A FAIR Taxonomy for Cyber Risk Scenarios

An Analyst's Guide for Defining Risk Scenarios for Continuous Risk Management

February 25, 2025

Authors:

Pankaj Goyal
Director, Standards & Research
FAIR Institute
Pankaj@FAIRInstitute.org

Cody Scott
Senior Industry Analyst, Security & Risk
Forrester
cscott@forrester.com

Todd Tucker
Managing Director
FAIR Institute
TTucker@FAIRInstitute.org

Table of Contents

Executive Summary

Effective cyber risk management begins with well-defined risk scenarios. Organizations that clearly articulate their risk scenarios can make informed decisions, strategically allocate resources, and strengthen their overall security posture. However, many governance, risk, and compliance (GRC) programs struggle with risk registers that contain vague, irrelevant, or poorly quantified scenarios, leading to ineffective risk prioritization and misaligned security investments.

This guide provides a structured approach to defining and refining cyber risk scenarios, ensuring that they accurately represent probable loss events. By leveraging a standardized risk scenario taxonomy, organizations can enhance decision-making, improve communication, and optimize resource allocation. Additionally, this guide addresses common pitfalls in risk scenario development and offers practical strategies for improving the quality and actionability of risk registers.

With a clear understanding of cyber risk scenarios, organizations can transition from generic risk concerns to quantifiable, business-aligned risk management practices that drive better security outcomes.

Introduction

Risk scenarios are the cornerstone of a well-structured cyber risk management program. Clearly defined risk scenarios empower organizations to make informed decisions, strategically allocate resources, and enhance their overall risk posture. Conversely, vague, inaccurate, or irrelevant risk scenarios can lead to flawed decision-making, wasted resources, and misaligned priorities.

Many GRC (Governance, Risk, and Compliance) and Cyber Risk Management teams dedicate substantial effort to developing enterprise risk registers. However, these registers often exhibit fundamental flaws, including:

- **Incorrectly Defined Risk Scenarios**: These scenarios lack specificity and fail to reflect real-world situations, hindering their applicability to actual risk assessments.
- **Irrelevant Risk Scenarios**: These scenarios focus on hypothetical or low-impact risks, diverting attention from more critical threats and potential losses.
- **Excessive Number of Risk Scenarios**: Overloading the risk register with too many scenarios creates unnecessary complexity and impedes actionable insights.
- **Poorly Measured Risk Scenarios**: These scenarios lack effective quantification of potential impact and likelihood, making it difficult to prioritize risks and allocate resources appropriately.

This guide aims to assist practitioners and leaders in accurately defining risk scenarios and constructing a structured, actionable risk register. It will introduce a taxonomy of risk scenarios to serve as a practical reference.

The guide will also address common misconceptions about risk scenarios, helping teams refine and clean up existing risk registers by identifying and eliminating elements that do not constitute true risk scenarios.

Key benefits of well-defined risk scenarios include:

- **Informed Decision-Making**: Clear risk scenarios enable organizations to make data-driven decisions regarding resource allocation, security investments, and risk mitigation strategies.
- **Strategic Resource Allocation**: By understanding the potential impact and likelihood of various risks, organizations can allocate resources effectively to address the most critical threats.

- **Enhanced Risk Posture**: Well-defined risk scenarios facilitate proactive risk management, enabling organizations to identify and address vulnerabilities before they are exploited.
- **Improved Communication**: A clear and structured risk register fosters better communication and collaboration among stakeholders, ensuring everyone understands the organization's risk landscape.

By addressing the common pitfalls in risk scenario development and providing a structured approach, this guide aims to empower organizations to build robust risk registers that support effective cyber risk management.

What Is a Cyber Risk Scenario?

The risk scenario is the starting point of an analysis. Think of it as a problem that needs to be analyzed and solved. A risk scenario describes a time-bound, probable loss event and specifies the threat actor and method, the asset at risk, and the effect or consequence that may occur during that time.

Risk assessment prepares you to answer three questions:

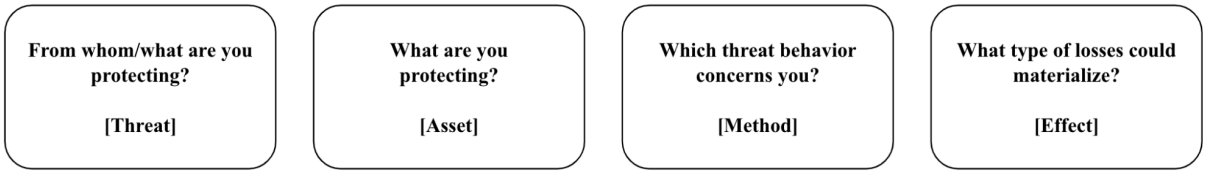
1. What can go wrong? (i.e., the scenario conditions causing concern)
2. How often will it occur? (i.e., the loss event frequency of the scenario)
3. How much do we stand to lose? (i.e., the loss event magnitude if that scenario occurs)

Defining the risk scenario is the first step to answering these questions, and how well you set up the first question determines how well you can answer questions two and three. In other words, the less clearly defined the scenario is, the less “solvable” or useful your answer will be.

Scoping a risk scenario is the act of translating real-world concerns or situations into probable loss events. A risk scenario contains 4 key elements (Figure 1):

1. **Threat**: anything capable of acting against an asset in a manner that can result in loss
2. **Asset**: anything of value that can be affected in a manner that results in loss
3. **Method**: a specific attack vector used to access or affect the asset
4. **Effect**: how a business loss is expected to materialize with a given asset (expressed in terms of how asset confidentiality, integrity, and availability impacts generate loss)

Figure 1: The FAIR Cyber Risk Scenario Model



A scenario can be described as a risk statement using these factors:

"[Threat] impacts [asset] via [method], causing [effect(s)]."

Consider the following example:

"Nation-state threat actor impacts sensitive patient records via a ransomware attack with data exfiltration, causing an information privacy loss (confidentiality)."

Properly defining and scoping a risk scenario also serves as a means test to validate that the scenario or scenarios are the most relevant, plausible, and probable. For example, we may be concerned about threat actors compromising user accounts via a phishing attack, but what is the risk? Or, to frame it differently, what is *at risk*? Why are we concerned about phishing attacks (e.g., user training shows higher fail rates, new APT group announced, etc.)? What do the user accounts have access to? What controls exist already to deter or prevent this from happening? If you can translate the generic "phishing attack" concern into 4 components of a risk scenario, then you can assess its risk to the business. Otherwise, you're just debating a vague concern.

The purpose of scenario scoping is to hone in on what matters most. When getting started, it's common for practitioners to feel obligated to model and quantify every possible impact to the n^{th} degree in order to be as "accurate" as possible. But this is a mistake. The goal is not to model every possible scenario in which phishing attacks could lead to loss. Instead, it is to identify the most relevant threat, method, asset, and effects that represent the most probable ways in which your organization could be materially impacted *in order to* make decisions. The four components of a risk scenario give the practitioner substantial flexibility to achieve this.

For example, in the phishing scenario above, perhaps the security team is primarily concerned with threat communities and wishes to create multiple scenarios to reflect different threat actors to see how relatively susceptible they are to compromise. In this case, the Threat component will be more granular in the scenario scope to quantify each threat actor's relative capability to overcome an asset, while the remaining three scenario components may remain the same.

On the other hand, if the security team is less concerned about individual threat actors and more about different business assets that could be impacted, they may use data about general threat event frequencies reflecting a wider range and instead focus on different asset groups and forms

of loss. The risk scenarios' four components help you determine where to focus, and what data you'll need to accomplish the analysis.

Comparing Ineffective to Effective Risk Scenario Definitions

Most risk statements today are not written as a scenario, leading to generally poor-quality risk registers. Risk statements tend to have generic titles, such as "network intrusion," "lack of enforced MFA credentials on user accounts," or "inability to detect large file transfers." In practice, a risk statement usually reflects a control failure, an audit finding, or a new vulnerability or misconfiguration that needs to be addressed. As such, they are missing elements (e.g., threat, loss) that are essential to assessing risk.

This summary format isn't necessarily a problem, but none of these are risks on their own. These statements lack essential context about what can go wrong. Consider the following examples, compared to more effective statements:

Ineffective Risk Statement	Effective Risk Scenario
"Phishing is a big risk to our organization."	"Cybercriminals impact **company funds (cash and cash equivalents)** via **a phishing-based business email compromise (account takeover),** causing **a direct financial loss (financial fraud).**"
"Data breaches are a major concern."	"A **disgruntled employee (privileged insider)** impacts **proprietary research and trade secrets (intellectual property)** via **unauthorized file transfers (data exfiltration without ransomware),** causing **a competitive disadvantage and loss of future revenue (proprietary data loss).**"
"We might get hit by ransomware."	"A **ransomware gang (cyber criminals)** impacts **customer billing and payment processing (business process generating revenue)** via **encryption malware and extortion (ransomware with data exfiltration),** causing **service downtime and ransom payment demands (business interruption and cyber extortion).**"

Ineffective Risk Statement	Effective Risk Scenario
"Weak passwords could lead to account compromise."	"A **hacker using automated tools (script kiddies)** impacts **executive email archives (confidential business information)** via **brute-force login attempts (credential-based attack),** causing **exposure of sensitive company strategy (information privacy loss).**"
"Third-party vendors introduce cybersecurity risks."	"A **nation-state-backed espionage group (nation-state actors)** impacts **a cloud-based supplier management platform (business process impacting third-party revenue)** via **malicious software updates (supply chain attack),** causing **disruptions in production and exposure of supplier contracts (business interruption and proprietary data loss).**"

Taxonomy of a Cyber Risk Scenario

When creating a **cyber risk scenario**, it is essential to precisely define its components. Minor distinctions—such as using *"cybercriminals"* versus *"cyber threat actor"*—can significantly improve clarity, ensuring stakeholders understand the risk accurately and can take targeted mitigation actions.

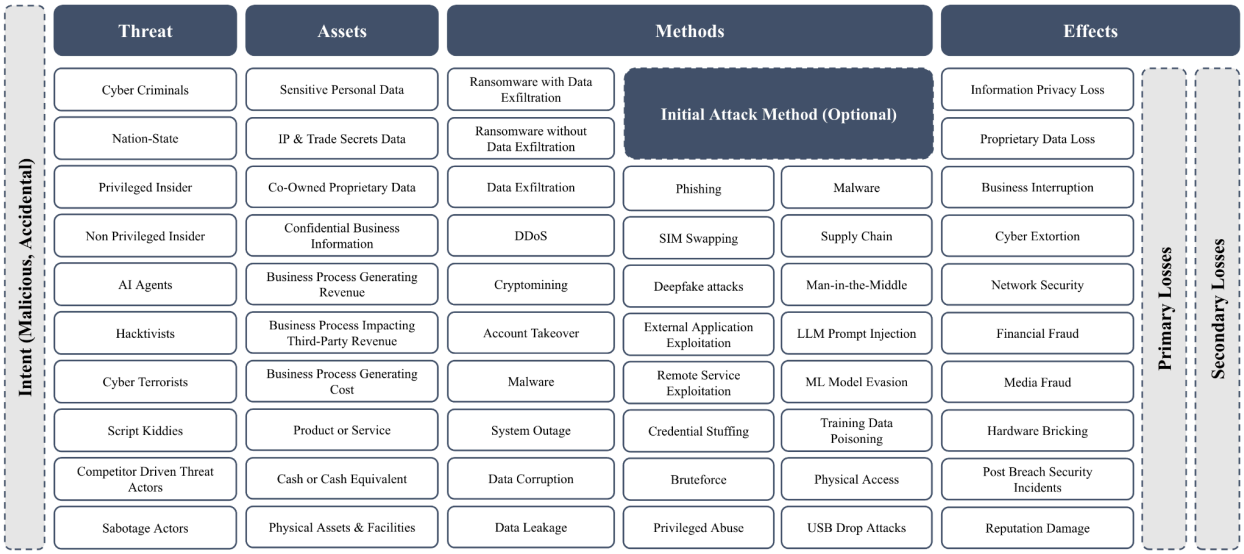
Below, we introduce a **taxonomy for creating cyber risk scenarios** to help practitioners develop **well-defined, actionable, and easily understood** scenarios.

Please keep the following in mind:

- Our focus is on cyber risk scenarios, though FAIR may also address operational risks related to technology systems, such as system outages.
- This is not a comprehensive taxonomy—it is our first iteration, and we welcome feedback from the risk community to refine and enhance it further. There is likely a "long tail" of threats, assets, methods, and effects that are not captured here, and we wish to include the most prominent ones.
- This should serve as a starting point for your organization. As you mature, you will likely expand upon this taxonomy.

- A common dilemma is how much precision is enough. A "cyber threat actor" is often too imprecise, while "APT X" is often too precise. The answer may depend upon the maturity of your risk program. If you have a very highly mature risk program with stakeholders' buy-in, then you can increase the level of precision in creating risk scenarios. Our taxonomy has been built for an organization with maturing risk programs.

Figure 2: The FAIR Cyber Risk Scenario Taxonomy



Threat

A *threat*, or *threat actor*, is anything or anyone capable of acting against an asset in a manner that can result in loss. The term *threat* is normally applied to all types, including non-human threats such as natural disasters; *threat actor* generally refers to humans, whereby intent is a consideration. In this guide, we'll limit the taxonomy to common *threat actor* types.

Threat Actor Types

The taxonomy defines the following ten (10) types of threat actors.

1. Cybercriminals

Cybercriminals are financially motivated individuals or groups that exploit vulnerabilities for profit, often using ransomware, phishing, or fraud schemes. They may operate independently or as part of organized crime syndicates.

Examples:

- LockBit – A notorious ransomware gang that extorts businesses by encrypting their data.

- FIN7 – A financially motivated hacking group known for targeting financial institutions and retailers.

2. Nation-State Actors

Nation-state actors are government-backed cyber operatives conducting cyber espionage, cyber warfare, or disruption campaigns to further political, economic, or military objectives.

Examples:

- APT29 (Cozy Bear) – A Russian state-sponsored group linked to cyber espionage against governments and critical infrastructure.
- APT41 – A Chinese-linked hacking group known for both espionage and financially motivated attacks.
- North Korea's Lazarus Group – A state-sponsored group involved in cyber theft and espionage, responsible for the Sony hack and WannaCry ransomware.

3. Privileged Insiders

Employees or contractors with elevated system access who misuse their privileges for financial gain, sabotage, or espionage. These individuals can cause significant damage as they already have access to sensitive systems.

Examples:

- Edward Snowden (NSA leaks) – A former NSA contractor who leaked classified intelligence documents.
- Tesla Insider Sabotage (2020) – A former employee who allegedly modified source code and stole proprietary data.

4. Non-Privileged Insiders

Employees, contractors, or third-party vendors with limited access who inadvertently or intentionally contribute to security breaches. Unlike privileged insiders, they typically have restricted access but may still cause harm through negligence or social engineering attacks.

Examples:

- Twitter 2020 Hack – Employees were manipulated via social engineering, allowing attackers to take over high-profile accounts.
- Marriott Data Breach – A third-party contractor's compromised credentials led to the exposure of millions of customer records.

5. AI Agents

Autonomous or semi-autonomous AI-driven systems that can be used maliciously to conduct cyberattacks, automate exploitation, or manipulate digital environments. These may be controlled by human operators or operate independently within set parameters.

Examples:

- AI-powered phishing bots – Malicious AI systems that generate realistic spear-phishing emails with deepfake voices.
- Autonomous malware – AI-enhanced malware that adapts in real-time to evade detection.
- Adversarial AI attacks – AI systems that manipulate machine learning models (e.g., fooling facial recognition systems).

6. Hacktivists

Hacktivists are politically or ideologically motivated cyber actors who conduct cyberattacks to promote a cause, expose perceived injustices, or disrupt organizations they oppose. They typically engage in website defacements, DDoS attacks, and data leaks.

Examples:

- Anonymous – A loosely affiliated hacktivist group known for targeting governments and corporations.
- LulzSec – A group that carried out high-profile attacks on government agencies and businesses.
- Killnet – A pro-Russian hacktivist group conducting DDoS attacks on Western institutions.

7. Cyber Terrorists

Cyber terrorists use cyber capabilities to cause fear, disruption, or physical harm in support of terrorist objectives. Their attacks may include disrupting critical infrastructure, spreading propaganda, or stealing sensitive information.

Examples:

- ISIS-affiliated cyber groups – Known for doxxing military personnel and spreading propaganda.
- DarkSide (Colonial Pipeline attack) – Although financially motivated, their attack had broad implications for critical infrastructure.

8. Script Kiddies

Inexperienced, amateur hackers who use pre-made hacking tools and scripts to launch attacks with little technical expertise. They often seek notoriety or engage in cyberattacks for fun rather than strategic purposes.

Examples:

- Teen hacker behind the 2022 Uber breach – Used stolen credentials and social engineering to gain access.
- Low-skill ransomware attacks – Many use readily available ransomware-as-a-service (RaaS) tools.

9. Competitor-Driven Threat Actors (Corporate Espionage)

Companies or hired cyber mercenaries conducting cyber espionage to steal intellectual property, trade secrets, or disrupt competitors. These actors operate in the shadows and may be tied to nation-states or independent groups.

Examples:

- Operation Night Dragon – A cyber espionage campaign targeting energy companies.
- Hacking of pharmaceutical companies – Nation-states and competitors targeting vaccine research.

10. Disgruntled Employees (Saboteurs)

Employees who intentionally harm an organization due to personal grievances, revenge, or dissatisfaction. They may delete critical data, sabotage systems, or leak sensitive information.

Examples:

- Cisco employee deleting virtual machines (2020) – A former engineer deleted over 16,000 WebEx accounts, causing business disruption.
- Tesla insider threat case (2020) – A disgruntled employee attempted to sabotage manufacturing systems.

Intent of a Threat Actor

When you are defining a threat actor, you should capture the potential intent of the threat actor clearly. Intent can impact the losses significantly on both primary and secondary losses. As an example, a malicious privileged insider might try to send out your confidential IP to competitors resulting in significant loss of future revenue to the organization. On the other hand, an accidental leakage from a privileged insider might not reach a competitor.

We identify two types of intent:

- **Malicious**: the threat actor acts purposefully to inflict harm
- **Accidental**: the threat actor unwittingly acts to cause harm

Note that some scenarios might involve both malicious and accidental threat actors. For example, a phishing attack executed by a cybercriminal (malicious actor) might result in a privileged insider (accidental actor) granting privileges to the cybercriminal. In this scenario, it's best to focus on the malicious actor as the threat and consider the accidental actor as part of the attack method.

Asset

An *asset* is anything of meaningful business value that can be affected in a manner that results in loss. This financial loss can be realized immediately, in the short term (in less than one year), or over longer periods of time.

For our purposes, an asset may or may not be reflected on the balance sheet of the business. For example, brand value is rarely reflected on a balance sheet, except after an acquisition, where it is recorded as a component of goodwill. For another example, business data that has been captured and managed by the business is rarely reflected on the books. Even when an asset is recorded in a firm's asset register, its net book value rarely reflects the true value to the business.

Also, many traditional IT assets, such as physical servers, network hardware, and storage equipment, are rarely specified as assets when defining a cyber risk scenario. They certainly may be part of a scenario asset as they can be useful for understanding the impact of controls and vulnerabilities, but when used alone, they often fail to describe business value sufficiently.

Asset Types

The taxonomy defines the following five (5) types of assets across 10 categories.

1. Data

Data is one of the most valuable assets of any organization. A data breach, theft, or loss can lead to significant financial and reputational damage, even when the business services that rely on the data are unaffected. The types of losses include:

- Regulatory fines (e.g., GDPR, CCPA penalties)
- Litigation and legal costs
- Criminal prosecution of corporate officers and directors
- Customer loss due to reputational damage
- Loss of intellectual property (IP), impacting future revenue
- Operational disruptions and recovery costs

Within the data type of assets, we define four categories:

- Sensitive Personal Data: customer records, employee PII, health data (e.g., HIPAA data).
- Intellectual Property (IP) and Trade Secrets: proprietary algorithms, patents, R&D, and AI-generated datasets (e.g., vector databases, synthetic data repositories, AI-driven knowledge graphs)
- Co-owned Proprietary Data: jointly held data in partnerships or M&A deals
- Confidential Business Information: financial reports, M&A plans, future strategy

2. Business Process

A business process is a structured series of activities or tasks that an organization performs to achieve a specific business goal or outcome. These processes typically involve people, technology, data, and workflows and are designed to produce consistent and repeatable results. A cyber incident affecting business processes can lead to revenue loss, operational downtime, and increased costs.

Within the business process type of assets, we define three categories:

- Business Process Generating Revenue: payment systems, order fulfillment, service delivery, and others
- Business Process Impacting Third-Party Revenue: supply chain operations, product fulfillment, and others
- Business Process Generating Cost: financial operations, procurement, payroll, and others

As such, they may cause the following types of losses:

- Permanent revenue loss or delayed revenue realization
- Legal damages awarded to third parties for impacts on their operations and increased legal costs
- Increased costs and lost productivity for impaired business operations

3. Product or Service

Product or service includes the items and/or services that customers purchase, lease, or subscribe from your business. For a software company, this would include on-premise software or software-as-a-service delivered to customers. For an automotive company, this would include the vehicles sold or leased to customers. Products may be digital, physical, or a combination of both.

The types of losses here may include:

- Permanent or temporary impairment of brand reputation

- Legal damages awarded to customers for the harms they suffer and increased legal costs for responding to lawsuits
- Permanent revenue loss or delayed revenue realization
- Increased costs to satisfy product recalls or otherwise rectify damages

4. Cash and Cash Equivalents

Cash and cash equivalents include the monetary assets held by your business physically or digitally. They include cash of any currency and other transferable instruments such as stocks, bonds, cryptocurrency, gift card balances, and more. They include assets that are owned by your business and those belonging to others that are in your custody (e.g., deposit accounts of your clients) or for which you owe a duty of care.

Direct financial losses from cyber incidents can be immediate and severe, particularly in attacks targeting financial assets. These include:

- Bank accounts and cash reserves: targeted via fraud, wire transfer scams, or account takeovers
- Securities and investment portfolios: cyber manipulation of trading systems
- Cryptocurrency and digital assets: theft of digital wallets, unauthorized crypto transactions

5. Physical Assets & Facilities

Physical assets and facilities are those tangible items your business uses to operate. Many of them include embedded software and are attached to a network, and may be called “operational technology” (OT) or “Internet of Things” (IoT). Therefore, physical assets often rely on cyber assets. These assets may be owned or leased by your company; in some cases they may be owned by others but still put your business at risk.

Cyberattacks can have real-world consequences if they target physical infrastructure. These include:

- Buildings and physical premises: smart office systems, access control systems, etc.
- Manufacturing equipment: industrial control systems (ICS), SCADA, etc.
- Vehicles and transportation: connected cars, autonomous vehicle software, logistics tracking, etc.
- Telecommunications networks: satellites, cellular networks, wireless and wired LANs/WANs, etc.
- Utilities: systems that provide electricity, water, sewage, and other vital services

Method

A *method* is a specific attack vector used to access or affect the asset. These methods lead to the impact of an attack (Effect) on business operations, data integrity, and financial stability.

Discussions of risk scenarios sometimes leave out method as a defining element. For example, the authors of *Measuring and Managing Information Risk: A Fair Approach*, leave method out of their tables (e.g., Table 6.1 on page 97) enumerating risk scenarios. However, cyber risk scenarios involving different methods are often quite different from one another in terms of the level of risk and the controls necessary to reduce their risk, so we've included method as a defining element in our taxonomy.

Method Types

The taxonomy defines the following ten (10) types of methods.

1. Ransomware with Data Exfiltration

Attackers encrypt critical data while also stealing sensitive information to extort the victim further. This increases regulatory, reputational, and financial risks. Possible impacts include:

- Business disruption due to encrypted systems
- Regulatory fines from data exposure (e.g., GDPR, CCPA)
- Double extortion (pay ransom or risk data leak/publication)

Example: The Clop ransomware group steals and leaks data if victims refuse to pay.

2. Ransomware without Data Exfiltration

Attackers encrypt data and demand ransom for decryption but do not steal information. Possible impacts include:

- Business downtime and operational impact
- Financial loss due to ransom payment and recovery costs
- Potential reputational damage

Example: The Ryuk ransomware group is known for high-impact encryption-only attacks.

3. Data Exfiltration (Without Ransomware)

Attackers steal sensitive data for financial gain, competitive advantage, or espionage without encrypting or disrupting systems. Possible impacts include:

- Intellectual property (IP) loss

- Regulatory fines and lawsuits (e.g., GDPR violations)
- Brand damage and loss of customer trust

Example: Hotel chain data breach exposing 500 million customer records.

4. Data Corruption *(Destructive or Accidental)*

Data is altered, manipulated, or deleted, intentionally or accidentally, leading to operational or financial loss. Possible impacts include:

- Inaccurate financial reports, supply chain disruptions
- Regulatory non-compliance (incorrect data reporting)
- Loss of critical business records

Example: A banking trojan modifies transaction details, leading to financial losses.

5. Distributed Denial of Service (DDoS)

Attackers flood servers, applications, or networks with massive traffic to disrupt services. Possible impacts include:

- Website or service downtime, leading to revenue loss
- Increased infrastructure costs to mitigate attack
- Reputation damage due to service unavailability

Example: Mirai botnet launched large-scale DDoS attacks on cloud providers and enterprises.

6. Cryptomining (Cryptojacking)

Attackers hijack computing resources to mine cryptocurrency, leading to performance degradation and financial losses. Possible impacts include:

- Increased cloud/infrastructure costs (excessive CPU/GPU usage)
- Business performance degradation (slow applications, IT instability)
- Potential regulatory risks in highly regulated environments

Example: The Smominru botnet infected servers worldwide for large-scale cryptomining.

7. Account Takeover (Business Email Compromise, Wire Transfer Fraud, etc.)

Cybercriminals manipulate financial transactions, deceive employees, or exploit system vulnerabilities to steal money. Possible impacts include:

- Direct financial loss from fraudulent transactions
- Reputation damage and potential lawsuits

- Loss of executive and customer trust

Example: Business Email Compromise (BEC) attacks result in an account takeover.

8. Wiper Malware (Destructive Attack)

Attackers deploy malware designed to permanently destroy data and systems, often for political, financial, or ideological reasons. Possible impacts include:

- Permanent data loss (without ransom demands)
- Business shutdown due to destroyed infrastructure
- Regulatory and legal repercussions

Example: NotPetya (2017) wiped data across global corporations.

9. System Outage (Non-Malicious Causes Included)

An incident causes unexpected downtime for critical systems, whether due to cyberattacks, internal errors, or third-party failures. Possible impacts include:

- Revenue loss from downtime
- Disrupted supply chain and partner dependencies
- Regulatory impact in sectors like finance and healthcare

Example: Cloud outages from misconfigurations or cyberattacks (e.g., AWS downtime).

10. Data Leakage (Accidental or Intentional Exposure)

Sensitive information is exposed unintentionally, often due to misconfigurations, employee errors, or insufficient access controls. Possible impacts include:

- Regulatory fines and compliance failures
- Competitive disadvantage if proprietary data is leaked
- Loss of customer trust due to exposed PII

Example: S3 bucket misconfigurations leading to exposed customer databases.

Initial Attack Method

To understand the attacker's method in more detail, we can take inspiration from the MITRE ATT&CK kill chains and clearly define an Initial Attack Method (IAM). This is an optional step in defining a scenario. An IAM is the starting point of a threat (or a loss) event. For example, an attacker may start with a phishing attack en route to a ransomware outcome.

Defining the IAM can help you identify the relevant controls more precisely. In our previous example, email filters and other phishing controls would help prevent an attacker from succeeding in this scenario. From a FAIR risk quantification perspective, specifying the IAM can also help you define the 'Threat Event Frequency' more precisely. For example, you may have good phishing attempt frequencies from your own company's experience and from others in your industry.

Our taxonomy specifies sixteen (16) IAM types. We will not define all of them here, but some common IAMs are:

1. Social engineering attacks involve manipulating individuals into revealing sensitive information or performing harmful actions. These include **phishing**, where attackers use deceptive emails or messages to steal credentials or install **malware**, and **SIM swapping**, which involves hijacking a victim's phone number to bypass multi-factor authentication (MFA) and take over accounts. **Deepfake attacks** leverage AI-generated voice or video impersonations to manipulate financial transactions or spread misinformation.

2. **Application** and **service exploitation** focuses on attacking vulnerabilities in externally exposed systems. **External application exploitation** targets weaknesses in web applications or cloud services, while remote service exploitation attacks services like RDP, SSH, or VPNs to gain unauthorized access.

3. Credential-based attacks exploit weak authentication practices. **Credential stuffing** involves using stolen username-password combinations from previous breaches, while brute force attacks systematically guess passwords to gain access. **Privilege abuse** occurs when attackers or insiders escalate their permissions to gain unauthorized control over systems or data.

4. Malware-based attacks include traditional malware (such as ransomware, spyware, and trojans) that compromise systems, steal data, or disrupt operations.

5. **Man-in-the-middle** (MitM) attacks occur when attackers intercept and manipulate communications, often by exploiting unencrypted or poorly secured network connections.

6. **Supply chain attacks** occur when adversaries compromise third-party vendors, software providers, or partners to infiltrate a target organization. These attacks often result in large-scale data breaches and malware distribution, as seen in incidents like SolarWinds.

7. **Physical access** threats involve attackers gaining unauthorized entry to secured locations to compromise systems directly. This can include insider threats, badge cloning, **USB drop attacks**, and unauthorized data center access. IoT attacks target vulnerabilities in connected devices such as smart sensors, industrial control systems, and security cameras to infiltrate networks or create large-scale botnets.

8. Finally, AI and machine learning (ML)-based attacks represent an emerging frontier in cyber threats. **LLM prompt injection** attacks manipulate AI-powered systems to bypass security controls or extract sensitive data. **ML model evasion** tricks AI-driven security solutions into misclassifying malicious inputs, while **training data poisoning** manipulates AI training datasets to degrade performance or introduce hidden vulnerabilities.

Effect

Loss *effect* is the type of loss expected to materialize from a threat actor attacking a specific asset. The effect is expressed in terms of how the asset is impacted (i.e., confidentiality, integrity, and availability) and, in turn, how it translates into a material loss to the business.

Loss Categories

The effects in our taxonomy come from the FAIR Materiality Assessment Model (FAIR-MAM), which describes ten (10) loss categories. These categories represent both primary and secondary losses. Primary losses occur directly as a result of the loss event and are more certain to materialize when a loss event occurs. Secondary losses occur indirectly from a loss event, typically due to actions or reactions by secondary stakeholders who have been harmed from or are motivated by an event. The loss effect *or effects* you choose for a cyber risk scenario can be based on either primary or secondary losses, or a combination of both.

You may already be familiar with the six (6) forms of loss in the standard FAIR Model. The FAIR Cyber Risk Management framework relies on FAIR-MAM to provide more granular cost estimations; it also describes how FAIR-MAM aligns to the Model's six forms of loss. It does so by mapping FAIR-MAM's twenty-six (26) loss *sub*-categories to the six forms of loss. For example, *Business Email Compromise (BEC)*, a FAIR-MAM sub-category of *Financial Fraud*, is mapped to the FAIR Model's *Replacement Cost* (*Primary Loss*) form of loss.

When defining a scenario, you may include multiple loss effects. For example, for a scenario involving a method of ransomware with data exfiltration, your loss effects might include *business interruption*, *cyber extortion*, and *information privacy loss*.

The FAIR-MAM ten categories of losses are defined here.

1. Information Privacy Loss

All costs explicitly related to the compromise of sensitive personal data. Includes costs for the forensic discovery of records breached. Sensitive personal data includes, but is not limited to, the following types:

- **Personal Financial Information (PFI)** — data that can be used to identify an individual's financial status, accounts, transactions, credit history, or tax history
- **Protected Health Information (PHI)** — data that relates to the health status, provision of healthcare, or payment for healthcare that can be linked to an individual
- **Payment Card Information (PCI)** as defined by the Payment Card Industry Data Security Standard (PCI-DSS)
- **Other Personally Identifiable Information** (PII), including any government-issued ID information such as unique identifiers (e.g., US social security number), driver's license, and passport details

2. Proprietary Data Loss

All costs related specifically to non-personal data such as intellectual property, trade secrets, customer or partner data (non-PII), AI systems, and internal corporate information. Includes the loss of market share to competitors due to the theft of IP and trade secrets (including AI systems) as well as the direct cost of recovering AI systems from data corruption.

3. Business Interruption

Costs directly related to an interruption of business processes impacting revenue or operating expenses or loss of third-party revenue-generating services. Includes revenue lost due to a business interruption or system outage as well as the incremental costs of workarounds as a result of an attack.

4. Cyber Extortion

Ransom and any ransom-related support costs for recovering data and/or systems following a ransomware attack. Does not include costs or losses related to business interruption, which are captured under Business Interruption.

5. Incident Investigation & Resolution

Forensic and legal costs associated with investigating and resolving a security incident. Includes the costs for notifying authorities, remediating system and network vulnerabilities, and restoring data. Also includes cybersecurity regulatory fines, the costs of any legal challenges to those fines, in connection with post-incident response as well as regulated or stated security and risk management posture.

6. Financial Fraud

All costs related to the theft of cash or other monetary instruments.

7. Media Fraud

All costs related to the fraudulent use of media or advertising content (e.g., logos, trademarks, or other media content that uniquely identifies a company).

8. Hardware Bricking

The costs to replace IT systems or devices along with the operating systems and applications that were destroyed during a wiper-type attack.

9. Post Breach Security Requirements

Costs spent to improve cybersecurity after a breach, both voluntary improvements and those mandated by a regulatory body or court.

10. Reputational Damage

Costs that may reduce future revenues or increase costs after a breach due to breach related damage to the reputation of the victim company.

Conclusion and Next Steps

This guide is designed to help GRC and Risk teams create structured, clear, and actionable cyber risk scenarios. Our goal is to establish this framework as a new industry standard for defining cyber risk scenarios in the future.

We will follow up with papers on which risk scenarios to consider and how to assess risk scenarios with a 'good enough' degree of accuracy to drive decisions. We will tackle questions such as:

- **How many scenarios do I need?**
- **How do I identify the "right" scenarios?**
- **How specific does the scenario need to be?**
- **How do I find the right data for my analysis?**
- **How do I know if my data/estimates are accurate?**

We welcome your feedback on the cyber risk taxonomy as we continue to refine and improve it, and additional questions or topics that you'd like us to cover. To reach us, email us at Standards@FAIRInstitute.org.