ActualTech Media

UncommonX

How the NIST Cybersecurity Framework Improves Risk Strategies

Lawrence Miller

CONTENTS

IN THIS PAPER

Discover how small and midsize businesses can reduce risk and implement enterprise-class security—without the cost and complexity of enterprise security operations.

Highlights include:

- Properly identifying and implementing appropriate security measures
- Outlining appropriate safeguards to ensure delivery of critical services
- Developing and implementing the appropriate activities to quickly identify the occurrence of a cybersecurity event
- The recovery activities that need to occur during and after an incident

The U.S. National Institute of Standards and Technology (NIST) has developed a Cybersecurity Framework offering organizations a simplified set of security controls that could be adopted to achieve a reasonable (that is, minimal) level of effective security controls. This framework has been broadly adopted across many different industries and businesses in recent years. It's a flexible and intuitive process built on five core functions of cybersecurity: Identify, Protect, Detect, Respond, and Recover (see **Figure 1**).

In this brief, we'll take a closer look at the five core functions defined in the NIST Cybersecurity Framework, as well as the categories within each function and how to apply the framework to your business risk strategy. Whether companies develop and implement a cybersecurity program in-house or outsource it to a managed security services provider (MSSP) or managed detection and response (MDR), it's important to ensure that the program follows these guidelines.

Identify

The purpose of the Identify function, according to NIST, is to "develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities." Part of that organizational understanding is visibility into what you have; it's difficult to protect something if you don't know you have it.

For an effective risk strategy, organizations need to have clear visibility to the organization's business objectives and the IT that supports those objectives. You must define and implement policies, procedures, and processes (better known as governance), while understanding and addressing risk (the categories of risk assessment and risk management, respectively). Finally, you must understand your role in the supply chain, as well as the upstream and downstream risks in your supply chain (this is supply chain risk management).

ASSET MANAGEMENT

Asset management is a critical first step in any organization's risk strategy, and that calls for a complete and accurate inventory of all your assets. Your assets can include hardware (both physical and virtual), communications (that is, telecommunications services), software, and data. A complete inventory of your assets ensures that you can identify your entire attack surface and drives other key activities, such as risk assessment, risk management, vulnerability management, and business continuity planning, to name a few.

The concept of asset management may seem simple and straightforward, but for many organizations it poses a significant challenge. It's actually quite difficult to ensure complete visibility across an entire hybrid digital landscape—spanning on-premises, multi-cloud, and

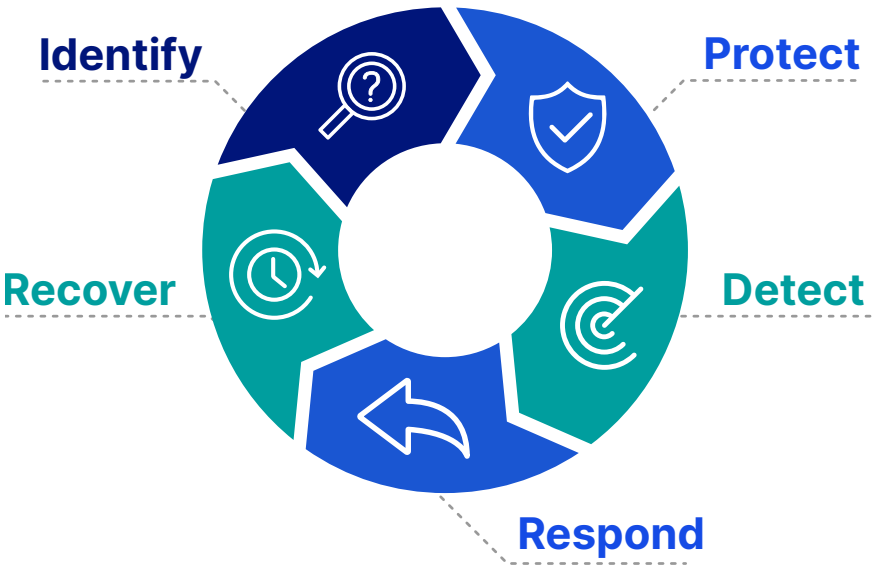

Figure 1: The five core functions of the NIST Cybersecurity Framework

remote/home office environments. For example, it's easy to overlook virtual assets, both on-premises and in the cloud. This is particularly true of ephemeral assets associated with container technologies and the microservices architecture used in modern, cloud-native applications.

> **For an effective risk strategy, organizations need to have clear visibility to the organization's business objectives and the IT that supports those objectives.**

In addition to knowing what assets must be protected, you need to prioritize your organization's assets based on classification levels, criticality, and business value. This information will help to inform such things as your risk assessments, security investment decisions, and business continuity/disaster recovery planning.

BUSINESS ENVIRONMENT

Security is a business problem that requires commitment from different stakeholders and leaders throughout your company to create and maintain a business environment that effectively addresses risk.

GOVERNANCE

Effective governance ensures that everyone in the organization understands their respective roles and responsibilities as it pertains to securing business processes and supporting IT. Your governance informs decisions and actions, and should be aligned to any applicable legal and regulatory requirements for your industry regarding cybersecurity and privacy.

RISK ASSESSMENT

Businesses must continuously identify, assess, and respond to risk, because business conditions continually change and the threat landscape evolves rapidly. The Cybersecurity Framework addresses the importance of knowing what you're protecting (that's asset management, as covered earlier). And the framework calls on you to identify threats to internal and external resources, look for vulnerabilities within assets, predict likelihoods and frequencies of occurrence, consider business impacts, and take care of risk treatment (which is also known as risk analysis).

Risk treatment options include:

- **Risk mitigation:** This means implementing one or more policies, controls, or other measures to protect an asset. The goal is to reduce the probability that the threat will be realized or reduce the impact of a realized threat to a level that the organization finds acceptable.
- **Risk assignment:** Here's where you transfer the liability for potential loss associated with a given risk to a third-party, such as an insurance carrier or service provider.
- **Risk avoidance:** You can eliminate a risk altogether by either getting rid of the asset or eliminating the condition that introduced the risk.
- **Risk acceptance:** You're formally acknowledging and accepting the potential loss associated with a given risk.

RISK MANAGEMENT STRATEGY

Risk management aligns your vulnerability and risk analysis to your cybersecurity investments and activities. It's an ongoing process that ensures your business can quickly and effectively adapt to a changing risk profile. An effective risk-management program helps ensure your business understands its risks and can make informed, business-centric decisions about cybersecurity investments and activities.

Due diligence is an important concept in risk management, requiring organizations to formally assess risk and the available risk treatment options for a given asset. It's essentially an exercise in cost-benefit analysis. If the cost to implement a policy, control, or other measure (such as a technology solution) is less than the potential loss or impact associated with a given risk, due diligence requires the organization to implement the risk treatment option.

SUPPLY CHAIN RISK MANAGEMENT

Recent attacks against SolarWinds, Colonial Pipeline, and JBS have brought supply chain risk management to the forefront, but the supply chain has long been a potential vulnerability. Organizations must recognize and implement appropriate security measures across the supply chain, and that includes a focus on vendors that provide not only goods but also services on which you rely. For example, the Target data breach of 2013 was the result of a vulnerability exploit in a third-party vendor's software used to remotely manage Target's heating, ventilation, and air conditioning and refrigeration systems.

Protect

The second function of the Cybersecurity Framework, known as Protect, outlines appropriate safeguards to ensure delivery of critical infrastructure services. It supports the ability to limit or contain the impact of a potential cybersecurity event.

> **Identity management and access control has taken on increased importance lately, as the widespread adoption of cloud technologies has been eliminating many of the traditional network perimeters**

Categories within the Protect function include identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

IDENTITY MANAGEMENT AND ACCESS CONTROL

This category addresses the need for proactive management of identities and credentials. It includes issuing, managing, verifying, revoking, and auditing credentials for authorized users, as well as for devices and processes. Among other things, it also covers physical and remote access, network segmentation, and permissions management based on the principles of least privilege and separation of duties.

Identity management and access control has taken on increased importance lately, as the widespread adoption of cloud technologies has been eliminating many of the traditional network perimeters that have been protecting the assets on a corporate network from external Internet threats by means of a firewall. The global pandemic has greatly accelerated this trend by forcing many organizations to support work-from-home (WFH) and work-from-anywhere (WFA) models. Thus, identity management has truly become the new perimeter, and threat actors know this. The majority of breaches today are the result of stolen or otherwise compromised credentials associated with authorized users.

AWARENESS AND TRAINING

The need for proactive end-user security awareness and training is well recognized by most organizations, but this training isn't always effectively implemented. Business email compromise, phishing, and ransomware attacks target end users who may be oblivious to the risks to their organization. This category addresses the need for awareness training for everyone, including end users, privileged users, security staff, executives, and third parties such as suppliers, customers, and partners. All players need to understand the risks, as well as individual roles and responsibilities.

Security awareness and training also helps you to ensure your security staff stays on top of the latest tactics, techniques, and procedures (TTPs) used by threat actors. It enables you to identify gaps in security skillsets that may potentially require additional training or staff.

DATA SECURITY

This category addresses data encryption at rest, in use (or "in process"), and in transit; data lifecycle management; capacity planning; data leak protection; data integrity; and the need to separate development, testing, and production environments.

INFORMATION PROTECTION PROCESSES AND PROCEDURES

An effective risk strategy requires an appropriate balance of people, processes, and technology. Your focus on information protection processes and procedures establishes security baselines and implements a formal systems development lifecycle. It also ensures operational best practices including configuration management, change management, backup and recovery, and data destruction. And it addresses the need for the following:

- Continuous improvement
- Threat intelligence sharing
- Vulnerability management
- Incident response, business continuity, and disaster recovery planning and testing

MAINTENANCE

The Maintenance category helps organizations ensure that local and remote maintenance is performed in a secure manner. This is particularly important given the prevalence of supply chain attacks.

> **An effective risk strategy requires an appropriate balance of people, processes, and technology.**

PROTECTIVE TECHNOLOGY

Organizations need to focus on correctly implementing and maintaining the right protective tools. This includes managing audit trails and logging, implementing the principle of lease functionality, protecting communications and control networks, and ensuring resilience.

Detect

Third on the list of key functions is Detect, helping organizations develop and implement the appropriate activities to quickly identify the occurrence of a cybersecurity event. Many cybersecurity incidents go unnoticed for months, allowing hackers ample time to explore your networks, locate sensitive information, and then slowly and carefully exfiltrate it.

ANOMALIES AND EVENTS

Organizations must ensure they have adequate resources, whether internal or external, to respond to potential threats and actual events. This includes establishing security baselines, analyzing detected events to understand TTPs, collecting telemetry across multiple sources throughout the environment, determining the impact of events, and creating alert thresholds.

SECURITY CONTINUOUS MONITORING

This category establishes the need for organizations to maintain 24/7/365 monitoring capabilities, whether in-house or through a third party (such as an MSSP).

DETECTION PROCESSES

This category ensures that an organization's resources know what they must do when a potential threat is identified or a security event has occurred. Detection processes must be regularly tested for effectiveness, and continuously improved.

Respond

The fourth function is Respond, which focuses on the appropriate activities to undertake when a cybersecurity incident is detected, so that your organization is able to contain the impact. Examples of categories within this function include response planning, communications, analysis, mitigation, and improvements.

RESPONSE PLANNING

Effective incident response begins with an incident response plan that has been regularly tested. All members of the incident response team must understand their roles and responsibilities during and after a cybersecurity incident.

The Colonial Pipeline ransomware attack is a good example of effective incident response planning. Of

course, there were lessons to be learned and improvements to be implemented, but the incident was quickly identified, critical systems were isolated, and the CEO was promptly notified and provided the information needed to make important decisions.

COMMUNICATIONS

Communications, both during and after an incident, are critical to effective incident response. This includes communications with both internal and external stakeholders, as well as customers, partners, and law enforcement.

> **Communications, both during and after an incident, are critical to effective incident response.**

Quickly and accurately identifying the scope and impact of a security incident is also critical. In some cases, organizations may be legally required to notify customers and partners of a data breach within a specified time period. Regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the EU General Data Protection Regulation (GDPR) impose specific breach notification requirements and strict penalties for non-compliance.

At the same time, if an organization can quickly determine that—through effective containment or strong encryption—sensitive data has *not* been compromised, it may be possible to avoid disclosing. If an incident has no real impact to customers and partners, avoiding disclosure saves embarrassment and potential reputation damage.

ANALYSIS

Analysis is conducted to ensure effective response and to support recovery activities. Such activities include conducting forensic investigation, determining the scope and impact of incidents, appropriately categorizing incidents, and performing containment and mitigation activities to resolve the incident and prevent an event from expanding.

MITIGATION

This category requires that incident response teams know how to respond to potential threats and tactical events and includes containment and mitigation activities.

IMPROVEMENTS

Finally, it's vital to identify relevant lessons taught by actual incidents, and also ensure that incident response plans are always kept up to date.

Recover

Recover is the last function in the NIST Cybersecurity Framework. It addresses the recovery activities that occur during and after an incident, through the execution of business continuity and disaster recovery plans.

Although business continuity and disaster recovery are closely related and have some similar activities—such as restoring systems and data from backup—these plans are distinctly different. A business continuity plan identifies and prioritizes an organization's systems and data in terms of business impact, to ensure a business can get back up and running as quickly as possible following an incident. A disaster recovery plan addresses the activities that must be performed to return a business to *normal* operation after an incident.

> **Although business continuity and disaster recovery are closely related and have some similar activities—such as restoring systems and data from backup—these plans are distinctly different.**

RECOVERY PLANNING

This is in some ways similar to response planning within the Response function, in that recovery planning requires organizations to document and regularly test their business continuity and disaster recovery plans and

ensure everyone in the organization understands roles and responsibilities. However, unlike incident response, outsourcing business continuity and disaster recovery can be difficult, if not impossible. That's because it requires a complete understanding of your organization's unique business operations.

IMPROVEMENTS

This category addresses the need for continuous improvement in your recovery planning. Many organizations don't regularly update or test business continuity and disaster recovery plans, and such plans can quickly become stale as a result. However, as with all other areas of technology, there are new innovations constantly being introduced which can help an organization execute more dynamic, flexible, and effective business continuity and disaster recovery plans.

> **If business operations are interrupted, failure to communicate quickly and accurately may result in misperceptions and loss of customers.**

COMMUNICATIONS

Finally, effective communications—both internally and externally—are critical during the recovery phase of an incident. If business operations are interrupted, failure to communicate quickly and accurately may result in misperceptions and loss of customers. For publicly traded companies, ineffective communications can negatively impact shareholder value.

Get Strategic with Your Security

UncommonX offers unmatched enterprise-class cybersecurity protection for mid-size organizations by combining adaptive threat and intelligence software with 24/7 industry experts, making it easy to constantly both map and fix root causes of security vulnerabilities. Taking a market-first inside-out approach to ongoing digital security risks through unique curated threat feeds and automated analytics, the UncommonX BOSS intelligent security operations platform provides clear contextual awareness to yield accelerated outcomes to mitigate and guard against threats. Learn more at UncommonX.com.