CRF – THREAT TAXONOMY (TT) 2024

THREAT TAXONOMY

CYBERSECURITY RISK FOUNDATION

TABLE OF CONTENTS

INTRODUCTION

The importance of preciseness and thoughtfulness in cybersecurity cannot be overstated. As organizations navigate through an often confusing myriad of directions they could take their cybersecurity programs, the specter of cybersecurity threats looms large, posing daunting challenges to the integrity and reliability of information systems. This whitepaper aims to dissect and categorize these threats, providing a structured framework to enhance the understanding and response to cyber risks. The rapid growth in the complexity and sophistication of cyber threats necessitates a comprehensive approach to their identification, classification, and mitigation. Our objective is to establish a taxonomy of cybersecurity threats that serves as a cornerstone for robust cybersecurity strategies, equipping organizations with the necessary insights to fortify their defenses in an increasingly interconnected world.

At the heart of effective cybersecurity management lies the precision in terminology and classification of threats. Misinterpretations or generalizations in understanding these threats can lead to inadequate or misaligned defense mechanisms. This paper addresses this gap by offering precise definitions and detailed classifications, ensuring a common language and understanding among all stakeholders, from technology professionals to executive management. We provide a holistic view of the cybersecurity landscape by meticulously categorizing threats into agents, activities, and impacts. This not only aids in identifying potential risks but also in prioritizing response strategies, thereby enhancing organizations' overall security posture.

Furthermore, the dynamic nature of cyber threats requires a proactive and preemptive approach. Introducing a systematic threat rating system in this whitepaper is a step towards prioritizing and managing the diverse threats identified. This system, based on extensive research and expert consensus, aids organizations in objectively assessing and focusing on the most pressing threats. As the digital realm continues to expand and integrate into every facet of business operations, our taxonomy strives to be an indispensable tool for organizations. It guides the development of comprehensive cybersecurity strategies tailored to each entity's unique needs and vulnerabilities. In essence, this whitepaper is not just an academic endeavor but a practical guide aimed at empowering organizations to navigate the complexities of cybersecurity and emerge resilient in the face of ever-evolving digital threats.

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.

A cybersecurity threat is 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."

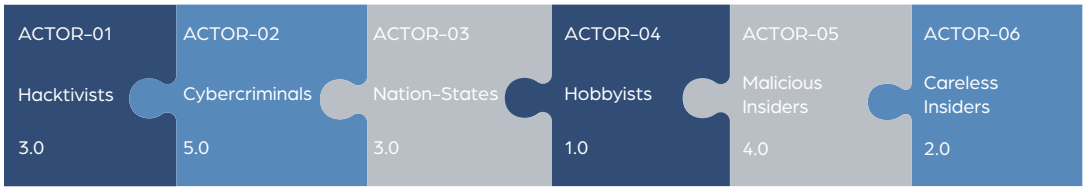
THREAT RATINGS

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 RATING
ACTOR-01	Hacktivists	3.0
ACTOR-02	Cybercriminals	5.0
ACTOR-03	Nation-States	3.0
ACTOR-04	Hobbyists	1.0
ACTOR-05	Malicious Insiders	4.0
ACTOR-06	Careless Insiders	2.0



CATEGORIES OF THREAT ACTIVITIES

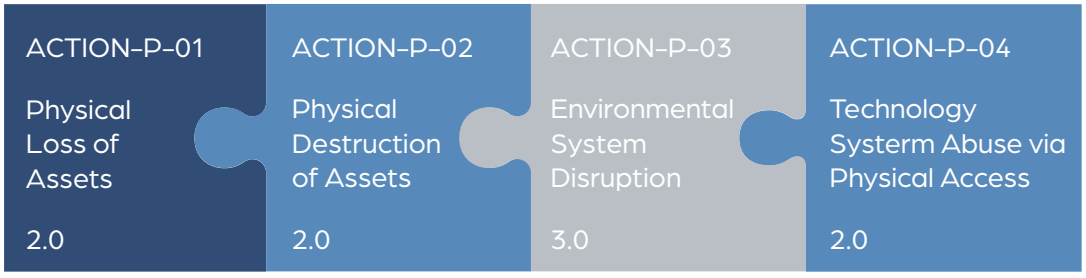
The following section focuses on threat actions, categorizing the specific methods threat actors use to cause potential harm to an organization's information systems. Understanding these methods is crucial for organizations to defend against cyber threats effectively and help organizations use technology 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

This section of the whitepaper addresses cybersecurity threats to an organization's information systems that originate from physical interactions. These threats encompass actions that could result in the theft, damage, or destruction of physical components of information systems.

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

THREAT ID	THREAT NAME	THREAT RATING
ACTION-P-01	Physical Loss of Assets	2.0
ACTION-P-02	Physical Destruction of Assets	2.0
ACTION-P-03	Environmental System Disruption	3.0
ACTION-P-04	Technology System Abuse via Physical Access	2.0

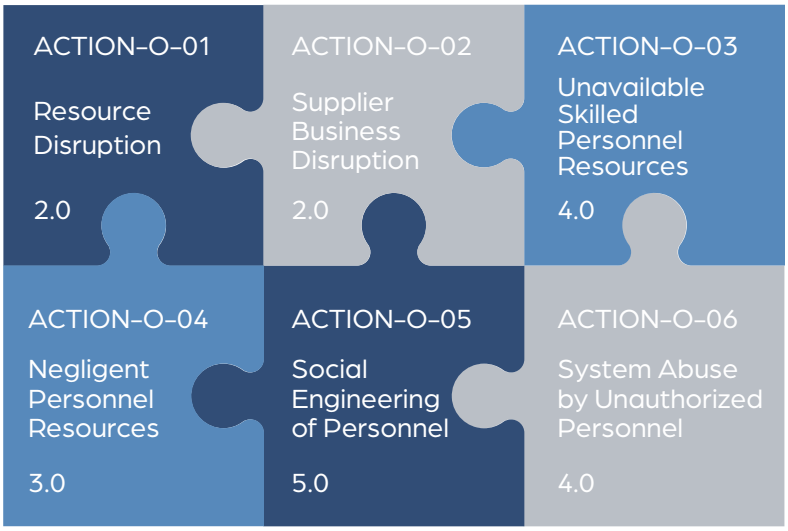


Operational Threats

This section focuses on cybersecurity threats to an organization's information systems caused by actions or failures of the organization's operational practices. These threats may arise from intentional and unintentional actions by staff members that lead to harm or compromise of the information systems.

The following is our taxonomy of operational threats to information systems:

THREAT ID	THREAT NAME	THREAT RATING
ACTION-O-01	Resource Disruption	2.0
ACTION-O-02	Supplier Business Disruption	2.0
ACTION-O-03	Unavailable Skilled Personnel Resources	4.0
ACTION-O-04	Negligent Personnel Resources	3.0
ACTION-O-05	Social Engineering of Personnel	5.0
ACTION-O-06	System Abuse by Authorized Personnel	4.0

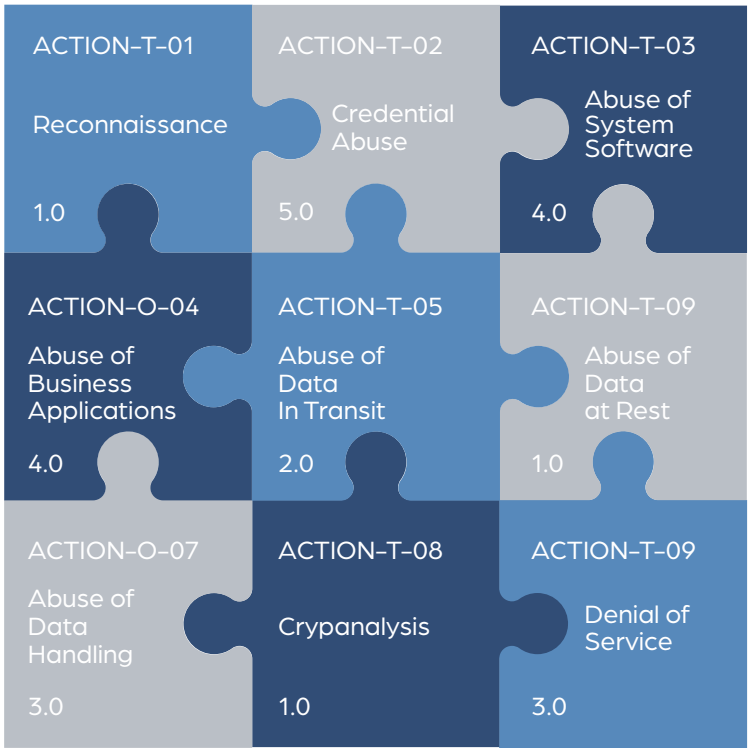


Technical Threats

This section delves into cybersecurity threats to an organization's information systems that are technical. These threats, often central in threat identification processes, encompass the range of technical actions executed by threat actors that potentially harm an information system.

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

THREAT ID	THREAT NAME	THREAT RATING
ACTION-T-01	Reconnaissance	1.0
ACTION-T-02	Credential Abuse	5.0
ACTION-T-03	Abuse of System Software	4.0
ACTION-T-04	Abuse of Business Applications	4.0
ACTION-T-05	Abuse of Data in Transit	2.0
ACTION-T-06	Abuse of Data at Rest	1.0
ACTION-T-07	Abuse of Data Handling	3.0
ACTION-T-08	Cryptanalysis	1.0
ACTION-T-09	Denial of Service	3.0

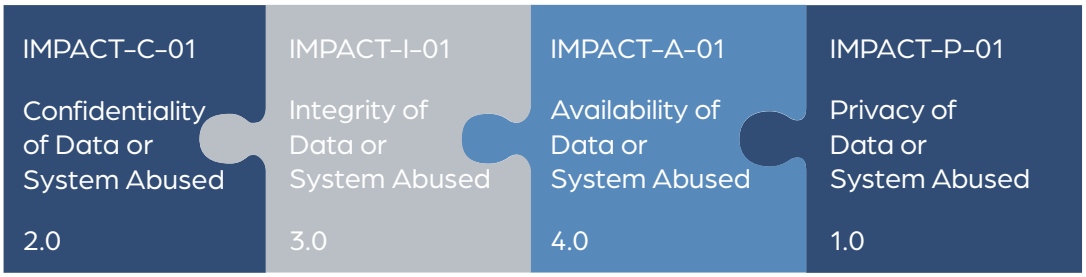


Categories of Threat to an Organization (Impacts)

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 clear and 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	THREAT 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 mission to 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®. 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

research@crfsecure.org • https://crfsecure.org