity community?

I have been at Black Kite for four years and have been conducting research since day one. My exposure to external, survey-based data breach research has shown me:

- **We tend to only get information from the last 12 months, which doesn't consider implications that haven't happened yet**
- **Answers may be subjective and are hard to validate**

However, these survey-based reports provide valuable insight into the concerns that CISOs have and where opportunities for growth may exist. It's important to note that this research is still important. Before survey-based research, we didn't have any real insight into the full scope of recovery from a data breach or ransomware attack.

My team of 14 researchers worked tirelessly to collect this information over a period of 40 days. The one overarching qualitative finding is: *The true cost of a data breach is often not fully realized immediately following the event.* Even after a few months, the full scope of damage may not yet be understood. Companies have to deal with the consequences in the eye of regulators, courts, and civil society for years.

Threat actors know how tiresome and costly it is for their targets. With this knowledge, threat actors like ransomware groups have evolved their extortion methods. In the past, extortion was only based on "not providing the decryption key." Now, extortion has multiple folds, namely not providing encryption keys, leaking sensitive information, and even DDoS attacks.

Infamous ransomware groups such as Conti and REvil have invested money in their weaponry to gather more information about their targets and find valuable assets such as PII. Even if these groups dissolve, we will continue to see a higher cost impact in years to come from attacks that have already occurred in 2022.

EXPERT INSIGHTS

BOB MALEY

Chief Security Officer, Black Kite

CISO Perspective: Why is this research so important for the cybersecurity community?

Cost of a Data Breach reports have been around for 18 years now. During that time, there has been a lot of discussion about the actual usefulness of these reports. When I was the CISO for the Commonwealth of Pennsylvania, I used these reports to request a budget for new projects. They were simple per-record reports and they were valuable at the time because we had no other real instruction for Information Security. InfoSec was never looked at as an income-producing organization; It was always an expense. With cost per record information, you could translate that into future savings by the ability to prevent a breach. At that point, the use of fear, uncertainty and doubt was effective.

Over time, that usefulness has been questioned. Now we tend to see other helpful information in these reports, but overall they lack real insight into what causes a breach. Without concrete information, the reader isn't able to understand what resources they need to prevent a breach.

This report takes a different approach, looking at publicly-visible data on breaches from the last 5 years. My most interesting takeaway is that **17% of those 1700 companies are above the critical threshold of ransomware susceptibility.** It is pointedly clear that these companies are not looking at the basics of cyber hygiene the way bad actors do, so breaches are continuing to happen.

That is why it is so important that we **change our thought processes** and *get away from standard best practices.* We must become agile and look at cybersecurity using the same tactics, tools, and procedures the bad actors use. With this approach, you can stay left of bang, i.e. prepared and adaptable, more often.

RECAP & RECOMMENDATIONS

The word ‘cost’ has always been synonymous with a financial figure or an amount to be paid to obtain something. The actual cost of a data breach is significantly more than that; More than the damages reported in news stories or lost revenue on a financial statement.

Indirect costs associated with a breach may be even greater than monetary loss, especially considering the ripple effect when innocent partners or customers are involved. Compromised customer records drastically increase the cost of a breach, leading to lost future business and possible lawsuits. Though not as popular in the media, lost intellectual property or reputational damage can devastate a company’s growth potential.

LEARN FROM PREVIOUS BREACHES AND UNDERSTAND THE WARNING SIGNS

Over the last few years, Black Kite Research has studied third-party risk across various geographies, industries, and attack methods. More often than not, the same vulnerabilities run rampant and come down to basic cyber hygiene. Known credential leaks, missing software patches, expired SSL certificates - All seemingly simple issues to fix can be the keys to the kingdom for adversaries.

It is imperative to continuously monitor your vendors, suppliers and partners to understand their attack surface and how weaknesses in their security programs might hurt your organization.

IN THE EVENT OF A BREACH, DO YOU KNOW YOUR FINANCIAL IMPACT?

Communicating risk, let alone vendor risk, throughout your organization is challenging, especially when it comes to senior financial leaders. Instead of trying to predict your financial impact in the event of a vendor breach, use a tool that runs thousands of simulations to automatically determine your probable financial impact.

Black Kite’s risk quantification tool utilizes Open FAIR™ to forecast potential loss in financial terms to help your organization maintain an acceptable level of exposure. Take this financial risk modeling one step further by indicating whether a vendor has access to your internal systems and input the number of PII, PHI or PCI records you share with them.

REFERENCES

1. 2021 REPORT: CYBERWARFARE IN THE C-SUITE
2. Cost of a Data Breach Report 2022 | IBM
3. Forbes: Hackers Keep Hitting Financial Services Despite Hefty Cyber Spend
4. Eight US Cities Impacted in New Series of Click2Gov Breaches | SecurityWeek.Com
5. The CISOs Report: Perspectives, Challenges and Plans for 2022 and Beyond - Black Kite
6. What is SQL injection - Examples & prevention | Malwarebytes
7. The SQL Injection Threat & Recent Retail Breaches
8. DBIR Report 2022 - Results and Analysis - Not the Human Element | Verizon Business
9. GDPR

Regional Distribution of Analyzed Breaches

Europe	44.97%
North America	36.60%
Asia Pacific	15.54%
Middle East/Africa	1.55%
South America	1.34%

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.

CONTACT US

info@blackkite.com

+1 (571) 335-0222

800 Boylston Street, Suite 2905
Boston, MA 02199