



UNDERSTANDING THE TRUE MAGNITUDE OF A CYBER INCIDENT



INTRODUCTION

According to IBM, it takes companies an average of 197 days to identify a breach and an additional 69 days to contain it. Even so, containing a breach and fully recovering from it are two different journeys. It could take weeks, months, or even years to fully recover from a cyber attack.

While most people tend to view the "cost" of a cyber incident in terms of the immediate money or data lost, a cyber incident can impact your organization in a number of ways that have long-term (and costly) business impacts.

To better understand the risk cyber incidents pose to your organization, it's important to understand the true magnitude of damage they could bring to your company. By leveraging the FAIR model's six Forms of Loss (FOL), we can paint a more complete picture of how direct and indirect losses rack up the total monetary cost of a cyber incident in the long run.

WHAT IS A CYBER INCIDENT?

At their core, cyber incidents are, "Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein," according to NIST.

One of the most important things to acknowledge is that a cyber incident can look like a wide range of attacks. Some of the commonly-known forms of a cyber incident include:

- Malware.
- Phishing.
- Man-in-the-middle attacks.
- SQL injections.
- Ransomware attacks.

GETTING FAMILIAR WITH TODAY'S THREAT LANDSCAPE

If you want to get a leg up on bad actors, you need to understand the threat landscape and how it's constantly evolving. Here are some key facts on today's cyber incident landscape:

- Nearly 50% of all data breaches occur in the cloud.
- Over 90% of all cyber attacks start with phishing.
- Ransomware is one of the fastest growing attack vectors in cybersecurity, with ransomware causing almost 30% of all third-party breaches in 2023.
- Encryption-less ransomware is on the rise, emphasizing the importance of data protection and regulatory compliance.

IDENTIFYING CYBER RISKS AND INCIDENTS WITH THE CIA TRIAD

The CIA triad is a model that organizations can utilize to better understand whether a tool, vendor, or other asset might pose a risk for a cyber incident.

The CIA triad poses confidentiality, integrity, and availability as three important concepts an organization must protect to prevent a cyber incident. If any one of the three pillars is compromised, the company is at risk of a cyber incident.



The confidentiality pillar represents the measures required to prevent unauthorized actors from accessing sensitive information.

The integrity pillar represents how a solution or company maintains the consistency, accuracy, and trustworthiness of data over time.

The availability pillar represents the idea that for authorized actors, private information should be consistently and readily accessible at all times.

With the CIA triad for guidance, you can effectively identify the signs of a budding cyber incident. If your data's confidentiality, integrity, or availability is at risk, it's time to prepare your organization for a potential cyber attack.

THE CIA TRIAD IN THE REAL WORLD

Here's what each part of the CIA triad might look like when employed in real-life situations:

- *Confidentiality*: In an organization, only employees who are specifically authorized can access company HR records.
- *Compromised confidentiality*: A ransomware group gains access to a company's data through a breach, allowing them to see personal employee data and information.
- *Integrity*: An e-commerce website keeping track of every purchase ever made with a specific credit card.
- *Compromised integrity*: A threat actor breaches an e-commerce website and changes the prices of the products listed for sale, causing customers to falsely believe they can buy products at a heavily discounted price.
- *Availability*: An employee having 24/7 access to their work schedule through their company's online employee platform.
- *Compromised availability*: A threat actor breaches the company's IT system, causing the security team to shut the system down. Now, employees can't access their schedules and don't know when they need to work.

HOW TO MEASURE THE TRUE IMPACT OF A CYBER INCIDENT

One of the best ways to understand the true magnitude of a cyber incident is by assessing loss through the lens of the FAIR model. The FAIR model (provided by the FAIR Institute) is a valuable framework that helps companies better understand, analyze, and quantify cyber and operational risk in financial terms. In this way, companies can use the FAIR model to translate various types of losses due to a cyber incident (e.g., productivity, reputational, etc) into a dollar amount.

The FAIR model uses the concept of Loss Magnitude to help a business measure the “magnitude” of how much revenue it could lose in the event of a cyber incident. Loss Magnitude is calculated by adding up primary losses and secondary losses. The distinction between primary and secondary loss is a matter of who exactly causes the loss to the organization.

Primary loss is a loss caused by the incident itself. This includes how the victim responds to the loss event. Examples of primary loss include the immediate cost of an attack and the amount money a business spends to investigate a cyber incident.

Secondary loss is caused by the reactions of outside parties (current and past customers, employees, the government, etc.). A fine from federal regulators for not taking the proper security precautions to prevent an incident is an example of a secondary loss.

Perhaps the biggest benefit to using the FAIR model is that it translates both qualitative and quantitative impacts into financial terms. Communicating the impact of a cyber incident via monetary value is often an easier way for executive teams to digest and discuss cyber incidents.

FAIR'S SIX FOL

The FAIR model further divides primary and secondary loss into six FOL. These six FOL consider the initial (primary) and future (secondary) costs of a cyber incident. With FAIR's FOL, you can identify and quantify both the immediate and the long lasting (and often overlooked) costs of a cyber incident that could heavily impact your bottom line.

The FAIR model's six FOL:

- Primary Loss:
 - Productivity.
 - Response.
 - Replacement.

- Secondary Loss
 - Competitive advantage.
 - Fines and judgements.
 - Reputation.

PRODUCTIVITY

Productivity loss is any loss caused by the inability to execute business operations that hinders the production of a product or the delivery of a service.

Example: A ransomware attack shuts down manufacturing operations for a major retailer. Productivity loss would total up the total cost of products the company could not produce (and therefore lost out on) while shut down.

RESPONSE

Response loss is any loss related to the cost or activities of managing and responding to a cyber incident.

Example: A ransomware group breaches an organization's customer data. Response loss would represent the costs of employing a public relations team to alert both customers and the media of the data breach.

REPLACEMENT

Replacement loss is any loss caused by replacing capital assets (employees, products, software, etc.).

Example: If a data breach is caused by an employee's negligence, the business must fire said employee and spend money and dedicate time to replace them. This can include:

- Recruit talent for interviews.
- Hold said interviews.
- Hire the new employee.
- Guide them through the onboarding process.
- Train them for their specific role.

COMPETITIVE ADVANTAGE

Competitive advantage loss is any loss brought on by damaged or compromised intellectual property or other competitive differentiators.

Example: A threat actor gains access to a company's private data, finds and steals the blueprints for a brand new product, and sells it to a competing company. Now, the competing company can use the blueprints as inspiration for its next product. The victim must then choose between scrapping the new product and losing money, or releasing the product and potentially being branded as a copycat.

FINES AND JUDGEMENTS

Fine and judgment loss is any loss from legal claims or judgments levied against a business through civil, criminal, or contractual actions.

Example: A company falls victim to a data breach because of subpar security practices, and fails to publicly disclose it. As a result, the company is fined by the local government and is sued by customers.

REPUTATION

Reputation loss is any loss from damaged customer trust and external stakeholder perspectives.

Example: A company suffers a huge data breach and its customers' private data falls into the hands of a threat actor. Now, customers and stakeholders no longer think the victim company is trustworthy enough to conduct business with, as it didn't take the proper precautions to prevent this kind of attack and protect their private data and information.

YAHOO LOSES \$350 MILLION AFTER REPUTATIONAL DAMAGE

- Back in 2013, Yahoo fell victim to a cyber attack that went on to affect all three billion users.
- Verizon originally planned to buy Yahoo for \$4.83 billion.
- Once the breach was disclosed to the public in 2016, the deal was delayed to further assess any damages that could stem from said attack.
- In the end, to make up for the reputational damage caused from the attack, Yahoo agreed to lower its asking price to \$4.48 billion (a \$350 million decrease).

THE CURSE OF SECONDARY LOSS

Primary loss is easy to see and quantify, but secondary loss is harder to track. Between primary and secondary loss, secondary losses are the true danger — as they often result in costs and damages that accrue over time (even long after the attack is seemingly over).

If a company falls victim to a cyber incident, it's imperative that the cybersecurity and leadership teams take a long-term view of how said incident could impact the entire business. This might look like creating a cost estimate for each secondary FOL category over the next several weeks, months, or years to fully account for potential secondary losses and avoid any surprises.

SECONDARY LOSS IN THE REAL WORLD

To help illustrate how pervasive secondary loss can be, here are some recent real-world examples.

Equifax

In 2017, an unpatched framework in one of [Equifax's](#) databases caused the loss of personal and financial information of almost 150 million people. Not only did Equifax fail to fix a critical vulnerability months after a patch had been issued, but the business also waited to inform the public of the breach for weeks after its discovery.

In 2019, this breach and negligence brought on a \$575 million fine from the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and the U.S. federal government. As a result, Equifax must now keep an eye out for any additional lawsuits or fines that could stem from this incident — such as the additional \$45 million in settlements Equifax had to pay in 2020 for the same incident.

T-Mobile

In 2022, [T-Mobile](#) was hit with a class action lawsuit regarding a data breach in 2021. Impacting 77 million people, the cyber incident was caused by a threat actor gaining “unauthorized access” to T-Mobile's systems. The theft was discovered when customer data was listed for sale on a cybercriminal forum.

In addition to the \$350 million T-Mobile paid in class member legal fees, the company also agreed to incrementally spend \$150 million to improve its data security practices from 2022 to 2023. In the end, because of a data breach in 2021, T-Mobile had to pay \$500 million over the course of two short years.

Capital One

In 2019, [Capital One](#) fell victim to a data breach that affected over 100 million people. The very next year, the U.S. The Office of the Comptroller of the Currency fined the company \$80 million over the breach. Then in 2021, Capital One agreed to pay \$190 million in settlements from a class-action lawsuit regarding the breach (two years after the breach occurred).

HOW TO MITIGATE ALL TYPES OF LOSS

When most people think about the costs of a cyber incident, they think about primary loss. However, cyber incidents can cause ripple effects that impact your organization for years to come. By following the FAIR model, you can see the full financial impact a cyber incident poses to your organization – including those sneaky secondary losses – to make better business decisions.

For third-party risk management (TPRM) specifically, Black Kite provides the high-level context necessary to make smarter business decisions that will keep your organization safe from a potential third-party vendor attack that could incur secondary loss for years to come.

To further strengthen your secondary loss prevention, Black Kite continuously implements three FAIR scenarios (Data Breach, Ransomware, and Business Interruption) into our cyber risk quantification (CRQ) solution.

HOW BLACK KITE USES FAIR SCENARIOS

Black Kite provides a complete picture of third-party cyber risk through our technical cyber rating, compliance correlation, and cyber risk quantification (CRQ) solutions. Black Kite leverages the Open FAIR™ model in our CRQ solution to ensure you get the most accurate probable financial impact based on the cyber incident scenarios you need to prepare for.

Data Breach

Black Kite's Data Breach scenario assesses and mitigates the risks associated with data breaches (reputational damage, non-compliance fines, intellectual property theft, etc.) by analyzing a vendor's:

- Security controls
- Compliance results
- Industry-specific threat data

Ransomware

Black Kite's Ransomware scenario assesses the likelihood of a ransomware attack and helps to identify areas of vulnerability through analyzing a vendor's:

- Security controls
- Emerging attack vectors
- Previous ransomware incidents

Business Interruption

Black Kite's Business Interruption scenario highlights areas to improve and ensure business continuity by assessing:

- How environmental factors such as earthquakes, floods, and pandemics can disrupt business operations
- Supply chain risk that could lead to disruptions in the supply of goods and services
- Geopolitical risks, such as riots or protests

Additionally, Black Kite's CRQ solution puts the cyber risk a third-party vendor poses to your organization (should they experience a security incident) in financial terms. With these FAIR scenarios and Black Kite's CRQ solution, your security teams can assess nearly all third-party cyber risk use cases to prepare for any secondary losses said risks could incur.

ABOUT BLACK KITE




Our deep insights help you ease the stress of cyber ecosystem risk management. We do this by giving you more than a risk score. Our automated system provides real-time and accurate risk intelligence. Our data is accurate, reliable and detailed so you can improve business resilience by making informed risk decisions across your entire ever-changing cyber ecosystem.


With Black Kite you get More than a Score™.


**EXPERIENCE THE BLACK KITE PLATFORM
YOURSELF WITH A FREE CYBER ASSESSMENT**



CONTACT US

 info@blackkite.com

 +1 (571) 335-0222

 800 Boylston St. Suite 2905
Boston, MA 02199