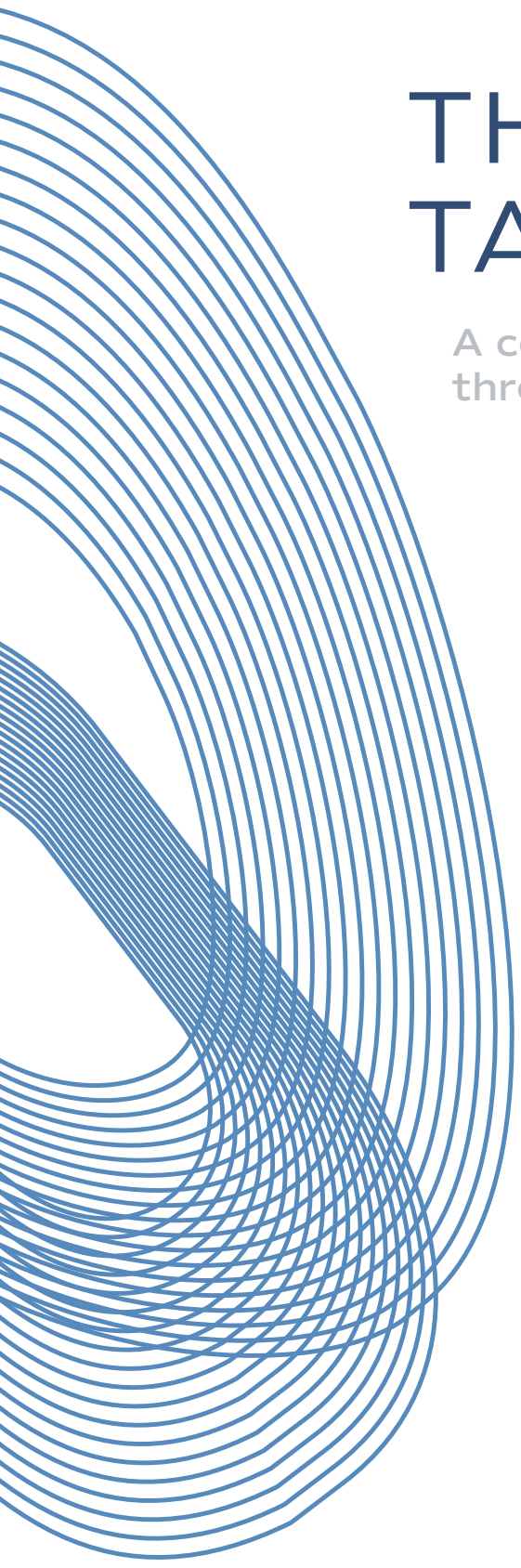
CYBERSECURITY
RISK FOUNDATION

TT
2025

THREAT TAXONOMY

A comprehsensive cybersecurity threat taxonomy and threat model



crfsecure.org

TABLE OF CONTENTS

INTRODUCTION

As the cybersecurity landscape continues to evolve, organizations require more than just reactive threat awareness—they need a precise and strategic framework for understanding, categorizing, and prioritizing the threats they face. Since 2015, we have maintained this taxonomy of cybersecurity threats to information systems. The 2025 edition of the *CRF – Threat Taxonomy* builds upon the foundational work of previous years by significantly expanding the depth of its threat definitions and introducing a more granular approach to threat modeling.

This expanded edition comprehensively maps many of the cybersecurity community's most recognized threat models. By aligning the CRF taxonomy with these established models, we offer a harmonized structure that organizations can rely on for strategic alignment and operational consistency.

This update's core is a new threat rating system that allows organizations to assess threats by type or origin, severity, and likelihood based on a consistent set of modeling criteria. Each threat in the taxonomy is now evaluated across multiple dimensions—such as its potential impact on confidentiality, integrity, and availability, as well as the difficulty of exploitation based on attacker resources and technical accessibility. This structured approach empowers organizations to better prioritize threats and align their cybersecurity safeguards accordingly.

Unlike traditional threat intelligence reports focusing on active indicators and tactical IOCs, the CRF Threat Taxonomy is purpose-built for governance and safeguard selection. It is designed to help organizations establish a shared vocabulary, rate and prioritize threats in context, and support informed decision-making across all levels of the organization—from cybersecurity practitioners to business executives. We hope that this year continues to move the discussion forward and better define a framework for understanding the threats facing organizations today.

DEFINITION

When discussing any topic in the domain of cybersecurity, precision in terminology is not merely an academic exercise; it is a foundational aspect of effective communication and understanding. Too often, technology professionals assume that everyone speaks the same language, and this assumption leads to confusion among practitioners. As we delve into cybersecurity threats' complex and evolving landscape, a clear and precise definition of terms is paramount. Defining terms ensures that all stakeholders, from technology professionals to executive management, are aligned in their understanding and approach. Precise definitions enable us to categorize and evaluate threats accurately, design appropriate defense mechanisms, and implement effective policies and procedures. They form the bedrock upon which we build our strategies, analyze risks, and measure the efficacy of our cybersecurity initiatives. In this whitepaper, we endeavor to establish a common language that will aid in navigating the intricate dynamics of cybersecurity, thereby fostering a coherent and unified response to the myriad of challenges we face in protecting our information systems and the valuable data they contain.

That being said, for this discussion, we shall define cybersecurity threats as:

> **"Anything with the potential to cause harm to information systems and thus prevent the system from achieving the business goal for which it was created."**

While the term "cybersecurity threats" might initially appear straightforward, it encompasses a multitude of nuances and complexities that demand careful consideration. The primary aim of this research is not only to crystallize our understanding of what constitutes a cybersecurity threat but also to classify the various forms these threats can take. We hope that our detailed exploration into the nature of these threats will guide organizations in formulating and implementing appropriate safeguards. These protective measures are crucial for mitigating the risk of threat realization, thus ensuring the robustness and resilience of their information systems. This research aims to empower organizations to develop more effective, preemptive strategies by deepening the understanding of cybersecurity threats and delineating their various forms. These strategies are vital in safeguarding their technological infrastructure and the overarching goals and objectives of their business operations.

SCOPE

In our endeavor to establish a comprehensive taxonomy of cybersecurity threats, we identify three main categories as the scope for any such classification: threat agents, threat activities, and threat impacts on an organization. This tripartite framework provides a holistic view of the cybersecurity landscape, encompassing the full spectrum of risks and challenges that organizations may encounter.

1. **Threat Agents:** This category delves into the various entities initiating cybersecurity threats. These agents can range from individual hackers and insider threats to organized cybercriminal groups, nation-state actors, and even unintentional actors like employees who inadvertently cause security breaches. Understanding the nature and motivations of these agents is crucial for predicting potential attack vectors and designing defenses tailored to specific adversaries.
2. **Threat Activities:** Here, we explore the diverse actions or methods threat agents employ to compromise cybersecurity. This category includes many activities, such as phishing, malware attacks, ransomware, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs). By dissecting these activities, we gain insight into the operational tactics of threat agents, enabling us to anticipate better and counteract their maneuvers.
3. **Threats to an Organization (Impacts):** This final category focuses on the consequences or impacts of cybersecurity threats on an organization. Impacts vary significantly in scale and severity, ranging from data breaches and financial losses to reputational damage and operational disruptions. Understanding these impacts is essential for assessing the potential risks associated with different threats and prioritizing cybersecurity initiatives accordingly.

Our taxonomy aims to provide a structured and comprehensive framework for analyzing cybersecurity threats by defining and examining these three categories. This approach enhances our understanding of the threat landscape and informs the development of more effective strategies and solutions to protect organizations from the myriad cybersecurity risks they face.

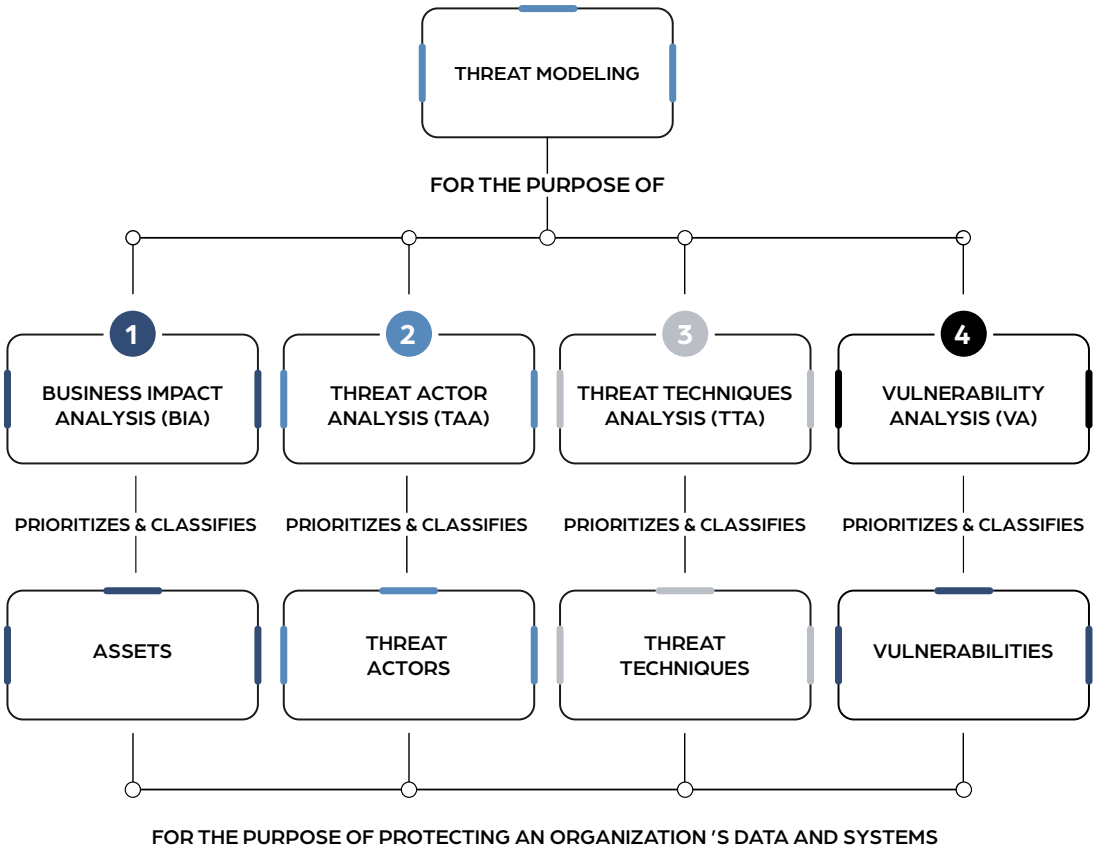
This whitepaper establishes a structured framework for creating and modeling cybersecurity threats rather than focusing on threat intelligence. We aim to construct a comprehensive taxonomy that categorizes and delineates the various facets of cybersecurity threats. This taxonomy is intended to serve as a foundational tool for understanding and systematically addressing the complexities inherent in cybersecurity.

While threat hunters and forensic specialists will undoubtedly find value in the discussions presented here, they are not the sole or primary audience due to the detailed analysis of threat behaviors and classifications. This paper aims to offer a broad spectrum of cybersecurity professionals, including policymakers, IT security strategists, and risk management personnel, a robust conceptual model. This model aids in the identification, categorization, and understanding of potential threats. It is a guide to help these professionals develop more effective cybersecurity strategies and frameworks tailored to this taxonomy's unique organization and requirements, which aims to bridge the gap between theoretical understanding and practical application. Providing a clear and detailed classification of threats enables a more strategic approach to cybersecurity, facilitating better decision-making, risk assessment, and resource allocation. In essence, while the insights within this whitepaper will undoubtedly resonate with threat hunters and forensics experts, its broader intent is to empower a wide range of cybersecurity stakeholders with the knowledge and tools necessary for developing comprehensive, proactive defenses against the entire landscape of cyber threats.

THREAT MODELING

While traditional threat modeling approaches such as Microsoft STRIDE and DREAD have proven valuable for software and vulnerability analysis, this taxonomy embraces a broader view of threat modeling—one that supports governance, risk management, and strategic decision-making across the organization. We recognize that threat modeling can serve different purposes depending on the context and stakeholders involved. To that end, we propose four distinct lenses for modeling threats.

1. **Business Impact Analysis (BIA):** Threat modeling through a BIA lens focuses on understanding how specific threats could disrupt critical business functions. This approach evaluates the potential consequences of threats on availability, confidentiality, integrity, and regulatory or reputational standing—helping prioritize safeguards based on organizational impact rather than technical risk alone.
2. **Threat Actor Analysis (TAA):** TAA emphasizes modeling threats based on potential adversaries' capabilities, motivations, and intent. By profiling actors such as cybercriminals, insiders, or nation-state groups, organizations can better understand who might target them, why, and how persistent or resourced such actors may be.
3. **Threat Techniques Analysis (TTA):** This perspective organizes threats around the specific methods and tactics adversaries use, such as phishing, credential stuffing, or lateral movement. It allows organizations to map their defenses against known techniques and identify gaps where current safeguards may fall short.
4. **Vulnerability Analysis (VA):** VA-based threat modeling examines how susceptible systems, processes, or people are to exploitation. This includes known technical flaws, misconfigurations, and human factors like social engineering susceptibility, offering insight into which threats are most likely to succeed based on existing weaknesses.



Most traditional threat modeling efforts focus narrowly on vulnerability analysis—identifying and assessing technical flaws that attackers could exploit. While this approach is valuable, it often overlooks the broader context in which threats operate. The CRF Threat Taxonomy expands, recognizing that effective threat modeling must surpass just system weaknesses. By incorporating business impact, adversary intent, and attack techniques, this model enables organizations to evaluate where they are vulnerable, who might target them, how those attacks might unfold, and what the consequences could be. This more holistic approach supports better prioritization, aligns cybersecurity with organizational risk, and ensures that threat modeling informs both strategic planning and operational defense.

THREAT RATINGS

We have introduced a systematic threat rating system to prioritize and manage the various threats identified in our taxonomy. Each threat has been assigned a numerical value, reflecting its priority within the broader cybersecurity landscape. This rating system is designed to assist organizations in objectively assessing the significance of each threat, guiding them in allocating their cybersecurity resources and efforts.

The core aim of these ratings is to provide a quantifiable measure of the urgency and necessity of implementing specific controls to counteract each identified threat. While every threat warrants attention in a comprehensive defense strategy, resource constraints often necessitate prioritization. Our rating system offers a structured approach for organizations to focus their limited resources on the most pressing threats strategically.

These threat ratings are the culmination of extensive research and collaboration among contributors to this project, leveraging insights from industry-standard threat models and real-world observations of cyber attacks. It's important to note that these ratings are based on a consensus among participating experts and, though inherently qualitative, reflect a collective judgment on the relative importance of each threat.

The ratings are presented on a scale from one to five, with higher ratings indicating a greater priority in developing an organization's defensive capabilities. It's crucial to understand that these scores primarily assess the likelihood of a threat materializing rather than the potential impact of such an occurrence. Organizations should integrate these ratings into a more comprehensive risk management model that also considers the potential consequences of each threat. However, this research focuses on the likelihood of occurrence, providing a foundational guide for organizations to begin structuring their cybersecurity defenses.

CATEGORIES OF THREAT ACTORS

To begin, we will delve into the diverse array of potential threat actors in the cybersecurity landscape. Our goal is to categorize these actors not through an exhaustive enumeration but by identifying key groups and types that represent the broad spectrum of origins and motivations behind cyber threats. This categorization is crucial as it aids in understanding the varied nature of threats, their potential tactics, and the implications for cybersecurity strategies. While specific actors within each category can be numerous and varied, our focus lies in presenting a structured framework that encapsulates the primary sources of cyber threats.

Among these categories, nation-state actors are acknowledged as significant contributors to the cybersecurity threat landscape. However, it is essential to note that our discussion does not attempt to list every possible nation-state actor. Instead, we provide an overview of the characteristics and objectives typical of such actors, offering insights into their potential impact on cybersecurity. Another unconventional yet pertinent category is natural phenomena, conceptualized as 'Mother Nature.' This inclusion acknowledges that environmental events can inadvertently become catalysts for cybersecurity incidents by directly impacting technological infrastructure or creating chaotic environments that malicious actors may exploit. By exploring these varied categories of threat actors, we aim to present a comprehensive picture that aids organizations in developing robust, adaptable cybersecurity strategies.

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTOR-01	Hacktivists	Individuals or groups who launch cyberattacks for ideological, social, or political reasons.	3.50
ACTOR-02	Cybercriminals	Threat actors engaging in cybercrime for financial gain (e.g., ransomware gangs, fraud rings).	4.00
ACTOR-03	Nation-States	Government-sponsored groups conducting cyber espionage, cyber warfare, or disruption.	3.50
ACTOR-04	Corporate Spies	Competitors or private groups engaging in cyber espionage for economic gain.	3.00
ACTOR-05	Hobbyists	Individuals, often with limited skills, who engage in cyber activities for fun, learning, or recognition.	3.50
ACTOR-06	Malicious Insiders	Employees or contractors who intentionally compromise security, steal data, or sabotage systems.	3.00
ACTOR-07	Careless Insiders	Employees who unintentionally expose an organization to risk through negligence or lack of security awareness.	3.50
ACTOR-08	Compromised Insiders	Employees whose accounts or credentials have been stolen and are being used by external attackers.	3.00

CATEGORIES OF THREAT ACTIVITIES

The following section focuses on threat actions, categorizing the specific methods threat actors use to cause potential harm to an organization's information systems. Understanding these methods is crucial for organizations to defend against cyber threats effectively and help organizations use technology to achieve their business goals. Our taxonomy details these actions, providing a clear framework for identifying and responding to various attack strategies. This precise knowledge is essential for enhancing an organization's cybersecurity measures against various potential threats.

Physical Threats

Physical Threats involve the direct, tangible compromise of an organization's information systems or supporting infrastructure. These threats range from the theft of devices and physical assets to sabotage or targeted destruction of facilities and hardware. They also include environmental and infrastructure disruptions, such as power loss or natural disasters, and physical intrusion or tampering with systems that can bypass digital controls entirely. Despite the growing emphasis on digital threats, physical attacks remain a critical risk—especially in sectors with distributed or high-value environments.

These threats can be broken down further into the following sub-categories of threats:

1. Device and Asset Theft (ACTION PT)
2. Sabotage and Targeted Destruction (ACTION PD)
3. Environmental and Infrastructure Disruptions (ACTION PE)
4. Physical Intrusion and System Tampering (ACTION PI)

The following is our full taxonomy of physical or environmental threats to information systems:

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION PT-01	Theft of Computing Devices	Stealing physical IT assets such as laptops or workstations containing sensitive data.	2.33
ACTION PT-02	Theft of Mobile Devices	Stealing physical IT assets such as smartphones or tablets containing sensitive data.	2.33
ACTION PT-03	Theft of Storage Media	Unauthorized removal of USB drives, external hard disks, or backup tapes containing confidential data.	2.50
ACTION PT-04	Theft of Server or Network Equipment	Illicit removal of enterprise infrastructure such as servers, routers, or network switches from secured facilities.	3.00
ACTION PT-05	Theft of Access Credentials or Security Tokens	Theft or tampering with IT equipment during transit to an organization.	2.17
ACTION PT-06	Theft of Access Credentials or Security Tokens	Stealing smart cards, key fobs, or authentication tokens that grant system access.	2.50
ACTION PT-07	Scavenging for Discarded IT Equipment	Retrieving improperly disposed computers, hard drives, or storage devices for data exploitation.	1.50
ACTION PD-01	Intentional Vandalism of IT Equipment	Deliberately damaging computers, servers, or network hardware.	2.33
ACTION PD-02	Sabotage of Storage Media	Destroying hard drives, SSDs, or backup tapes to make data permanently unrecoverable.	3.00
ACTION PD-03	Cutting Cables and Network Disruption	Severing fiber-optic lines, network cables, or power feeds to disable infrastructure.	2.50
ACTION PD-04	Sabotage of Power Supply	Introducing power surges or voltage fluctuations to damage IT hardware.	2.50
ACTION PD-05	Overheating Attacks via HVAC Tampering	Manipulating cooling systems to overheat and shut down data center equipment.	2.00
ACTION PD-06	Malicious Hardware Destruction (Bad USB Attacks)	Plugging in a specialized device to send high-voltage surges that destroy internal components.	2.83
ACTION PD-07	Arson or Fire-Based Attacks	Deliberately setting fires to destroy IT infrastructure, server rooms, or data centers.	3.67
ACTION PD-08	Use of Explosives or Bombing Attacks	Deploying explosive devices to demolish critical IT assets or facilities.	3.83
ACTION PD-09	Chemical or Acidic Substance Attacks	Using corrosive chemicals to degrade and destroy IT equipment.	2.83
ACTION PD-10	Electromagnetic Pulse (EMP) or Microwave Attacks	Disrupting or permanently disabling IT systems using high-intensity electromagnetic energy.	3.00

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION PE-01	Earthquakes	Structural collapse due to seismic activity causes IT system outages.	2.67
ACTION PE-02	Hurricane	High winds and debris destroy physical IT infrastructure and communication lines.	2.67
ACTION PE-03	Tornado	High winds and debris destroy physical IT infrastructure and communication lines.	2.67
ACTION PE-04	Tsunami	Water intrusion results in catastrophic loss of on-premises IT operations.	2.67
ACTION PE-05	Thunder and Lightning Storms	Lightning surges cause power failures and equipment damage.	2.00
ACTION PE-06	Flooding	Water intrusion from floods, storm surges, or burst pipes damages IT assets.	2.50
ACTION PE-07	Corrosive Environmental Conditions	Pollution, airborne particles, or saltwater corrosion deteriorate IT hardware.	1.67
ACTION PE-08	Water Contamination	Exposure to excessive humidity or accidental leaks damages hardware.	1.67
ACTION PE-09	Fire	Excessive smoke or direct fire exposure leads to system damage.	3.67
ACTION PE-10	Extreme Heat	Temperature extremes cause overheating, component failures, or condensation damage.	2.00
ACTION PE-11	Extreme Cold	Temperature extremes cause overheating, component failures, or condensation damage.	2.00
ACTION PE-12	Radiation and Space Weather Disruptions	Solar flares or geomagnetic storms disrupt satellite communications and IT infrastructure.	1.83
ACTION PE-13	Structural Facility Damage	Building failure due to natural disasters or structural issues destroys IT infrastructure.	2.67
ACTION PE-14	Biological Contaminants	Long-term exposure to mold, bacteria, or organic hazards degrades IT assets.	1.50
ACTION PI-01	Unauthorized Physical Access to Secure Areas	Gaining access to restricted locations like data centers or server rooms.	2.67
ACTION PI-02	Tailgating or Piggybacking into Secure Facilities	Following an authorized person into a controlled area without proper credentials.	2.50
ACTION PI-03	Badge Cloning or Credential Theft	Replicating or stealing access cards, RFID badges, or biometric credentials.	2.50
ACTION PI-04	Direct Physical Modification of IT Systems	Manually altering configurations, firmware, or tampering with hardware.	3.33
ACTION PI-05	Implanting Hardware Spy Devices	Attaching keyloggers, USB sniffers, or network taps for data interception.	2.33
ACTION PI-06	Malware Injection via External Media	Plugging in infected USB drives or removable storage to deploy malware.	3.33
ACTION PI-07	Firmware or Supply Chain Tampering	Installing malicious firmware before IT assets reach their destination.	3.50

Resource Threats

Resource Threats emerge when the underlying services, supply chains, or personnel essential to operations are disrupted or unavailable. These include infrastructure and service outages, failures across critical suppliers or third-party ecosystems, and workforce or talent shortages that leave organizations unable to maintain or secure their systems. As modern enterprises become increasingly interconnected and reliant on external partners, resource threats have evolved into significant systemic risks that can impact cybersecurity indirectly but severely.

These threats can be broken down further into the following sub-categories of threats:

1. Infrastructure and Service Disruptions (ACTION RD)
2. Supplier and Supply Chain Failures (ACTION RS)
3. Workforce and Talent Shortages (ACTION RW)

The following is our full taxonomy of resource threats to information systems:

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION RD-01	Electrical Power Supply Interruption	Loss or instability of electrical power affecting critical systems and operations.	2.67
ACTION RD-02	Communication Network Failure	Breakdown of communication infrastructures, including internet, telephone, or radio systems.	2.50
ACTION RD-03	Transportation System Disruption	Obstruction or failure of transportation networks hindering the movement of goods and personnel.	1.83
ACTION RD-04	Water Supply Disruption	Interruption or contamination of water resources essential for facility operations.	2.00
ACTION RD-05	Natural Gas Supply Interruption	Disruption in the delivery of natural gas required for heating or industrial processes.	1.50
ACTION RD-06	Fuel Supply Shortage	Unavailability of fuel necessary for generators, vehicles, or equipment.	2.00
ACTION RD-07	Critical Material Shortage	Insufficient availability of essential materials or components necessary for production or services.	2.00
ACTION RD-08	Sanitation Service Failure	Breakdown in waste management or sanitation services impacting operational hygiene.	1.33
ACTION RD-09	Emergency Services Unavailability	Inaccessibility of critical emergency services such as fire, medical, or law enforcement support.	2.00

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION RS-01	Supplier Financial Insolvency	Supplier's financial instability leading to inability to fulfill contractual obligations.	2.00
ACTION RS-02	Supplier Cybersecurity Breach	Cyberattack on a supplier compromising their systems and affecting service delivery.	3.00
ACTION RS-03	Supplier Operational Failure	Internal failures within a supplier's operations causing delays or cessation of services.	2.00
ACTION RS-04	Supplier Legal or Regulatory Non-Compliance	Supplier's failure to adhere to legal or regulatory standards resulting in operational restrictions.	1.33
ACTION RS-05	Supplier Labor Disputes	Strikes or labor conflicts within a supplier's workforce disrupting their services.	1.33
ACTION RS-06	Supplier Geopolitical Instability	Political unrest or instability in a supplier's region affecting their operational capabilities.	2.00
ACTION RS-07	Supplier Natural Disaster Impact	Natural disasters affecting supplier facilities leading to service interruptions.	2.00
ACTION RS-08	Supplier Intellectual Property Theft	Loss of critical intellectual property at the supplier leading to competitive disadvantages or operational halts.	1.83
ACTION RS-09	Supplier Dependency on Sub-tier Suppliers	Disruptions in sub-tier suppliers impacting the primary supplier's ability to deliver services.	2.17
ACTION RW-01	Workforce Health Crisis	Widespread illness among staff reducing available skilled personnel.	2.33
ACTION RW-02	Key Personnel Attrition	Departure of critical staff leading to gaps in essential skills and knowledge.	1.83
ACTION RW-03	Recruitment Challenges	Difficulty in attracting qualified candidates for essential roles.	1.67
ACTION RW-04	Training Deficiencies	Insufficient training programs resulting in underqualified personnel.	2.00
ACTION RW-05	Employee Strikes or Work Stoppages	Labor actions leading to temporary loss of workforce availability.	2.33
ACTION RW-06	Security Clearance Revocations	Loss of personnel due to revoked security clearances impacting sensitive operations.	2.33
ACTION RW-07	Remote Work Limitations	Inability to perform duties remotely due to technological or policy constraints.	1.67
ACTION RW-08	Geopolitical Travel Restrictions	Travel bans or restrictions preventing personnel from accessing necessary locations.	1.33
ACTION RW-09	Competitive Talent Poaching	Competitors attracting away key talent, leading to skill shortages.	1.67

Human Threats

Human Threats originate from individuals within or interacting with the organization and often stem from behavior rather than technology. This category includes human error and negligence, such as misconfigurations or accidental data loss; social engineering and deception, where attackers manipulate people to gain access; and insider misuse or privilege abuse, in which trusted users intentionally or unintentionally undermine security. These threats highlight the importance of organizational culture, education, and access control in any cybersecurity strategy.

These threats can be broken down further into the following sub-categories:

1. Human Error and Negligence (ACTION HN)
2. Social Engineering and Deception (ACTION HS)
3. Insider Misuse and Privilege Abuse (ACTION HM)

The following is our full taxonomy of human threats to information systems:

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION HN-01	Mishandling of Sensitive Information	Employees unintentionally exposing confidential information through improper storage, disposal, or sharing practices.	2.33
ACTION HN-02	Misdelivery of Sensitive Information	Sending confidential data to unauthorized recipients due to errors in email addresses or mailing information.	2.33
ACTION HN-03	Unsafe Use of Personal Devices	Accessing corporate networks or data from unsecured personal devices, increasing risk of data breaches.	2.33
ACTION HS-01	Phishing Attacks	Deceptive communications, such as emails or messages, tricking individuals into revealing sensitive information or performing actions compromising security.	2.50
ACTION HS-02	Spear-Phishing	Targeted phishing attacks aimed at specific individuals or organizations.	2.67
ACTION HS-03	Whaling	High-value spear phishing attacks targeting executives or senior personnel.	3.17
ACTION HS-04	Vishing (Voice Phishing)	Using phone calls to deceive individuals into revealing confidential information.	1.83
ACTION HS-05	Smishing (SMS Phishing)	Sending fraudulent text messages to trick recipients into divulging personal or financial information.	1.83
ACTION HS-06	Impersonation (Pretexting)	Pretending to be a trusted individual or authority figure to extract sensitive information or gain access.	2.50
ACTION HS-07	Watering Hole Attacks	Compromising websites frequented by targeted individuals to deliver malicious content.	2.67
ACTION HS-08	Baiting	Enticing individuals with promises of rewards to encourage them to compromise security protocols.	2.17
ACTION HS-09	Quid Pro Quo	Offering a service or benefit in exchange for information or access, leading to security breaches.	2.00
ACTION HM-01	Insider Unauthorized Data Access	Accessing sensitive information without a legitimate business need or authorization.	2.50
ACTION HM-02	Insider Data Manipulation	Altering or falsifying data without authorization, compromising data integrity.	3.00
ACTION HM-03	Insider Privilege Abuse	Exceeding authorized access levels to manipulate systems or data improperly.	3.33

Technical Threats

Technical Threats represent deliberate, technology-driven actions designed to exploit systems or data. These include reconnaissance activities that gather information for future attacks, credential abuse, and software and data exploitation techniques—such as attacks on system software, business applications, or data in transit and at rest. The category also includes cryptanalysis aimed at breaking encryption and denial-of-service (DoS) attacks intended to disrupt availability. These threats are often visible in cybersecurity discussions and require continuous adaptation to emerging tools and techniques.

These threats can be broken down further into the following sub-categories of threats:

1. Reconnaissance (ACTION TR)
2. Credential Abuse (ACTION TCA)
3. Abuse of System Software (ACTION TAS)
4. Abuse of Business Applications (ACTION TAA)
5. Abuse of Data in Transit (ACTION TDT)
6. Abuse of Data at Rest (ACTION TDR)
7. Abuse of Data Handling (ACTION DH)
8. Cryptanalysis (ACTION TC)
9. Denial of Service (ACTION TDS)

The following is our full taxonomy of technical threats to information systems:

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TR-01	Passive Reconnaissance	Collecting information about the target without direct interaction, such as harvesting data from public websites, social media, and online forums.	1.50
ACTION TR-02	Active Reconnaissance	Directly interacting with the target's systems to gather information, including methods like network scanning, port scanning, and vulnerability scanning.	2.00
ACTION TR-03	Network Scanning	Using tools to identify active devices, open ports, and services running on a network to detect potential entry points.	2.00
ACTION TR-04	Port Scanning	Sending data packets to specific ports on a target system to identify open or closed ports, which can reveal available services and potential vulnerabilities.	2.00
ACTION TR-05	Vulnerability Scanning	Employing automated tools to detect known vulnerabilities in systems, applications, or networks that could be exploited.	2.00
ACTION TR-06	OS Fingerprinting	Determining the operating system of a target system by analyzing its responses to network probes, aiding in tailoring specific exploits.	1.50
ACTION TR-07	Service Enumeration	Identifying network services and their versions running on a target system to find potential vulnerabilities associated with specific service versions.	2.00
ACTION TR-08	DNS Interrogation	Gathering information about domain names, IP addresses, and network infrastructure by querying DNS records.	1.50
ACTION TR-09	Email Harvesting	Collecting email addresses associated with a target organization from public sources, which can be used in phishing attacks.	1.50
ACTION TR-10	Social Engineering	Manipulating individuals to divulge confidential information, such as organizational structure or security practices, without direct system interaction.	3.00
ACTION TR-11	Application Footprinting	Analyzing a target's website to gather information about its structure, technologies used, and potential vulnerabilities.	1.50
ACTION TR-12	WHOIS Database Querying	Accessing WHOIS databases to obtain registration details of domain names, including administrative contacts and hosting providers.	1.50
ACTION TR-13	Metadata Extraction	Retrieving metadata from publicly available documents or images to uncover information like author details, software used, or creation dates.	1.50
ACTION TR-14	Wireless Network Scanning	Detecting and analyzing wireless networks to identify access points, encryption types, and potential vulnerabilities.	2.00
ACTION TR-15	Physical Observation	Observing a target's physical premises to gather information about security measures, employee habits, or infrastructure layout.	1.50

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TCA-01	Credential Harvesting	Stealing user credentials through methods like phishing, malware, or exploiting vulnerabilities to collect usernames and passwords.	3.33
ACTION TCA-02	Credential Stuffing	Using large volumes of stolen credentials to attempt unauthorized access across multiple accounts, leveraging users' tendency to reuse passwords.	2.83
ACTION TCA-03	Brute Force Attacks	Systematically attempting all possible password combinations to gain unauthorized access to an account.	2.83
ACTION TCA-04	Password Spraying	Attempting a few commonly used passwords across many accounts to avoid detection and account lockouts.	2.83
ACTION TCA-05	Session Hijacking	Intercepting or stealing active session tokens to impersonate a user without needing their credentials.	3.33
ACTION TCA-06	Pass-the-Hash Attacks	Using hashed password representations to authenticate without cracking the actual password, exploiting weaknesses in authentication protocols.	3.33
ACTION TCA-07	Keylogging	Installing malicious software or hardware to record keystrokes, capturing credentials as users type them.	3.33
ACTION TCA-08	Man-in-the-Middle (MitM) Attacks	Intercepting communications between a user and a system to capture or alter credentials during transmission.	3.33
ACTION TCA-09	Credential Reuse	Taking advantage of users reusing passwords across multiple platforms to access additional systems once one set of credentials is compromised.	2.83
ACTION TCA-10	Token Theft	Stealing authentication tokens or cookies to impersonate users without needing their actual credentials.	2.83
ACTION TCA-11	Abuse of Default Credentials	Exploiting unchanged default usernames and passwords in systems or applications to gain unauthorized access.	2.83
ACTION TCA-12	Social Engineering for Credential Disclosure	Manipulating individuals into voluntarily revealing their credentials through deceptive tactics.	2.83
ACTION TCA-13	Credential Phishing	Crafting deceptive communications, such as emails or messages, to trick users into providing their login information.	2.83
ACTION TCA-14	Credential Theft via Malware	Deploying malicious software designed to extract stored credentials from infected systems.	3.33
ACTION TCA-15	Exploiting Insecure Credential Storage	Accessing poorly protected credential storage locations, such as plaintext files or weakly hashed password databases.	2.83
ACTION TCA-16	Abuse of Password Recovery Mechanisms	Manipulating password reset or recovery processes to gain unauthorized access to user accounts.	2.83
ACTION TCA-17	Credential Cracking	Using computational methods to decipher hashed or encrypted passwords, especially those that are weak or commonly used.	2.83
ACTION TCA-18	Abuse of Single Sign-On (SSO) Tokens	Exploiting vulnerabilities in SSO implementations to gain unauthorized access across multiple services.	2.83
ACTION TCA-19	Exploiting Third-Party Authentication Flaws	Taking advantage of weaknesses in third-party authentication providers to compromise user credentials.	2.83

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TAS-01	Memory Manipulation	Exploiting vulnerabilities such as buffer overflows to manipulate a system's memory, allowing execution of arbitrary code or system crashes.	2.83
ACTION TAS-02	Cache Poisoning	Injecting malicious data into a system's cache, leading to the use of incorrect or harmful information in subsequent operations.	2.50
ACTION TAS-03	Manipulation of Trusted Systems	Compromising systems that are inherently trusted within a network to facilitate unauthorized activities.	3.50
ACTION TAS-04	Maintaining System Persistence	Implementing methods to ensure continued unauthorized access to a system over an extended period.	3.50
ACTION TAS-05	Deployment of Rootkits	Installing rootkits to gain privileged access and conceal malicious activities.	3.50
ACTION TAS-06	Dissemination of Mobile Malware	Creating and distributing malware specifically targeting mobile devices.	3.00
ACTION TAS-07	Infected Trusted Mobile Apps	Compromising legitimate mobile applications to distribute malware.	3.00
ACTION TAS-08	Elevation of Privileges	Exploiting vulnerabilities to gain higher access levels within a system.	3.50
ACTION TAS-09	Deployment of Spyware	Installing software that secretly monitors user activity or displays unwanted advertisements.	2.33
ACTION TAS-10	Distribution of Malware	Spreading malicious code that attaches itself to legitimate files and replicates.	3.50
ACTION TAS-11	Rogue Security Software (Scareware)	Distributing fake security software that deceives users into thinking their system is compromised, prompting them to purchase unnecessary services.	2.50
ACTION TAS-12	Generation and Use of Rogue Certificates	Creating fake digital certificates to impersonate trusted entities or intercept secure communications.	3.17
ACTION-TAS-13	DNS Poisoning/ Spoofing	Manipulating DNS records to redirect users to malicious sites.	3.17
ACTION TAS-14	Misuse of Audit Tools	Exploiting legitimate auditing tools for malicious purposes.	2.50
ACTION TAS-15	Remote Code Execution	Exploiting vulnerabilities that allow attackers to execute arbitrary code on a remote system.	3.50
ACTION TAS-16	System Intrusion and Tampering	Gaining unauthorized access to systems and altering their configurations or data.	3.50

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TAA-01	Application Layer Injection	Exploiting vulnerabilities in business applications by injecting malicious code or commands, such as SQL injection or cross-site scripting (XSS), to manipulate application behavior or access unauthorized data.	3.50
ACTION TAA-02	Business Logic Abuse	Manipulating the legitimate functionalities of business applications to achieve malicious objectives, such as exploiting workflow processes to conduct unauthorized transactions or access restricted information.	2.67
ACTION TAA-03	Unauthorized Privilege Escalation	Exploiting application flaws to gain higher access levels within business applications, allowing unauthorized actions or data access beyond the intended permissions.	3.50
ACTION TAA-04	Abuse of Application Programming Interfaces (APIs)	Exploiting vulnerabilities in APIs to manipulate application behavior, access unauthorized data, or disrupt services.	3.50
ACTION TAA-05	Session Hijacking	Taking over a user's active session within a business application to impersonate the user and perform unauthorized actions.	3.17
ACTION TAA-06	Exploitation of Unpatched Vulnerabilities	Targeting known but unpatched vulnerabilities in business applications to gain unauthorized access or disrupt services.	3.50
ACTION TAA-07	Abuse of Third-Party Integrations	Exploiting weaknesses in third-party plugins or integrations within business applications to introduce malicious code or gain unauthorized access.	3.00
ACTION TAA-08	Misuse of Automation Features	Leveraging automation features within business applications, such as macros or scripts, to execute malicious actions or propagate malware.	2.83
ACTION TAA-09	Data Exfiltration via Application Features	Utilizing legitimate data export or reporting features within business applications to extract sensitive information without authorization.	2.83
ACTION TAA-10	Abuse of OAuth Tokens	Compromising or misusing OAuth tokens to gain unauthorized access to business applications or APIs, potentially leading to data breaches or unauthorized actions.	3.17
ACTION TAA-11	Exploitation of Default Credentials	Taking advantage of unchanged default usernames and passwords in business applications to gain unauthorized access.	2.67
ACTION TAA-12	Abuse of Error Handling	Manipulating error messages or debugging information in business applications to gather sensitive information or identify vulnerabilities for further exploitation.	2.00
ACTION TAA-13	Cross-Site Request Forgery (CSRF)	Forcing a logged-in user's browser to send unauthorized requests to a business application, potentially leading to unintended actions or data exposure.	2.67
ACTION TAA-14	Abuse of File Upload Functionality	Uploading malicious files through file upload features in business applications to execute arbitrary code or distribute malware.	3.50
ACTION TAA-15	Abuse of Search Engine Optimization (SEO)	Manipulating search engine algorithms to promote malicious or fraudulent business applications, misleading users and potentially leading to data breaches or financial loss.	2.00
ACTION TAA-16	Abuse of Social Media Trust	Exploiting the inherent trust in social media platforms to distribute malicious business applications or links, leading to unauthorized access or data compromise.	2.00
ACTION TAA-17	Abuse of Cloud Resources	Exploiting cloud-based business applications to conduct unauthorized activities, such as deploying malware or launching attacks against other systems.	3.00
ACTION TAA-18	Abuse of Software Update Mechanisms	Compromising the software update mechanisms of business applications to distribute malicious updates, leading to widespread exploitation.	3.50
ACTION TAA-19	Abuse of Application Configuration	Exploiting misconfigurations in business applications, such as default settings or overly permissive permissions, to gain unauthorized access or escalate privileges.	3.00
ACTION TAA-20	Web Application Attacks (Injection)	Conducting attacks like SQL injection or cross-site scripting (XSS) to exploit vulnerabilities in web applications.	3.50
ACTION TAA-21	Receipt of Unsolicited Emails (SPAM)	Sending unsolicited emails to users, which may contain malicious links or attachments.	1.00
ACTION TAA-22	Unsolicited Infected Emails	Distributing emails with malicious attachments or links to compromise recipient systems.	2.33

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TDT-01	Eavesdropping	Unauthorized interception of unencrypted communications to access sensitive information, such as passwords or personal details.	2.33
ACTION TDT-02	Man-in-the-Middle (MITM) Attack	Intercepting and potentially altering communications between two parties without their knowledge, leading to data theft or unauthorized data manipulation.	3.17
ACTION TDT-03	Packet Sniffing	Capturing and analyzing data packets as they traverse networks, exposing confidential information.	2.33
ACTION TDT-04	Replay Attack	Re-transmitting captured data packets to deceive systems into performing unauthorized actions or granting illegitimate access.	2.67
ACTION TDT-05	Session Hijacking	Taking over an active communication session by intercepting session tokens or cookies, allowing unauthorized actions under a legitimate user's identity.	3.17
ACTION TDT-06	SSL/TLS Hijacking	Exploiting vulnerabilities in SSL/TLS protocols to intercept and decrypt secure communications, compromising data confidentiality.	2.83
ACTION TDT-07	DNS Spoofing	Corrupting DNS data to redirect traffic to malicious sites, enabling interception or manipulation of data in transit.	3.17
ACTION TDT-08	Wi-Fi Eavesdropping	Intercepting data transmitted over unsecured or poorly secured Wi-Fi networks, capturing sensitive information.	2.33
ACTION TDT-09	Rogue Access Point	Setting up unauthorized wireless access points to intercept data from devices that connect to them, leading to data theft or injection of malicious content.	2.33
ACTION TDT-10	Evil Twin Attack	Creating a fraudulent Wi-Fi network that mimics a legitimate one, tricking users into connecting and exposing their data to interception.	2.33
ACTION TDT-11	Bluetooth Sniffing	Capturing data transmitted between Bluetooth devices to access sensitive information or inject malicious data.	1.83
ACTION TDT-12	Radio Frequency (RF) Interception	Using specialized equipment to intercept data transmitted over radio frequencies, such as mobile communications or satellite links.	2.33
ACTION TDT-13	Side-Channel Attack	Exploiting indirect information, such as electromagnetic emissions or power consumption, to infer data being processed or transmitted.	2.33
ACTION TDT-14	Traffic Analysis	Observing patterns and characteristics of data flow to deduce sensitive information without directly intercepting the content.	1.67
ACTION TDT-15	SSL Stripping	Downgrading a secure HTTPS connection to an unencrypted HTTP connection, allowing data interception.	2.33
ACTION TDT-16	ARP Spoofing	Sending falsified ARP messages to associate the attacker's MAC address with the IP address of a legitimate system, enabling data interception.	2.67

ACTION TDT-17	BGP Hijacking	Manipulating the Border Gateway Protocol to reroute data through malicious networks, facilitating interception or data manipulation.	3.50
ACTION TDT-18	Cable Tapping	Physically tapping into wired communication lines to intercept data transmissions.	2.83
ACTION TDT-19	Optical Fiber Tapping	Intercepting data transmitted over fiber optic cables by bending or splicing the fibers to extract light signals.	2.83
ACTION TDT-20	TEMPEST Attack	Exploiting electromagnetic emissions from electronic devices to reconstruct data being processed or transmitted.	2.83
ACTION TDT-21	SIM Card Cloning	Duplicating a SIM card to intercept mobile communications intended for the original device.	2.33
ACTION TDT-22	IMSI Catching	Using devices like IMSI catchers to intercept mobile phone communications by acting as fake cell towers.	2.33
ACTION TDT-23	Satellite Signal Interception	Capturing data transmitted via satellite links, potentially exposing sensitive information.	2.33
ACTION TDT-24	Microwave Link Interception	Intercepting data transmitted over microwave communication links, often used in telecommunications.	2.33
ACTION TDT-25	Cable Modem Hacking	Compromising cable modems to intercept or manipulate data transmitted over cable networks.	2.67
ACTION-TDT-26	VPN Traffic Decryption	Exploiting vulnerabilities in VPN protocols or implementations to decrypt and access data transmitted through VPNs.	2.83
ACTION TDT-27	Cloud Service Interception	Compromising cloud service communications to intercept data exchanged between clients and cloud servers.	3.50
ACTION TDT-28	API Traffic Interception	Intercepting data transmitted between applications and APIs, potentially leading to data theft or manipulation.	3.17

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TDR-01	Residual Data Recovery	Retrieving sensitive data from improperly sanitized or discarded storage media.	2.33
ACTION TDR-02	Unauthorized Decryption	Decrypting encrypted data without authorization, often by exploiting weak encryption methods or obtaining decryption keys illicitly.	2.83
ACTION TDR-03	Data Hiding	Concealing malicious data within legitimate data storage to evade detection.	2.33
ACTION TDR-04	Metadata Manipulation	Altering metadata associated with stored data to mislead or confuse data management processes.	2.00
ACTION TDR-05	Unauthorized Indexing	Creating unauthorized indexes of stored data to facilitate quicker access for malicious purposes.	2.00
ACTION TDR-06	Data Aggregation for Profiling	Combining various data sources to create detailed profiles without consent, potentially violating privacy regulations.	1.83

ACTION TDR-07	Unauthorized Backup Access	Accessing and potentially altering or deleting backup data without authorization, compromising data recovery processes.	3.50
ACTION TDR-08	Data Misplacement	Storing data in incorrect or unauthorized locations, leading to potential exposure or loss.	1.67
ACTION TDR-09	Data Duplication	Creating unauthorized copies of data, increasing the risk of data breaches and complicating data management.	2.17
ACTION TDR-10	Data Concealment	Hiding data within other data sets or storage locations to prevent detection by security measures.	2.50
ACTION TDR-11	Data Obfuscation	Deliberately making data unclear or unintelligible to conceal its true meaning or to hinder analysis.	2.00
ACTION TDR-12	Unauthorized Data Migration	Moving data to different storage systems or locations without authorization, potentially exposing it to additional risks.	3.00
ACTION TDR-13	Data Misclassification	Incorrectly labeling data sensitivity levels to either overexpose or unnecessarily restrict access to data.	1.67
ACTION TDR-14	Data Compression Abuse	Using data compression techniques to hide malicious data within compressed files, evading detection mechanisms.	1.67
ACTION TDR-15	Data Format Manipulation	Altering the format of stored data to disrupt processing or to exploit vulnerabilities in applications that handle the data.	2.50
ACTION TDR-16	Unauthorized Data Encryption	Encrypting data without authorization to lock out legitimate users or to prepare for ransom demands.	3.17
ACTION TDR-17	Data Integrity Attack	Deliberately altering data to compromise its accuracy and reliability, leading to incorrect decisions or operations.	3.17
ACTION TDR-18	Data Shadowing	Creating hidden copies of data that are not subject to standard security controls, increasing the risk of unauthorized access.	2.33
ACTION TDR-19	Data Residue Exploitation	Recovering leftover data fragments from storage media that were not properly sanitized, potentially exposing sensitive information.	2.33
ACTION TDR-20	Unauthorized Metadata Access	Accessing metadata without permission to gather information about data structures, usage patterns, or to facilitate further attacks.	1.83
ACTION TDR-21	Data Archiving Abuse	Misusing archiving processes to store unauthorized data or to hide malicious activities within legitimate archives.	1.83
ACTION TDR-22	Data Retention Policy Manipulation	Altering data retention policies without authorization to retain or delete data inappropriately, potentially violating compliance requirements or hindering investigations.	2.50
ACTION TDR-23	Data Storage Misconfiguration	Intentionally or negligently setting incorrect configurations on storage systems, leading to potential data exposure or loss.	3.00
ACTION TDR-24	Data Disposal Negligence	Failing to properly delete, destroy, or sanitize data when it is no longer needed, leading to potential unauthorized access, data breaches, or regulatory non-compliance.	3.00

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TDH-01	Data Leakage/Theft	Unauthorized access and extraction of sensitive data from an organization's systems, leading to potential data breaches and loss of confidentiality.	2.83
ACTION TDH-02	Data Tampering	Unauthorized alteration of data within a system, compromising its integrity and potentially leading to incorrect decision-making or operational failures.	3.00
ACTION TDH-03	Data Injection	Introducing malicious or unauthorized data into a system to manipulate its operations or corrupt legitimate data.	3.17
ACTION TDH-04	Data Exposure	Inadvertent or deliberate exposure of sensitive data to unauthorized entities, compromising confidentiality.	2.83
ACTION TDH-05	Data Misuse	Unauthorized or inappropriate use of data beyond its intended purpose, leading to potential privacy violations or security risks.	2.33
ACTION TDH-06	Data Hoarding	Accumulating and retaining unnecessary or outdated data, increasing the risk of unauthorized access and complicating data management.	1.67
ACTION TDH-07	Data Fragmentation	Splitting data into inconsistent or incompatible formats, hindering effective data management and security controls.	1.67
ACTION TDH-08	Data Scraping	Extracting large amounts of data from websites or databases without authorization, potentially violating terms of service and privacy policies.	1.67
ACTION TDH-09	Data Poisoning	Introducing false or misleading data into a system to corrupt its outputs or analytics, undermining trust in the data's integrity.	2.83
ACTION TDH-10	Data Snooping	Unauthorized browsing or accessing of data without a legitimate need, violating privacy and security policies.	2.33
ACTION TDH-11	Data Spillage	Accidental or intentional transfer of classified or sensitive data to an unprotected or unauthorized environment, leading to potential exposure.	2.33
ACTION TDH-12	Data Interception	Unauthorized capturing of data during transmission, leading to potential data breaches and loss of confidentiality.	2.83
ACTION TDH-13	Data Overexposure	Providing broader access to data than necessary, increasing the risk of unauthorized use or breaches.	2.33
ACTION TDH-14	Data Misrouting	Sending data to incorrect destinations, potentially exposing it to unauthorized parties.	2.50
ACTION TDH-15	Data Underclassification	Failing to assign appropriate sensitivity levels to data, resulting in inadequate protection measures.	1.83
ACTION TDH-16	Data Overclassification	Assigning excessively high sensitivity levels to data, leading to unnecessary restrictions and operational inefficiencies.	1.17
ACTION TDH-17	Data Aggregation	Combining data from multiple sources without considering cumulative sensitivity, potentially leading to exposure of confidential information.	1.83
ACTION TDH-18	Data Residue	Leaving remnants of data in storage after deletion attempts, which can be recovered by unauthorized parties.	1.83
ACTION TDH-19	Data Mislabeling	Incorrectly tagging data with metadata, causing mishandling and security lapses.	2.00
ACTION TDH-20	Data Synchronization Failure	Inadequate syncing of data across systems, leading to inconsistencies and potential security gaps.	2.00
ACTION TDH-21	Data Backup Negligence	Failing to properly back up data, risking loss of information and hindering disaster recovery efforts.	2.67
ACTION TDH-22	Data Restoration Failure	Inability to accurately restore data from backups, leading to data loss or corruption.	2.67
ACTION TDH-23	Data Masking Failure	Inadequate masking of sensitive data during testing or development, exposing it to unauthorized access.	1.83
ACTION TDH-24	Data Archiving Negligence	Failing to securely archive data, leading to potential loss or unauthorized access over time.	1.83
ACTION TDH-25	Data Retention Policy Violation	Retaining data longer than necessary or mandated, increasing exposure risk and potential legal liabilities.	2.17
ACTION TDH-26	Data Anonymization Failure	Ineffective anonymization techniques that allow re-identification of individuals.	1.83

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TC-01	Brute-Force Key Search	Attempting all possible keys systematically until the correct one is found to decrypt encrypted data.	2.33
ACTION TC-02	Differential Cryptanalysis	Analyzing differences in ciphertexts resulting from slight variations in plaintext to uncover patterns and deduce the encryption key.	2.33
ACTION TC-03	Linear Cryptanalysis	Using linear approximations to describe the behavior of the block cipher to find correlations between plaintext, ciphertext, and the key.	2.33
ACTION TC-04	Integral Cryptanalysis	Examining how sets of chosen plaintexts affect the sums of ciphertexts to exploit structural weaknesses in substitution–permutation networks.	2.33
ACTION TC-05	Algebraic Attacks	Representing the cipher as a system of algebraic equations and solving them to recover the encryption key.	2.33
ACTION TC-06	Related-Key Attacks	Exploiting relationships between multiple keys, such as similarities or predictable differences, to uncover the original key.	2.33
ACTION TC-07	Side-Channel Attacks	Gathering information from the physical implementation of a cryptosystem, such as timing information or power consumption, to deduce the key.	2.50
ACTION TC-08	Meet-in-the-Middle Attack	Reducing the complexity of brute-force attacks by simultaneously encrypting from the plaintext side and decrypting from the ciphertext side to find a match in the middle.	2.33
ACTION TC-09	Impossible Differential Cryptanalysis	Identifying differentials that cannot occur and using this information to eliminate possible keys.	2.33
ACTION TC-10	Boomerang Attack	Combining two differentials to form a quartet structure that helps in analyzing the cipher and recovering the key.	2.33
ACTION TC-11	Slide Attack	Exploiting the self-similarity in the encryption process by finding fixed points that remain unchanged under certain transformations.	2.33
ACTION TC-12	XSL Attack	Utilizing advanced algebraic techniques to solve systems of equations representing the cipher, aiming to recover the key more efficiently than brute-force methods.	2.33
ACTION TC-13	Quantum Cryptanalysis	Applying quantum computing algorithms, such as Shor's algorithm, to solve mathematical problems underlying cryptographic systems, potentially breaking them.	3.00
ACTION TC-14	Differential-Linear Cryptanalysis	Combining differential and linear cryptanalysis techniques to exploit both differential characteristics and linear approximations in a cipher.	2.83
ACTION TC-15	Mod-n Cryptanalysis	Analyzing the modular arithmetic properties of a cipher to find weaknesses and recover the key.	2.83
ACTION TC-16	Impossible Differential Cryptanalysis	Identifying differentials that cannot occur and using this information to eliminate possible keys.	2.83
ACTION TC-17	Truncated Differential Cryptanalysis	Focusing on partial differences in the plaintext and ciphertext to exploit structural properties of the cipher.	2.83

THREAT ID	THREAT NAME	THREAT DESCRIPTION	AGGREGATE RATING
ACTION TDS-01	TCP SYN Flood Attack	Overwhelms a target server by sending a rapid succession of SYN requests without completing the handshake, exhausting server resources and rendering it unresponsive.	2.83
ACTION TDS-02	UDP Flood Attack	Sends a large number of UDP packets to random ports on a target, causing the server to repeatedly check for applications listening at those ports and eventually become overwhelmed.	2.83
ACTION TDS-03	ICMP Flood Attack (Ping Flood)	Saturates the target with ICMP Echo Request (ping) packets, consuming both outgoing bandwidth and incoming processing resources, leading to a denial of service.	2.83
ACTION TDS-04	HTTP Flood Attack	Mimics legitimate HTTP GET or POST requests to attack a web server or application, exhausting resources and causing service degradation or failure.	2.83
ACTION TDS-05	Slowloris Attack	Maintains numerous simultaneous connections to the target web server by sending partial HTTP requests, keeping them open as long as possible and exhausting server resources.	2.83
ACTION TDS-06	Ping of Death Attack	Sends malformed or oversized ping packets to a target, causing buffer overflows and system crashes due to improper handling of such packets.	2.83
ACTION TDS-07	Smurf Attack	Exploits IP broadcast addressing by sending ICMP requests with a spoofed source IP of the target, causing multiple responses to flood and overwhelm the target system.	2.83
ACTION TDS-08	Fraggle Attack	Similar to a Smurf attack but uses UDP packets sent to broadcast addresses, causing multiple responses to flood the target and result in denial of service.	2.83
ACTION TDS-09	DNS Amplification Attack	Exploits open DNS resolvers by sending small queries with a spoofed source IP (the target's), resulting in large responses that overwhelm the target system.	2.83
ACTION TDS-10	NTP Amplification Attack	Leverages Network Time Protocol servers to send large responses to small requests with a spoofed source IP, flooding the target with unsolicited traffic.	2.83
ACTION TDS-11	Reflection Attack	Involves sending requests to a server with the source IP address spoofed to that of the target, causing the server to send responses to the target and overwhelm it.	2.83
ACTION TDS-12	Application Layer DDoS Attack	Targets specific features of an application, such as search functions or login processes, with the intent to exhaust server resources and disrupt legitimate user access.	2.83
ACTION TDS-13	Protocol Exploit Attack	Exploits weaknesses in network protocols (e.g., TCP/IP) to cause a target system to become unstable or crash, leading to a denial of service.	3.00
ACTION TDS-14	Resource Exhaustion Attack	Consumes finite resources such as CPU, memory, or disk space on a target system, leading to degraded performance or system crashes.	2.83
ACTION TDS-15	Malformed Packet Attack	Sends deliberately malformed packets that exploit vulnerabilities in the target's protocol stack, causing system instability or crashes.	3.00
ACTION TDS-16	Teardrop Attack	An attacker sends fragmented packets to the target machine, which the system cannot reassemble due to a bug in the TCP/IP fragmentation reassembly code, causing the system to crash or become unstable.	3.00

ACTION TDS-17	Reflective Amplification Attack	An attacker sends forged requests to servers that generate large responses, with the responses directed to the target, overwhelming its resources. This method amplifies the attack's impact.	2.83
ACTION TDS-18	Fragmentation Attack	An attacker sends fragmented packets that the target system cannot reassemble, causing it to become unstable or crash.	3.00
ACTION TDS-19	Botnet-Based Distributed DoS (DDoS)	An attacker uses a network of compromised computers (botnet) to launch a coordinated attack on a target system, overwhelming it with traffic from multiple sources and causing denial of service.	2.83
ACTION TDS-20	Permanent Denial of Service (PDoS)	An attacker damages the target system's hardware or firmware, rendering it permanently inoperable and requiring replacement or reinstallation.	3.17
ACTION TDS-21	Advanced Persistent DoS (APDoS)	An attacker conducts a prolonged and sophisticated denial of service attack, often combining multiple attack vectors and techniques, to exhaust the target's resources over an extended period.	2.83
ACTION TDS-22	HTTP Slow POST Attack	An attacker sends a complete, legitimate HTTP header but specifies a large 'Content-Length' field and then sends the body slowly, consuming server resources and potentially leading to denial of service.	2.83

CATEGORIES OF THREAT TO AN ORGANIZATION (IMPACTS)

In this next section of the whitepaper, we explore the potential impacts of cybersecurity threats on an organization, framing them within a categorized taxonomy. This approach is designed to provide a structured understanding of how an organization can be affected by cyber threats. Recognizing that each type of threat carries its own unique set of implications, our taxonomy aims to categorize these impacts broadly, enabling organizations better to assess their susceptibility to different kinds of cyber incidents.

The taxonomy of impacts is divided into categories that reflect the diverse consequences of cybersecurity threats, ranging from financial losses and operational disruptions to reputational damage and legal repercussions. This categorization is crucial for organizations in prioritizing their cybersecurity efforts, as it highlights the areas of most significant risk and potential damage. By understanding the possible impacts, organizations can tailor their cybersecurity strategies to mitigate the most critical threats, safeguarding their assets, reputation, and long-term viability in an increasingly digital world

THREAT ID	THREAT NAME	AGGREGATE RATING
IMPACT C-01	Confidentiality of Data or System Abused	2.0
IMPACT I-01	Integrity of Data or System Abused	3.0
IMPACT A-01	Availability of Data or System Abused	4.0
IMPACT P-01	Privacy of Data or System Abused	1.0

CONCLUSION

As we conclude this comprehensive exploration of cybersecurity threat taxonomies, it is imperative to recognize the dynamic and ever-evolving nature of the cybersecurity landscape. The taxonomy presented in this whitepaper serves as a fundamental tool for organizations to categorize and understand the multifaceted aspects of cyber threats systematically. This understanding is critical for developing effective defense strategies and fostering a culture of security awareness and resilience within organizations. By delving into the intricacies of threat agents, activities, and their impacts, we have laid out a structured framework that assists in identifying, analyzing, and prioritizing cybersecurity threats. This framework is essential for enabling organizations to allocate their resources effectively and tailor their cybersecurity measures to the threats they are most likely to encounter.

Introducing a threat rating system further enhances this taxonomy by providing a quantifiable approach to threat prioritization. Based on a consensus of expert opinions and real-world data, this system offers organizations a pragmatic method for assessing the urgency and severity of different cyber threats. It is a step towards a more objective and data-driven approach to cybersecurity, where decisions are made based on theoretical understanding and practical, evidence-based insights. As the digital threat landscape grows in complexity, such tailored and strategic approaches to cybersecurity become increasingly vital.

In conclusion, this whitepaper underscores the necessity of a collaborative and informed approach to cybersecurity. The insights and frameworks presented here culminate extensive research and collective expertise, reflecting the collaborative nature of cybersecurity defense. We encourage ongoing dialogue and knowledge sharing within the cybersecurity community to refine and update this taxonomy continually. As cyber threats evolve, so too must our strategies and defenses. This taxonomy will serve as a living document, adapting to new challenges and emerging threats and aiding organizations in their unceasing quest to safeguard their digital assets. In the face of an ever-changing cybersecurity landscape, preparedness, adaptability, and continuous learning remain our most potent weapons.

ABOUT US

The Cybersecurity Risk Foundation's (CRF) purpose is to encourage global collaboration and knowledge-sharing among cybersecurity professionals. Established with the missionto address the practical challenges of cybersecurity that organizations face, the CRF embodies a collective endeavor to fortify digital landscapes against ever-evolving threats. Our foundation is built on the principle that unity in action and thought can significantly impact cybersecurity, promoting safer and more resilient digital environments for businesses and institutions across various sectors.

At the heart of the CRF is a vibrant community of experts, practitioners, and thought leaders who bring a wealth of experience and insights from diverse cybersecurity fields. This rich tapestry of knowledge forms the foundation of our collaborative efforts to develop, refine, and disseminate practical strategies and solutions to common cybersecurity challenges. Through workshops, whitepapers, forums, and collaborative research initiatives, the CRF facilitates the exchange of ideas and best practices, encouraging innovation and continuous learning among its members. Our goal is to create a dynamic repository of cybersecurity knowledge that addresses current threats and anticipates future challenges, equipping organizations with the tools and strategies they need to navigate the digital age securely.

We invite cybersecurity professionals and organizations to join our mission, contribute to our body of knowledge, and engage in collaborative initiatives. Whether through sharing experiences, participating in discussions, or contributing to our ongoing research efforts, your involvement can make a significant difference. Together, we can create a powerful force for change, driving the advancement of cybersecurity practices and fostering a culture of security that transcends organizational boundaries. The CRF is more than just a foundation; it is a community of shared purpose committed to making the digital world a safer place for everyone.

BIBLIOGRAPHY

Acknowledging the significance of a collaborative approach in researching and categorizing cybersecurity threats is essential. The collective efforts and shared knowledge of researchers, cybersecurity experts, and organizations worldwide form the backbone of our understanding of this ever-evolving field. This section highlights various pivotal works and contributions that have shaped our current perspective on cybersecurity threats. By referencing these diverse sources, we pay homage to the collaborative nature of cybersecurity research and underscore the importance of continual learning and adaptation in developing comprehensive, effective cybersecurity strategies. Including these references is a testament to the value of a united front in the ongoing battle against cyber threats.

A few of the research efforts, not including the numerous cybersecurity threat reports published by various cybersecurity vendors, that most influenced this threat taxonomy are:

- CAPEC – Common Attack Pattern Enumeration and Classification (CAPECTM). (n.d.). Capec.mitre.org. https://capec.mitre.org/
- MITRE. (2023). MITRE ATT&CKTM. Mitre.org. https://attack.mitre.org/
- Threat Taxonomy. (n.d.). ENISA. Retrieved January 18, 2024, from https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
- Initiative, J. T. F. T. (2012, September 17). Guide for Conducting Risk Assessments. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/30/r1/final
- A Taxonomy of Operational Cyber Security Risks. (2010, November 30). Insights.sei.cmu.edu. https://insights.sei.cmu.edu/library/a-taxonomy-of-operational-cyber-security-risks/
- Cebula, J., Popeck, M., & Young, L. (2014). A Taxonomy of Operational Cyber Security Risks Version 2 CERT ® Division. https://insights.sei.cmu.edu/documents/2273/2014_004_001_91026.pdf
- Secretariat, T. B. of C. (2011, June 20). Guide to Risk Taxonomies. Aem. https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html
- Sheffi, Y. (2020). 2. Understanding Vulnerability. MIT Press on COVID-19. https://covid-19.mitpress.mit.edu/pub/bj6vpgnl/release/1

We hope that future versions of this taxonomy will reference even more projects dedicated to this task as the cybersecurity community continues to work together to address this issue.


CYBERSECURITY
RISK FOUNDATION