A Comprehensive Guide to the NIST Cybersecurity Framework 2.0

Strategies, Implementation, and Best Practice

Jason Edwards

WILEY

A Comprehensive Guide to the NIST Cybersecurity Framework 2.0

A Comprehensive Guide to the NIST Cybersecurity Framework 2.0

Strategies, Implementation, and Best Practice

Dr. Jason Edwards
Texas, USA

WILEY

This edition first published 2025

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty
While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data Applied for:
Hardback ISBN: 9781394280360

Cover Design: Wiley
Cover Image: © Yuichiro Chino/Getty Images

Set in 9.5/12.5pt STIXTwoText by Straive, Chennai, India

To my beloved family. To my mom and dad, who are no longer with us but whose love and guidance continue to inspire me every day. To my wife, Selda, and my children, Michelle, Chris, Ceylin, and Mayra, for your endless love, patience, and encouragement. To my close family members: Derek, Meltem, Nilos, and Ken. And to my sisters, Robin, Kelly, and Lynn. This book is dedicated to you, with all my love and gratitude.

Contents

Preface

In today's digital age, cybersecurity has become indispensable to our personal and professional lives. **As a cybersecurity professor and professional with over two decades of experience, I have witnessed firsthand the evolution of cyber threats and the relentless efforts to mitigate them.** This book is born out of my passion for cybersecurity and a deep understanding of organizations' complexities in safeguarding their digital assets.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) has emerged as a cornerstone in cybersecurity. Since its inception, it has provided a structured and flexible approach to managing and reducing cybersecurity risks. The NIST CSF 2.0 represents a significant leap forward, incorporating the latest advancements and addressing the dynamic nature of cyber threats.

This book is designed to be a comprehensive resource for understanding and implementing the NIST CSF 2.0. It delves into the intricacies of the framework, offering detailed explanations of its core components, functions, and implementation strategies. Whether you are a cybersecurity professional, a business leader, or an academic, this guide aims to equip you with the knowledge and tools necessary to enhance your organization's cybersecurity posture.

I have endeavored to make this book accessible to a broad audience, from beginners to seasoned professionals. The language is clear and jargon-free, making complex concepts understandable. At the same time, the depth of coverage ensures that even those with advanced knowledge will find valuable insights.

In writing this book, I have drawn upon my extensive experience and the collective wisdom of cybersecurity experts and practitioners. The practical recommendations, case studies, and actionable advice included herein will bridge the gap between theory and practice, helping organizations implement the NIST CSF effectively and efficiently.

Cybersecurity is a continuous journey, and this book is a step toward mastering it. I invite you to embark on this journey with me, armed with the knowledge and confidence to navigate the ever-changing cyber threat landscape.

July, 2024

Jason Edwards
Texas, USA

Acknowledgments

I am deeply grateful to all those who have contributed to the creation of this book. This endeavor would not have been possible without the support, guidance, and encouragement of many individuals.

First and foremost, I would like to express my heartfelt appreciation to my family for their unwavering support and understanding throughout the writing process. To my wife, Selda, and my children, Michelle, Chris, Ceylin, and Mayra, your patience and encouragement have been my anchor. I am also thankful for the love and support from my extended family: Derek, Meltem, Nilos, Ken, and my sisters Robin, Kelly, and Lynn.

I am indebted to the organizations that have been pivotal in my professional development and the success of this book: Hallmark University, ThriveDX, Cybrary, and the LinkedIn subscribers to the Cyberspear newsletter that I operate.

I extend my gratitude to the following individuals for their insights, support, and encouragement:

Griffin Weaver, Seth Jaffe, Kurt Lubelan, Kim Kemp, Rob Fisher, Don Wuebben, Amy Read, Derek Burkes, Wendell Ladd, Wil Bennet, Ken Hamilton, Clarke Cummings, Gary McAlum, Amil Navarro, Joe Dubbs, Brennan Holland, Ann Kurtz, Allison Carrillo, Brady Justice, Jeff Spaeth, Kristyn Lette, Chinho Ko, Subash Poudyal, PhD, Kul Subedi, PhD, Jim Huseman, Gordon Bjorman, Dr. Angela Dogan, Jerry Smith, Dr. Patrick Woods, Jason Raab, Ankit Kalra, Leead Negri, Kesha Lindbergdashwork, Michael Castillo, Kelley Dadah, Luis Guillermo, Christopher Hickernell, Janice Pryor, Brett Wahlin, James Azar, Michelle Nasser, Luis Gutierrez, Marco Bart.

Your contributions have been invaluable, and I am immensely grateful for your support.

1

Introduction

Understanding the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) can be daunting for many. Its complexity often appears cryptic, bordering on magical for some, yet it is neither. The essence of this book is to demystify the NIST CSF, making it accessible and actionable for businesses of all sizes. It is crafted to serve as a bridge between the high-level guidelines of the NIST CSF and the practical needs of organizations striving to enhance their cybersecurity posture.

This guide is designed for a broad audience, from small businesses to large corporations. The scalability and adaptability of the NIST CSF are among its core strengths, allowing organizations to implement cybersecurity practices that align closely with their specific operational needs and risk profiles. This book will give readers insights into customizing and applying the Framework to best serve their unique circumstances.

Flexibility is a central theme throughout this guide. The cybersecurity controls and recommendations provided herein are meant to be adapted and modified to fit different organizations' specific needs and contexts. This approach encourages readers to think critically about how each control can be tailored to support their cybersecurity goals, reinforcing that there is no one-size-fits-all solution in cybersecurity.

The structure of this book mirrors the practical, hands-on approach to cybersecurity management. Each section within the chapters is designed to introduce one to three controls, accompanied by four to six actionable recommendations. These are crafted to provide readers with clear, actionable steps to improve their cybersecurity measures, making the content directly applicable to their daily operations.

It is important to note that the NIST CSF does not maintain a continuous numbering system for its categories and subcategories; some numbers are intentionally skipped due to their deprecation. This should not be seen as an error or oversight but as an intentional aspect of the Framework's design. The missing numbers highlight the Framework's evolution and adaptability to the changing cybersecurity landscape.

This book is intended to be a practical guide, not an exhaustive academic exploration of the NIST CSF. The aim is to equip readers with the knowledge and tools they need to effectively implement and benefit from the Framework rather than to showcase the historical development of the NIST standards or the technical prowess of its authors.

Adherence to any framework, including the NIST CSF, should not be rigid. This guide emphasizes the importance of tailoring the Framework to meet your organization's needs and circumstances. The goal is to use the NIST CSF as a foundation to build an effective and flexible cybersecurity strategy.

A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice, First Edition. Jason Edwards.

Finally, this book advocates for the principle of reiteration rather than duplication. It is designed to serve as a reference guide that can be consulted repeatedly, offering practical advice and insights rather than a novel narrative. The concise and direct nature of the recommendations and controls presented is intentional, aiming to provide clear guidance without unnecessary complexity. This approach underscores the book's overarching message: the value of pragmatic, adaptable cybersecurity practices that can be tailored to each organization's unique needs.

Why This Book?

The cybersecurity threat landscape is evolving at an unprecedented rate, with new vulnerabilities and attack vectors emerging continuously. This dynamic environment poses a significant challenge for organizations across all sectors, necessitating a robust approach to cybersecurity defense mechanisms. This book is a response to these challenges, offering a comprehensive exploration of the NIST Cybersecurity Framework as a pivotal tool in the fight against cyber threats. It aims to provide readers with a deep understanding of the Framework's structure and how it can be effectively implemented to safeguard digital assets.

Bridging knowledge gaps in cybersecurity practices is a core mission of this guide. Many organizations are disadvantaged, not due to a lack of effort or investment in cybersecurity but because of a fundamental misunderstanding or misapplication of critical principles and practices. This book seeks to rectify this issue by delivering clear, concise, and actionable information on the NIST Cybersecurity Framework, ensuring that readers can understand and apply these practices in a way that significantly boosts their cybersecurity posture.

Frameworks play a crucial role in establishing a comprehensive cybersecurity strategy. They provide a structured and systematic approach to managing and mitigating cyber risks. Among these, the NIST Cybersecurity Framework stands out for its flexibility, comprehensiveness, and adaptability to organizations of various sizes and industries. This book highlights the importance of such frameworks in responding to cyber incidents and fostering a culture of proactive cyber hygiene that can significantly reduce the likelihood and impact of cyberattacks.

This book distinguishes itself through its unique approach to discussing the NIST Cybersecurity Framework. Unlike other texts offering a superficial overview or a highly technical analysis, this guide balances depth and accessibility. It is designed to be of value to cybersecurity professionals while remaining approachable for those new to the field. The book's contributions lie in its practical recommendations, detailed breakdown of the Framework's components, and emphasis on real-world applicability.

Addressing the growing complexity of cybersecurity threats requires more than just theoretical knowledge; it demands a practical understanding of how frameworks like the NIST Cybersecurity Framework can be leveraged in real-world scenarios. This book bridges theory and practice, providing readers with the insights needed to transform their cybersecurity strategies from reactive to proactive.

By focusing on the NIST Cybersecurity Framework, this book fills a critical need for authoritative guidance on one of the world's most respected and widely adopted cybersecurity frameworks. The Framework's emphasis on continuous improvement, risk management, and adaptability makes it an invaluable tool for organizations seeking to navigate the complexities of today's cybersecurity landscape.

The practical applications of the NIST Cybersecurity Framework are vast, extending beyond mere compliance to drive meaningful improvements in cybersecurity practices. This book delves into

these applications, offering readers a clear path to understanding the Framework and using it to make tangible improvements to their cybersecurity defenses. It underscores the Framework's role as a set of guidelines and a catalyst for change in how organizations approach cybersecurity.

Finally, this book is an invitation to view cybersecurity through the lens of continuous improvement and strategic alignment. The NIST Cybersecurity Framework is not a static set of recommendations but a living document that evolves in response to new threats and technological advancements. By embracing the Framework's principles, organizations can enhance their cybersecurity posture and align their cybersecurity strategies with their broader business objectives, ensuring that cybersecurity is not just a technical necessity but a strategic asset.

Overview of Cybersecurity Challenges

The cybersecurity landscape is increasingly complex, characterized by various sophisticated threats that target every aspect of the digital environment. From advanced persistent threats to ransomware, phishing, and zero-day exploits, the variety and sophistication of these cyber threats pose a constant challenge to organizations. This complexity is further amplified by the rapid pace of technological advancements and the expanding digital footprint of businesses, making securing digital assets an ever-evolving battle.

Businesses and government sectors share common vulnerabilities that cyberattackers frequently exploit. These vulnerabilities often stem from outdated systems, unpatched software, insufficient network security practices, and employees' lack of cybersecurity awareness. The interconnected nature of digital systems means that a breach in one area can quickly escalate, affecting critical infrastructure, data integrity, and the confidentiality of sensitive information. This shared risk landscape underscores the need for comprehensive and adaptable cybersecurity strategies to protect against known and emerging threats.

The cost of cyber incidents to organizations extends beyond the immediate financial losses associated with data breaches or ransom payments. The long-term repercussions include damage to reputation, loss of customer trust, legal penalties, and the significant resources required for incident response and recovery. The intangible costs, such as the impact on employee morale and the loss of competitive advantage, can also be substantial. These factors together highlight the critical importance of implementing robust cybersecurity measures to mitigate the risk of cyber incidents.

Failure to implement a comprehensive cybersecurity framework like the NIST Cybersecurity Framework can severely affect organizations. Without the structured approach and best practices provided by such frameworks, organizations are often ill-prepared to identify, protect against, detect, respond to, and recover from cybersecurity incidents. This lack of preparedness can lead to increased vulnerability to cyberattacks, potentially resulting in devastating data breaches, financial losses, and erosion of stakeholder trust.

A cohesive cybersecurity strategy can impede an organization's ability to manage and respond to cyber incidents effectively. Without clear guidelines and protocols, the response to cybersecurity threats can be slow and disorganized, allowing attackers more time to exploit vulnerabilities and cause damage. This situation highlights the value of the NIST Cybersecurity Framework's structured approach to managing cyber risks and enhancing an organization's cybersecurity posture.

Organizations that neglect to implement the NIST Cybersecurity Framework may also find themselves at a competitive disadvantage. In an era where cybersecurity is a critical concern for customers and business partners, demonstrating a commitment to cybersecurity through adherence to recognized frameworks can be a significant competitive edge. Moreover, regulatory

compliance requirements are increasingly mandating the adoption of such frameworks, and failure to comply can result in legal and financial penalties.

The strategic alignment of cybersecurity practices with business objectives is another critical aspect that can be compromised without the guidance of the NIST Cybersecurity Framework. Cybersecurity is not just a technical issue but a business imperative that affects every aspect of an organization's operations. A framework-based approach ensures that cybersecurity measures are effective and aligned with the organization's goals, risk tolerance, and operational requirements.

In conclusion, the challenges the modern cybersecurity landscape poses are significant but not insurmountable. The NIST Cybersecurity Framework offers an adaptable strategic roadmap for organizations to enhance their cybersecurity defenses, manage cyber risks, and maintain resilience against cyber threats. The consequences of not implementing such a framework can be severe, affecting an organization's financial health, reputation, and operational capability. Therefore, adopting and adapting the NIST Cybersecurity Framework is essential for any organization committed to safeguarding its digital assets and maintaining trust in an increasingly digital world.

2

Understanding the NIST Cybersecurity Framework 2.0

The National Institute of Standards and Technology (NIST) Cybersecurity Framework represents a paradigm shift in national and organizational approaches to cybersecurity. Initially conceptualized to improve the cybersecurity postures of critical infrastructure entities, the Framework has universally been recognized for its adaptability and effectiveness across various sectors. This adaptability is rooted in its design, which allows organizations of different sizes, from small local businesses to global enterprises, to apply the Framework tailored to their unique risk environments and cybersecurity challenges.

Understanding the historical context of the NIST Cybersecurity Framework is essential. It was developed in response to increasing and evolving cyber threats facing organizations and national infrastructure. The Framework's purpose was to create a common language and systematic methodology for managing cybersecurity risk, emphasizing the importance of cybersecurity to the national and economic security of the United States and beyond. This emphasis on a unified approach has facilitated better communication and understanding among stakeholders across different sectors.

The NIST Cybersecurity Framework is built on key principles and objectives to enhance organizations' ability to manage and reduce cybersecurity risks. These principles encourage a holistic view of cybersecurity, integrating it into the organization's overall risk management processes. The Framework's objectives serve as guideposts for organizations, aiming to transform reactive, disjointed responses into a proactive, strategic, and coherent cybersecurity posture.

The Framework's scope and applicability are deliberately broad, designed to be relevant across different sectors, and adaptable to varying organizational sizes and complexities. This universal applicability ensures that the Framework can serve as a foundational tool for entities in industries diverse in energy, healthcare, finance, and education, irrespective of their current cybersecurity maturity.

A critical aspect of the NIST Cybersecurity Framework is its ability to complement other standards and practices. This attribute is precious for organizations that have invested in cybersecurity measures or are bound by sector-specific regulations. By providing a high-level, strategic view of cybersecurity risk management, the Framework can help harmonize existing efforts, making them more effective and cohesive.

The Framework encourages organizations to adopt a continuous improvement approach to cybersecurity, emphasizing the dynamic nature of cyber threats and the need for ongoing assessment and adaptation of cybersecurity practices. This approach helps organizations respond to incidents and anticipate and mitigate potential threats before they can impact the organization.

A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice, First Edition. Jason Edwards.

Integration of the NIST Cybersecurity Framework into organizational processes can dramatically enhance not only the security but also the resilience of organizations. By providing a structured yet flexible approach, the Framework helps entities develop a cybersecurity strategy that aligns with business objectives, addresses relevant risks, and leverages existing practices and investments.

Finally, the widespread adoption and endorsement of the NIST Cybersecurity Framework underscore its significance and utility in improving national and organizational cybersecurity postures. By fostering a shared understanding and approach to managing cybersecurity risk, the Framework has become an essential resource for organizations seeking to navigate the complex and evolving cybersecurity landscape.

Fundamental Changes from Version 1.X

The evolution from NIST CSF 1.X to 2.0 represents a significant leap forward in addressing the complexities of modern cybersecurity landscapes. This update reflects the collective insights and experiences of a broad range of stakeholders, incorporating the latest best practices and addressing emerging threats. The revisions ensure that the Framework remains a cutting-edge tool for managing cybersecurity risk, adaptable to the rapid changes in the cyber domain.

One of the most significant updates in Version 2.0 is refining the core functions and categories. This addressed the evolving nature of cyber threats and the increasing sophistication of cyberattackers. The updates enhance the clarity and applicability of the Framework, ensuring that it aligns with current cybersecurity challenges and technologies. These changes encourage a more intuitive and practical application of the Framework across different organizational contexts.

The modifications to the implementation tiers are particularly noteworthy. These changes are designed to guide organizations in evolving their cybersecurity practices from reactive to proactive stances. The revised tiers help organizations better understand their cybersecurity maturity levels and provide a more straightforward path for advancement, emphasizing risk management and resilience.

Enhancements in communication and information sharing reflect the growing recognition of the importance of collaboration in cybersecurity. The updated Framework underscores the need for effective communication among internal and external stakeholders, facilitating a more coordinated and agile response to cybersecurity threats. This focus on information sharing is critical in an era where threats can evolve rapidly and spread across organizational and national boundaries.

The introduction of new recommendations for supply chain risk management is a response to the increasing interconnectedness of organizations and the recognition that a chain is only as strong as its weakest link. The updates guide assessing and managing the cybersecurity risks associated with suppliers and partners, an area highlighted by several high-profile breaches.

The changes from Version 1.X to 2.0 also include a more explicit emphasis on privacy and civil liberties, reflecting growing concerns about the balance between security and individual rights. This inclusion demonstrates the Framework's adaptability to broader societal and regulatory changes and underscores the importance of considering these factors in cybersecurity practices.

The revision process also introduced new elements to enhance organizations' resilience to cyber incidents. This resilience is not merely about preventing breaches but ensuring that an organization can operate effectively during and after a cyber event. The updated Framework emphasizes not just the technical aspects of cybersecurity but also the need to incorporate business continuity and recovery planning into the overall cybersecurity strategy.

Furthermore, the updated NIST CSF encourages a more integrated cybersecurity and business strategy approach. Organizations can ensure that cybersecurity measures contribute to overall business performance and value creation by aligning cybersecurity objectives with business goals. This alignment is critical in today's environment, where cybersecurity is not just an IT issue but a strategic business concern.

Lastly, the transition to Version 2.0 highlights the importance of adaptability and customization in cybersecurity. The updated Framework provides a more nuanced approach to applying its principles, recognizing that each organization's cybersecurity needs and challenges are unique. It emphasizes the importance of tailoring the Framework to fit an organization's specific context and risk profile, thereby making it a more effective tool for managing cybersecurity risks.

Core Components of the Framework

The NIST Cybersecurity Framework is structured around core components that offer a comprehensive approach to managing cybersecurity risk. These components are Functions, Categories, and Subcategories, which provide a framework for organizing and sustaining an organization's cybersecurity activities. Understanding and implementing these core components is fundamental to leveraging the Framework effectively.

The Functions provide a high-level organizational view of the lifecycle of managing cybersecurity risks. They encompass Identify, Protect, Detect, Respond, and Recover, creating a strategic foundation for developing a comprehensive cybersecurity program. This structure supports a continuous feedback loop for ongoing improvement, ensuring that cybersecurity measures evolve in line with the changing threat landscape and business requirements.

Categories and Subcategories further break down these Functions into more specific objectives, offering a detailed and actionable approach to achieving the broader outcomes defined by the Functions. Each Category addresses a particular aspect of cybersecurity, such as Asset Management or Access Control. At the same time, Subcategories provide specific targets for each Category, such as establishing data classifications or implementing least privilege principles.

Informative References are another crucial component, offering guidance and resources for achieving the objectives in the Subcategories. These references include industry standards, guidelines, and best practices, providing a rich repository of information to help organizations implement the Framework effectively. They serve as a bridge between the high-level guidance provided by the Framework and the specific actions needed to implement it.

Customization is a fundamental feature of the NIST Cybersecurity Framework, allowing it to be adapted to the diverse needs and circumstances of different organizations. The Framework can be tailored to various sectors, risk environments, and business models, making it a versatile tool applicable to multiple entities. This adaptability is crucial for ensuring the Framework remains relevant and practical across different contexts and industries.

The Framework's integration with existing compliance requirements demonstrates its flexibility and utility. Organizations can align their NIST CSF implementation with other regulatory and industry-specific requirements, streamlining compliance efforts and reducing redundancy. This integration ensures that cybersecurity measures are not just about meeting regulatory obligations but are embedded into the organization's overall risk management strategy.

Overall, the core components of the NIST Cybersecurity Framework form a cohesive and comprehensive approach to cybersecurity. By understanding and applying these components,

organizations can develop a robust cybersecurity program that protects against threats, supports their business objectives, and fosters resilience in the face of cyber incidents.

The Functions: Govern, Identify, Protect, Detect, Respond, and Recover

The Govern function is essential for establishing and maintaining a framework for managing cybersecurity risk aligned with organizational strategies and objectives. It involves the development of policies, processes, and standards that guide the organization's cybersecurity efforts, ensuring they are integrated with overall governance structures. This function emphasizes the importance of senior leadership commitment and oversight in fostering a culture of cybersecurity throughout the organization.

Effective governance requires clear communication, defined roles and responsibilities, and regular evaluation of cybersecurity policies and practices. It also involves considering cybersecurity in the context of other business risks, ensuring it is an integral part of the organization's overall risk management framework. This holistic approach helps ensure that cybersecurity investments are aligned with business priorities and effectively mitigate risks.

The Identify function is foundational to effective cybersecurity management. It involves understanding the organization's business context, resources, and cybersecurity risks. This function is critical for identifying the assets, systems, and data that need protection and understanding the threat landscape and the organization's vulnerabilities.

Asset management, risk assessment, and risk management strategies are core components of the Identify function. They enable organizations to prioritize their cybersecurity efforts based on specific risks, vulnerabilities, and business imperatives. This targeted approach ensures that resources are allocated effectively and that the organization's cybersecurity measures are commensurate with the level of risk.

The Protect function is about implementing appropriate safeguards to ensure the delivery of critical services. This includes measures to control access to assets, protect data integrity and confidentiality, and maintain secure environments for information processing. The Protect function covers a broad range of activities, from identity management and access control to data encryption and maintenance of security technologies. It is about creating a barrier against threats while ensuring business operations can continue unimpeded. This function also involves employee training and awareness, as human factors are crucial in maintaining a secure environment.

Effective protection strategies require a layered approach, combining physical, technical, and administrative measures. This multifaceted strategy ensures that if one line of defense fails, others are in place to mitigate the risk. Regular updates and patches to security systems and continuous monitoring for anomalies are essential practices within the Protect function to keep defenses robust and responsive to emerging threats.

The Detect function is critical for promptly identifying the occurrence of a cybersecurity event. This function is rooted in the understanding that no defense can be foolproof. Therefore, continuous monitoring and detection processes are essential to identify and mitigate threats as soon as they emerge. This involves deploying advanced threat detection technologies, regular system, and network analysis, and establishing baseline behaviors for anomaly detection.

Timeliness and accuracy are key in the Detect function, as early detection can significantly reduce the impact of a cyber incident. Organizations need to establish and maintain detection