FREE DOWNLOAD

DVMS Institute®

Fundamentals of Adopting the NIST Cybersecurity Framework

Volume 1 of the

Create, Protect, and Deliver Digital Business Value series

tso
a Williams Lea company

CHAPTER 1

Looking through the wrong end of the telescope

1 Looking through the wrong end of the telescope

> *"To change ourselves effectively, we first had to change our perceptions."*
> Stephen R. Covey (2004)

It's too complex. It's too costly. It's a technical problem – let the IT department handle it. This new tool will solve ... and the list goes on.

Have you heard these statements? Did you guess we're talking about cybersecurity?

Many organizations faced with real-life cybersecurity challenges look through the telescope from the wrong end. What they see is a small part of the whole. Cybersecurity isn't the problem. The problem with cybersecurity is twofold: the first problem is one of perception; the second results from looking through the telescope incorrectly – in other words, it is a failure to see the whole.

Instead of approaching cybersecurity from an enterprise level, the organization relegates it to the IT department. Then it asks the wrong questions about cybersecurity – as if it were a piece of hardware or software – for example, "How much will this cost?"

Another aspect of this wrong-end-of-the-telescope perspective is that the organization approaches value creation for stakeholders by focusing on profit or revenue targets. The idea of cybersecurity being a technical problem and stakeholder value being dependent on money demonstrates a failure to approach value from the perspective of stakeholders versus the bottom line – an additional way to look through the wrong end of the telescope.

When an organization provides or produces something of genuine value for its stakeholders, it's a certainty that there will be someone who tries either to access, change, steal, or sell it, deprive the organization of its use, or worse. This "thing" of value may not be obvious; for example, the convenience of credit card processing. It could be fuel through a pipeline or patient records. The point, however, is that if it has value to you or your stakeholders, then it has value to "them."

> *"It is not necessary to change. Survival is not mandatory."*
> W. Edwards Deming

We need to change the mental model associated with cybersecurity from a technical challenge to one that considers cybersecurity to be essential to value production. This change in perception is the magic bullet to address these issues – but it is not easy.

The best way to approach creating a different mental model is to ask different questions. Ask questions that focus on creating and protecting value:

- What is valuable to us?
- What is valuable to our stakeholders?
- How is that value protected?
- Are we prepared to respond when something compromises any aspect of value?

If the organization doesn't proactively take appropriate steps to protect that value, does it provide value? Another way to ask this question is this: If the value we deliver doesn't have appropriate protections for value-stakeholders, is it still valuable to them?

One of the themes you'll see repeated throughout this book is that value creation and value protection are two different sides of the same coin. It's essential to do both: value *must* be protected at an appropriate level for the organization, understanding that value changes over time. Cybersecurity *is* an intrinsic aspect of business value.

The idea of a shift in perception is associated with another theme: the need to apply systems thinking, which views cybersecurity as an enterprise responsibility, and not that of a single department (or similar internal organizational unit).

1.1 For NIST Cybersecurity Professional (NCSP) students

The material in this book provides the rubric for the NCSP Foundation course. It presents the narrative that accompanies your course material. The book contains more information than will fit into the course. Consequently, we recommend that you read the whole book instead of focusing on just the material in the syllabus.

If you understand the flow of the story in this book, it will be easier to pass the course examination.

1.2 Using the book

The key to adopting and applying systems thinking when dealing with complex problems is to look at the system as a "whole" (rather than a "hole") and to develop an innate understanding of its components and behaviors. This approach to creating and protecting value concurrently requires you to understand the existing threat landscape. It also requires you to understand how the threat landscape evolves with technology. You'll find this material in **Chapter 2**.

Another "different" aspect to consider when developing new mental models is the assumption linking cybersecurity with technology. "How should we position cybersecurity outside of IT?" There's an answer in history. In his 1985 book *Innovation and Entrepreneurship*, Peter Drucker wrote: "Customers pay for what is of use to them and gives them value. Nothing else constitutes 'quality.'" (Drucker, 1985). In **Chapter 3**, you'll find a discussion about the link between quality and value explored in the context of the model we've created, called the *CPD Model* (CPD being an abbreviation for "creating, protecting, and delivering" digital business value). This chapter also discusses how to determine what to protect and how much protection is needed. What is the risk to the organization if ...? These questions require applying a principled approach to enterprise risk management (ERM).

Chapter 4 presents our approach to adopting the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST-CSF). Although you can jump directly to that chapter, we recommend reading Chapters 2 and 3 first. Doing so will make it easier to apply the NIST-CSF discussion.

Chapter 5 presents a more detailed discussion of the CPD Model that is briefly introduced in Chapter 3. It provides an overlay for any organization desiring to apply the new concept to link business value creation with its protection. The model presents a view of this system of systems, presented in the context of the NIST-CSF. This approach makes it easier to understand how to adopt the NIST-CSF and adapt it to fit the organizational need.

Every organization represents a potentially complex system – in effect, a system of systems – from a single-person company to a multinational enterprise (including government and military entities). Among the many things it must do, it must manage stakeholders, produce something, move things or people, communicate, provide accounts payable and receivables, etc. Each of these represents a "subsystem" of the whole. The core capability of adapting to a dynamic environment means that this system of systems must continually adapt to seek an equilibrium that optimizes the likelihood of survival.

> *"[A] mind, once stretched by a new idea, never regains its original dimensions."*
> Oliver Wendell Holmes Sr.

Think about this quotation. Now consider this: *Once an organization sees the "whole" and understands that value drives its adaptation to its environment, it can't "unsee" it*. "Seeing" enables the organization to change its perception of strategy and risk. Risk is an intrinsic aspect of strategy, creating a single entity: *strategy-risk*. Strategy-risk is a concept that subsumes creating value as part of what it takes to protect and deliver business value.

As noted above, Drucker linked value with quality. From this perspective, the only way to deliver value is to change the perception of cybersecurity from a technical challenge to an organizational requirement. Everyone is responsible for quality, not just the IT department.

Viewed from this perspective, as the perception of value changes, so does the perception of quality. It requires the organization to see the enterprise as a whole, not as isolated or disparate parts. The idea of seeing the whole is a crucial aspect of systems thinking.

There's more to adopting the NIST-CSF than the mere framework. The material in **Chapter 6** introduces a holistic approach to understanding what comes next. The chapter addresses the core point that cybersecurity is not a technical problem – it's an enterprise problem. The board of directors (or equivalent governing body) must accept responsibility and be held accountable for cybersecurity.

Nearly every aspect of an organization has some digital dependency; therefore every organization has to figure out how to create and protect digital business value. Accepting this point of view lays the foundation for adopting and adapting the NIST-CSF.

When value or quality changes, it stands to reason that the organization must change along with it. The idea that change is constant is not new. The concepts of stability and change are not mutually exclusive, yet many organizations seek stasis in place of stability. At its core, a stable organization can adapt to change by evolving internal needs, external requirements, and the threat environment.

How an organization perceives cybersecurity is shaped by its leadership and normalized in its culture. In too many cases, perception is achieved by looking through the wrong end of a telescope. The problem with cybersecurity is not about cybersecurity; it's about the perception of cybersecurity.

> *"I am not crazy; my reality is just different from yours."*
> Cheshire Cat in Alice in Wonderland (Lewis Carroll)

1.3 The rest of the story

This book provides a practical approach to adopting the NIST-CSF.

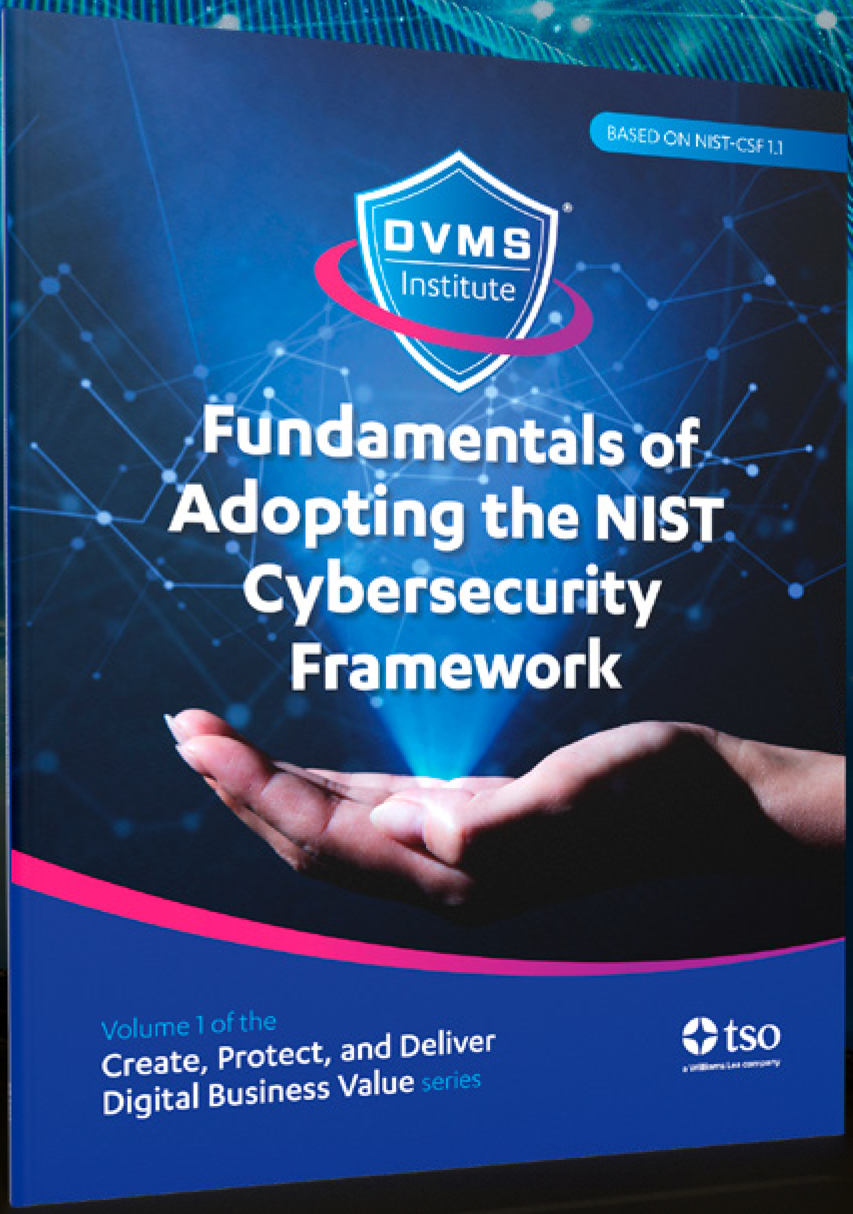
The second book provides more detailed information for the practitioner and the specialist. It covers the following topics:

- Developing a deep understanding of the threat landscape to be proactive
- Dealing with complexity
- Cybersecurity and the Digital Value Management System (DVMS)

- An adaptive way of working
- Cybersecurity within a system
- Strategy-risk: creating, protecting, and delivering digital business value
- Innovation for effect
- Overview of the DVMS.

The first two books focus on cybersecurity and introduce the DVMS as an overlay. The third book presents the DVMS as an enabler for an adaptive, cyber-resilient organization. It describes a scalable way for any organization to treat value creation and value protection as aspects of quality, regardless of size.

The three books will help you to recognize when you are looking through the wrong end of the telescope.


BASED ON NIST-CSF 1.1
DVMS Institute
Fundamentals of Adopting the NIST Cybersecurity Framework
Volume 1 of the
Create, Protect, and Deliver Digital Business Value series
tso