precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 10 July 2022

With our focus on reducing cyber risk, let's take a look at frameworks.

Ensuring that your organization adheres to industry standard and regulatory best practices for IT security can be aided by a cybersecurity framework.

Dr. Ronald Walcott
Managing Director

WHAT IS IT?

Cybersecurity frameworks provide a set of standards for security in various industries to understand their security posture and those of their vendors. By having a framework in place, the process and procedures that the organization must take for assessment, monitoring and mitigation become much easier to define. With that being said, there are various types of frameworks which govern different sectors.

TODAY, WE'D FOCUS ON THE NIST CYBERSECURITY FRAMEWORK.

The Cybersecurity Framework

The framework consists of three main components:

1. Core – Desire cybersecurity outcomes organized in a hierarchy and aligned to detailed guidance and controls
2. Profiles – Alignment of the organization's requirements and objections, risk appetite and resources using the desired outcomes of the framework core.
3. Implementation Tiers – A qualitative measure of organizational cybersecurity risk management practices.

Key Framework Attributes

- Common and accessible language
- Adaptable to various technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living Document
- Guided by many perspectives – private, academia and public sector

Why use the Cybersecurity Framework?

The Framework provides a common language and systematic methodology for managing cybersecurity risk. The Core includes activities to be incorporated in a cybersecurity program that can be tailored to meet any organization's needs. The Framework is designed to complement, not replace, an organization's cybersecurity program and risk management processes.

The process of creating Framework Profiles provides organizations with an opportunity to identify areas where existing processes may be

In this Issue:

strengthened, or where new processes can be implemented. These Profiles, when paired with the Framework's easy-to-understand language, allows for stronger communication throughout the organization. The pairing of Framework Profiles with an implementation plan allows an organization to take full advantage of the Framework by enabling cost-effective prioritization and communication of improvement activities among organizational stakeholders, or for setting expectations with suppliers and partners. Additionally, Profiles and associated implementation plans can be leveraged as strong artifacts for demonstrating due care.

The Implementation Tiers component of the Framework can assist organizations by providing context on how an organization views cybersecurity risk management. The Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program. The Tiers may be leveraged as a communication tool to discuss mission priority, risk appetite, and budget.

Supporting Risk Management with the Framework

The Framework helps guide key decision points about risk management activities through the various levels of an organization from senior executives, to business and process level, and implementation and operations as well.

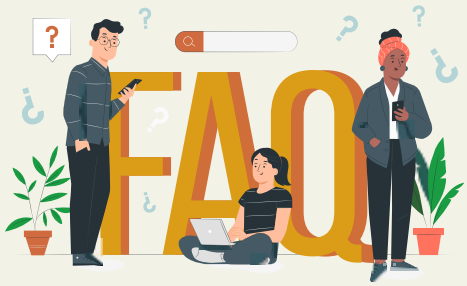
Who should use the Framework?

The Cybersecurity Framework is for organizations of all sizes, sectors, and maturities.

While the Framework was designed with Critical Infrastructure (CI) in mind, it is extremely versatile.

With built-in customization mechanisms (i.e., Tiers, Profiles, and Core all can be modified), the Framework can be customized for use by any type of organization.

Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it enables scalability. A small organization with a low cybersecurity budget, or a large corporation with a big budget, are each able to approach the outcome in a way that is feasible for them. It is this flexibility that allows the Framework to be used by organizations which are just getting started in establishing a cybersecurity program, while also providing value to organizations with mature programs.



Frequently Asked Questions:

DOES THE FRAMEWORK APPLY ONLY TO CRITICAL INFRASTRUCTURE COMPANIES?

No. Although it was designed specifically for companies that are part of the U.S. critical infrastructure, many other organizations in the private and public sectors (including federal agencies) are using the Framework. NIST encourages any organization or sector to review and consider the Framework as a helpful tool in managing cybersecurity risks.

DOES THE FRAMEWORK BENEFIT ORGANIZATIONS THAT VIEW THEIR CYBERSECURITY PROGRAMS AS ALREADY MATURE?

The Framework can be used by organizations that already have extensive cybersecurity programs, as well as by those just beginning to think about putting cybersecurity management programs in place. The same general approach works for any organization, although the way in which they make use of the Framework will differ depending on their current state and priorities.

Upcoming Events

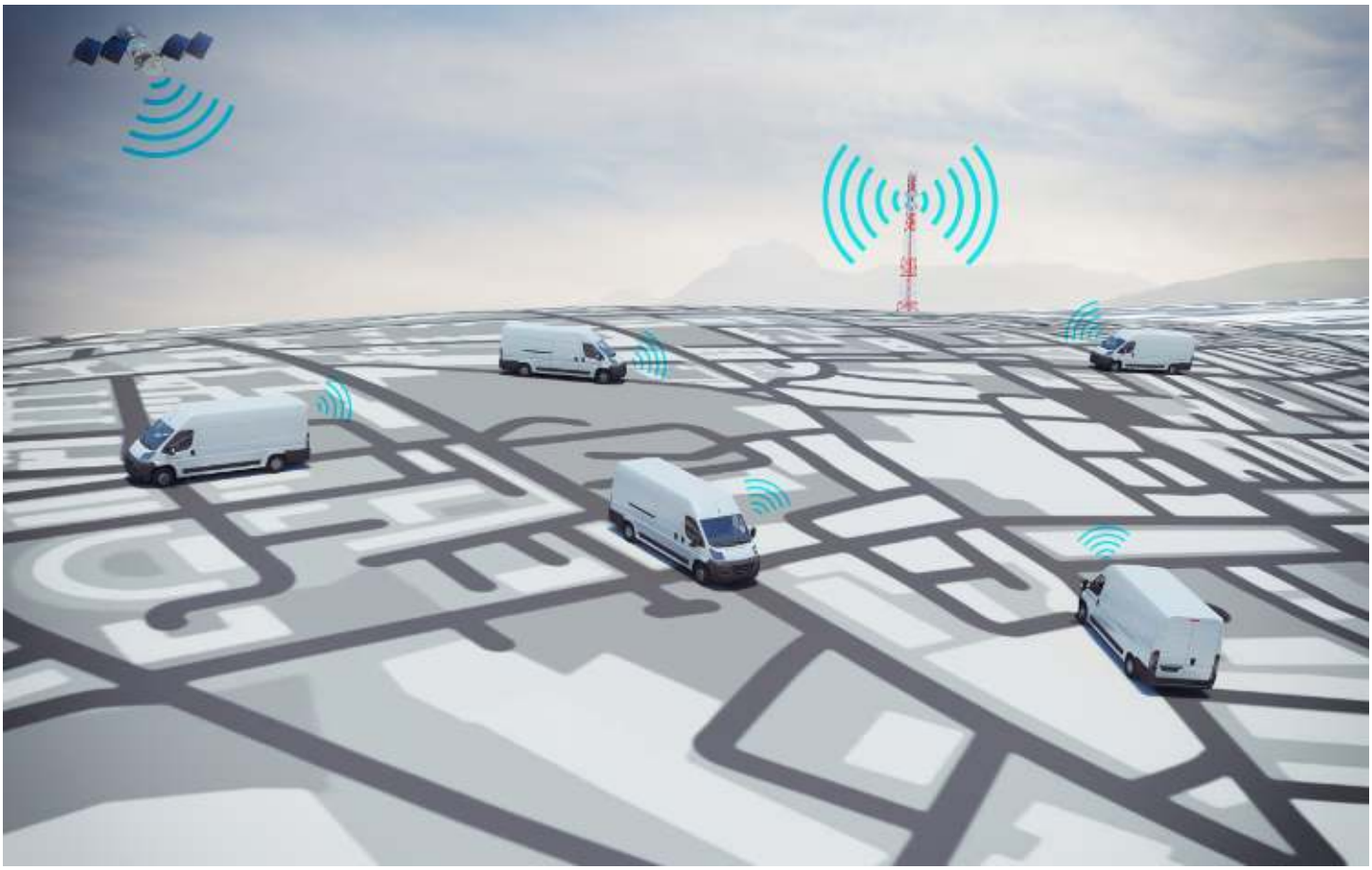
GOVERNMENT CYBERSECURITY SUMMIT
July 26, 2022

CRYPTOCURRENCY & PAYMENTS SECURITY SUMMIT
August 2, 2022

CONNECTED DEVICES CYBERSECURITY SUMMIT
September 20, 2022

Headline News:

GPS Tracker Made in China Conduit for Vehicle Hacking



Severe vulnerabilities in a popular GPS tracking device made in China could allow hackers to remotely surveil vehicles' locations and shut down their engines, say security researchers in a warning echoed by the U.S. government.

Cybersecurity firm BitSight says it uncovered six vulnerabilities in a hard-wired GPS tracker made by MiCODUS. Boston-based BitSight estimates there are 1.5 million active tracking devices made by the Shenzen-based manufacturer deployed across the globe that are used by 420,000 different customers in more than 160 countries.

Organizations identified by BitSight as using trackers include a Fortune 50 energy company, a national military in South America, a nuclear power plant operator and a state on the east coast of the United States.

"If China can remotely control vehicles in the United States, we have a problem," said Richard Clarke, a former presidential adviser on cybersecurity.

The firm estimates Russia is the country with the greatest number of vulnerable devices and in the top three of countries with the most users.

The vulnerabilities include a hard-wired master password and vulnerability to SMS-based commands that can be executed without authentication. There are no patches, leading the U.S. Cybersecurity and Infrastructure Security Agency to advise that the trackers be isolated from internet connectivity. The agency is not aware of any active exploitation of the vulnerabilities.

Source: https://www.databreachtoday.eu

868-610-7237 | salesinfo@precision-cyber.com | www.precision-cyber.com | 1st Floor, Brair Place, 10-12 Sweet Road St. Clair, Port of Spain, Trinidad