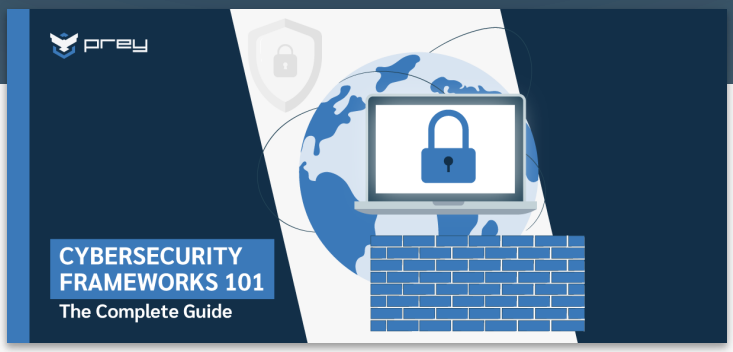
Cybersec Essentials

Cybersecurity Frameworks 101 - The Complete Guide

Cybersecurity frameworks provide the structure and methodology you need to protect your important digital assets. Find out which framework best suits your needs!

BY NICOLAS POGGI

June 3, 2022



Today, it's virtually inevitable that digital technology and data will be essential to some aspects of your life. It could be your work, relationships, living situation, and so forth. For example, you're utterly dependent on devices and data if you run a business. Unfortunately, people with bad intentions are eager to steal the data you and your business need to function. Their motivations vary, but malicious actors generally either want to profit from your devices and data or disrupt them—or both.

It's also shocking that a recent survey from Insight found that over 70% of business leaders are NOT convinced that their companies can withstand a possible cyber attack. With these fears, many companies create ideal frameworks to maintain, monitor and disable cybersecurity risks before they happen.

What can you do to achieve the best cybersecurity under these circumstances?

There are ways to achieve a satisfactory level of cybersecurity, including data security solutions and database security. Frequently, the best way to meet this objective is to adopt a cybersecurity framework. A framework provides the structure and methodology to protect your critical digital assets.

While a cybersecurity framework provides a set of "best practices" for measuring risk tolerance and establishing controls, selecting which one is appropriate for your firm may be challenging.

What is a cybersecurity framework?

A cybersecurity framework is, essentially, a system of standards, guidelines, and best practices to manage risks that arise in the digital world. They typically match security objectives, like avoiding unauthorized system access, with controls like requiring a username and password.

If that is confusing, it might help first understand what a framework is. In the physical world, a framework is a beam system that holds up a building. In the world of ideas, a framework is a structure that underpins a system or concept. A framework is a way of organizing information and, in most cases, related tasks.

Frameworks have been around for a long time. For example, in financial accounting, frameworks help accountants keep track of financial transactions. An accounting framework is built around concepts like assets, liabilities, costs, and controls. Cybersecurity frameworks take the framework approach to the work of securing digital assets. The framework is designed to give security managers a reliable, systematic way to mitigate cyber risk no matter how complex the environment might be.

Cybersecurity frameworks are often mandatory, or at least strongly encouraged, for companies that want to comply with state, industry, and international cybersecurity regulations. For example, in order to handle credit card transactions, a business must pass an audit attesting to its compliance with the Payment Card Industry Data Security Standards (PCI DSS) framework.

Why do you need cybersecurity standards and frameworks?

Cybersecurity frameworks provide guidelines and best practices for organizations to follow to secure their systems, networks, and data. These frameworks help organizations establish a culture of security and reduce the risk of data breaches and cyberattacks. Implementing cybersecurity frameworks also helps businesses to comply with relevant regulations and laws.

Organizations need cybersecurity frameworks to protect their valuable assets from cyber threats. Cybersecurity frameworks provide a comprehensive approach to cybersecurity that includes policies, procedures, and technical controls. These frameworks help organizations identify and manage risks, detect and respond to cyber threats, and recover from cybersecurity incidents. Implementing cybersecurity frameworks also helps businesses to build trust with their customers, partners, and stakeholders by demonstrating a commitment to cybersecurity and protecting sensitive information.

But, what happens if you don't adhere to cybersecurity standards and frameworks?

The risks of not adhering to international cybersecurity standards and frameworks are numerous and severe, not only for organizations, but also for their employees and users that employ their

services. Failure to comply with these regulations can lead to data breaches, legal and financial consequences, and reputational damage. For example, in the science-fiction film "The Terminator," a failure to adhere to proper cybersecurity standards results in an AI system, Skynet, gaining self-awareness and launching a nuclear attack on humanity, so, let's hope that the guys at OpenAI are doing their paperwork.

Here are the five most common risks of not adhering to international cybersecurity standards and frameworks:

1. **Data breaches** - These can lead to loss of sensitive data, legal liabilities, and reputational damage. In 2020, the average cost of a data breach was $3.86 million, according to IBM's Cost of a Data Breach Report.
2. **Financial penalties** - Non-compliance with regulations can result in significant fines. For example, the European Union's General Data Protection Regulation (GDPR) can impose fines of up to 4% of a company's annual revenue.
3. **Legal liabilities** - Failure to adhere to cybersecurity standards can result in lawsuits, particularly in cases where customer data is compromised.
4. **Reputational damage** - A data breach or cyber attack can result in a loss of customer trust and damage to a company's reputation.
5. **Business disruptions** - A cyber attack can result in downtime, lost productivity, and lost revenue. According to a 2020 study by Ponemon Institute, the average cost of downtime due to a data breach was $274,000.

Types of cybersecurity frameworks

At one of his most important conferences, Frank Kim, previous CISO for the SANS Institute and one of the top cybersecurity experts provided an excellent explanation for these various framework types. He split them into three categories and outlined their purposes –

Control frameworks:

Control frameworks in cybersecurity provide specific controls or security measures that organizations can implement to protect their information systems and data. These frameworks offer a set of guidelines for organizations to follow to reduce their risk of cyber attacks. Examples of control frameworks in cybersecurity include the Center for Internet Security (CIS) Controls, which consists of 20 critical security controls, and the Payment Card Industry Data Security Standard (PCI DSS), which provides a set of requirements for securing credit card data and transactions.

Think of control frameworks as a recipe for securing your organization's information systems and data. Just as a recipe provides step-by-step instructions for preparing a meal, a control framework provides a set of guidelines that an organization can follow to protect its systems and data. By following these guidelines, organizations can better protect their assets from cyber threats.

In short, control frameworks must:

- Develop an essential strategy for the security team
- Provide a baseline set of controls
- Assess the current technical state
- Prioritize control implementation

Program frameworks:

Program frameworks are a type of cybersecurity framework that focuses on the development and management of cybersecurity programs. These frameworks provide guidelines and best practices for developing, implementing, and maintaining a cybersecurity program tailored to an organization's needs. Activities include risk assessment, policy development, training, awareness, incident response planning, and ongoing monitoring and improvement.

Program frameworks function as a roadmap for building and maintaining a strong cybersecurity program. These frameworks provide a structured approach to cybersecurity management that can be adapted as the organization's needs change over time. They help organizations establish a strong foundation for cybersecurity and better manage cybersecurity risks. Common cybersecurity frameworks include NIST, CIS, and ISO/IEC 27001.

In short, program frameworks must:

- Assess the state of the security program
- Build a comprehensive security program
- Measure program security/ competitive analysis
- Simplify communication between the security team and business leaders

Risk frameworks:

Risk frameworks in cybersecurity are essential tools used by organizations to identify, assess, and manage cybersecurity risks. They provide a structured approach to risk management, allowing organizations to identify and prioritize potential threats, assess the likelihood and impact of those threats, and develop strategies for mitigating or managing those risks. Risk frameworks are designed to help organizations maintain a strong cybersecurity posture and protect their systems and data from cyber threats.

To explain this concept in simpler terms, risk frameworks are like a checklist that organizations use to identify and prioritize potential cybersecurity risks. They help organizations understand the risks they face and develop strategies for managing those risks. Just as a doctor uses a checklist to diagnose a patient's symptoms and develop a treatment plan, an organization can use a risk framework to diagnose its cybersecurity risks and develop a plan to manage those risks.

In short, risk frameworks must:

- Define key process steps to assess/manage risk

- Structure program for risk management
- Identify, measure, and quantify risk
- Prioritize security activities

Cybersecurity frameworks list

There are many different IT security frameworks because each cybersecurity framework is designed to address different cybersecurity challenges, risks, and compliance requirements. Some frameworks are more comprehensive than others, some are industry-specific, and some are designed for specific regulatory compliance. Organizations need to choose the framework that best fits their specific needs and requirements.

1. NIST Cybersecurity Framework (CSF): A voluntary framework developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risk.
2. ISO/IEC 27002 and 27001: A widely recognized international standard for information security management systems (ISMS).
3. Payment Card Industry Data Security Standard (PCI DSS): A set of requirements designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.
4. Center for Internet Security (CIS) Controls: A set of 20 security controls designed to provide specific and actionable ways to stop the most pervasive and dangerous attacks.
5. HITRUST CSF: A comprehensive security framework specifically designed for healthcare organizations to manage risk and comply with regulations.
6. Federal Risk and Authorization Management Program (FedRAMP): A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
7. Cybersecurity Capability Maturity Model (C2M2): A framework developed by the Department of Energy to help organizations assess and improve their cybersecurity capabilities.

The NIST cybersecurity framework

The NIST Framework for Improving Critical Infrastructure Cybersecurity, sometimes just called the "NIST cybersecurity framework," is, as its name suggests, intended to be used to protect critical infrastructure like power plants and dams from cyber attacks. However, its principles can apply to any organization that seeks better security. It is one of several NIST standards that cover cybersecurity.

Like most frameworks, the NIST cybersecurity framework is complex and broad in scope. The basic document describing it runs 41 pages. The implementation of the framework can involve

thousands of person-hours and hundreds of pages of documentation, procedures, controls, etc. At the root, though, the framework is fairly easy to understand.

The framework's core is a list of cybersecurity functions that follow the basic pattern of cyber defense: identify, protect, detect, respond, and recover. The framework provides an organized mechanism for identifying risks and assets that require protection. It lists the ways the organization must protect these assets by detecting risks, responding to threats, and then recovering assets in the event of a security incident.

WHAT ARE THE FIVE ELEMENTS OF THE NIST CYBERSECURITY FRAMEWORK?

IDENTIFY

The **Identify** function establishes the framework for future cybersecurity-related measures taken by your company. Determining what exists, what dangers are involved with those settings, and how it connects to your company goals is critical to Framework's success.

PROTECT

The framework contains a category known as PR.DS, which stands for "Protect Data Security." Going deeper into the framework, PR.DS has seven sub-categories, each intended to ensure the protection of data. These include controls for protecting data at rest (PR.DS-1), protecting data in transit (PR.DS-2), and so on. To comply with PR.DS-1, for instance, the organization might mandate encryption of data at rest.

DETECT

The Detect function necessitates the creation and implementation of the necessary operations to detect the presence of a cybersecurity incident. It allows for the prompt detection of cybersecurity occurrences.

RESPOND

To guarantee that the cybersecurity program is always improving, the Respond function performs response planning, analysis, and mitigation operations.

RECOVER

It enables a fast return to regular activities in order to mitigate the effect of a cybersecurity occurrence. Recovery Planning, Improvements, and Communications are examples of outcomes for this Framework's Core function.

CIS

CIS was built in the late 2000s by a volunteer-expert coalition to create a framework for protecting companies from cybersecurity threats. It comprises 20 controls that experts from all fields regularly update – government, academia, and industry – to be consistently modern and on top of cybersecurity threats.

CIS works well for organizations that want to start with baby steps. Their process is divided into three groups. First, they start with the basics, then move into foundational, and finally, organizational. CIS is also a great option if you want an additional framework that can coexist with other industry-specific compliance standards (such as HIPAA and NIST).

This organization works with benchmarks, or guidelines based on commonly used standards, such as NIST and HIPAA, that not only map security standards to help companies comply with them but offer alternative basic security configurations for those who don't require compliance but want to improve their security.

These benchmarks are divided into two levels. The first is recommendations for essential security configurations that don't affect services performance, and the second is a more advanced level of benchmarks that offer higher-level security configuration recommendations, with a possible cost of dramatic performance.

ISO/IEC 27001

ISO 27001/27002, also known as ISO 27K, is the internationally recognized standard for cybersecurity. The framework mandates (assumes) that an organization adopting ISO 27001 will have an Information Security Management System (ISMS). ISO/IEC 27001 requires that management systematically manage the organization's information security risks, taking threats and vulnerabilities into account.

The framework then requires the organization to design and implement information security (InfoSec) coherent and comprehensive controls. The goal of these controls is to mitigate identified risks. The framework suggests that the organization adopt an ongoing risk management process. To get certified as ISO 27001-compliant, an organization must demonstrate to the auditor that it is using what ISO refers to as the "PDCA Cycle."

PDCA Cycle

What is the PDCA cycle? The PDCA cycle is a business management method that focuses on four main steps that every company should consider implementing. The four steps are:

- **Plan** — means establishing the ISMS itself along with policies, objectives, processes, and procedures for risk management.
- **Do** — refers to implementing the actual functioning ISMS, including implementing InfoSec policies, procedures, and so forth.
- **Check** — involves monitoring and reviewing the ISMS, measuring process performance compared to policies and objectives.
- **Act** — is the process of updating and improving the ISMS. It may mean undertaking corrective and preventive actions based on internal audits and management reviews.

Companies and government agencies adopt ISO 27001 to get certified for compliance. Otherwise, it's a lot of work without much to show for the effort. ISO certifies compliance through the work of approved audit firms. A company goes through applying for certification with ISO, which usually involves working with an experienced consultant who may then also act as the auditor and certifying authority.

Cybersecurity frameworks like GDPR help to protect personal user data.

Some frameworks exist for a specific industry or security scenario.

- COBIT, for example, is a control framework for IT systems used in financial accounting. It's a core part of compliance with the Sarbanes Oxley Act.
- HIPAA, a law designed to protect the privacy of patientes, comprises regulations and a framework. It's a specific set of control requirements coupled with a certification process to attest to compliance.
- The EU GDPR rules that protect personal information are somewhat softer in nature.

How managed service providers can help organizations implement cybersecurity frameworks

Managed Service Providers (MSPs) can play a crucial role in helping organizations implement cybersecurity frameworks. MSPs are third-party service providers that offer a range of IT services, including cybersecurity services. They can help organizations by providing expert guidance on selecting and implementing the right cybersecurity framework based on their specific needs and requirements. MSPs can also help organizations streamline their cybersecurity operations, improve their overall security posture, and ensure regulatory compliance.

Here are five benefits of using MSPs to implement cybersecurity frameworks:

1. **Expertise:** MSPs have a team of cybersecurity experts who possess the necessary skills and knowledge to help organizations implement the most appropriate cybersecurity frameworks. They can also provide ongoing support and training to ensure that the organization's cybersecurity posture remains strong.
2. **Cost-effectiveness:** Hiring an MSP is often more cost-effective than hiring and maintaining an in-house cybersecurity team. MSPs can provide the same level of expertise and service at a fraction of the cost.
3. **Scalability:** MSPs can provide flexible services that can be scaled up or down based on the organization's needs. This allows organizations to adjust their cybersecurity requirements based on their changing business needs.
4. **Time-saving:** MSPs can handle the entire cybersecurity implementation process, from selecting the right framework to training employees. This frees up the organization's internal IT team to focus on other critical tasks.
5. **Access to advanced technologies:** MSPs often have access to the latest cybersecurity technologies and tools. This means that organizations can benefit from the latest cybersecurity advancements without having to invest in expensive technologies themselves.

Takeaways

Cybersecurity frameworks provide a basis for achieving a strong security posture and preventing data breaches. In some cases, they enable an organization to become certified compliant with a specific regulation. Adopting a framework requires a decision to commit time and resources to the project. If done right, however, it's worth it! The framework offers an organized way to become secure and continually measure the effectiveness of the security controls established by the framework.

ABOUT THE AUTHOR

NICOLAS POGGI

Nicolas Poggi is the head of mobile research at Prey, Inc., provider of the open source Prey Anti-Theft software protecting eight million mobile devices. Nic's work explores technology innovations within the mobile marketplace, and their impact upon security. Nic also serves as Prey's communications manager, overseeing the company's brand and content creation. Nic is a technology and contemporary culture journalist and author, and before joining Prey held positions as head of indie coverage at TheGameFanatics, and as FM radio host and interviewer at IndieAir.

On the same Issue

THE FUTURE OF CYBERSECURITY IN SCHOOLS: TRENDS, TIPS AND TOOLS

Explore the future of cybersecurity in schools: new tools, malware prevention, and industry trends. Stay informed to ensure a secure educational environment.

November 29, 2023

KEEP READING

DEVELOPING AN ADVANCED CYBERSECURITY STRATEGY FOR K-12 SCHOOLS

Are you ready to strengthen your school's cybersecurity? Learn how to conduct risk assessments, audit security practices, and implement technical controls. Protect yo...

October 2, 2023

KEEP READING

WHY DEVICE SECURITY POLICIES ARE IMPORTANT FOR SCHOOLS

Discover the vital role of device security policies in safeguarding K-12 schools from cyber threats. Dive into the full guide to bolster your school's digital safety!

August 22, 2023

KEEP READING

INCIDENT RESPONSE PLANNING FOR SCHOOLS

Learn how to build a robust incident response plan and defend against cyber threats. Get proactive and safeguard your institution's digital assets - Read more now!

August 8, 2023

KEEP READING

GET STARTED

ES

Status

All systems operational