Why you should adopt the NIST Cybersecurity Framework

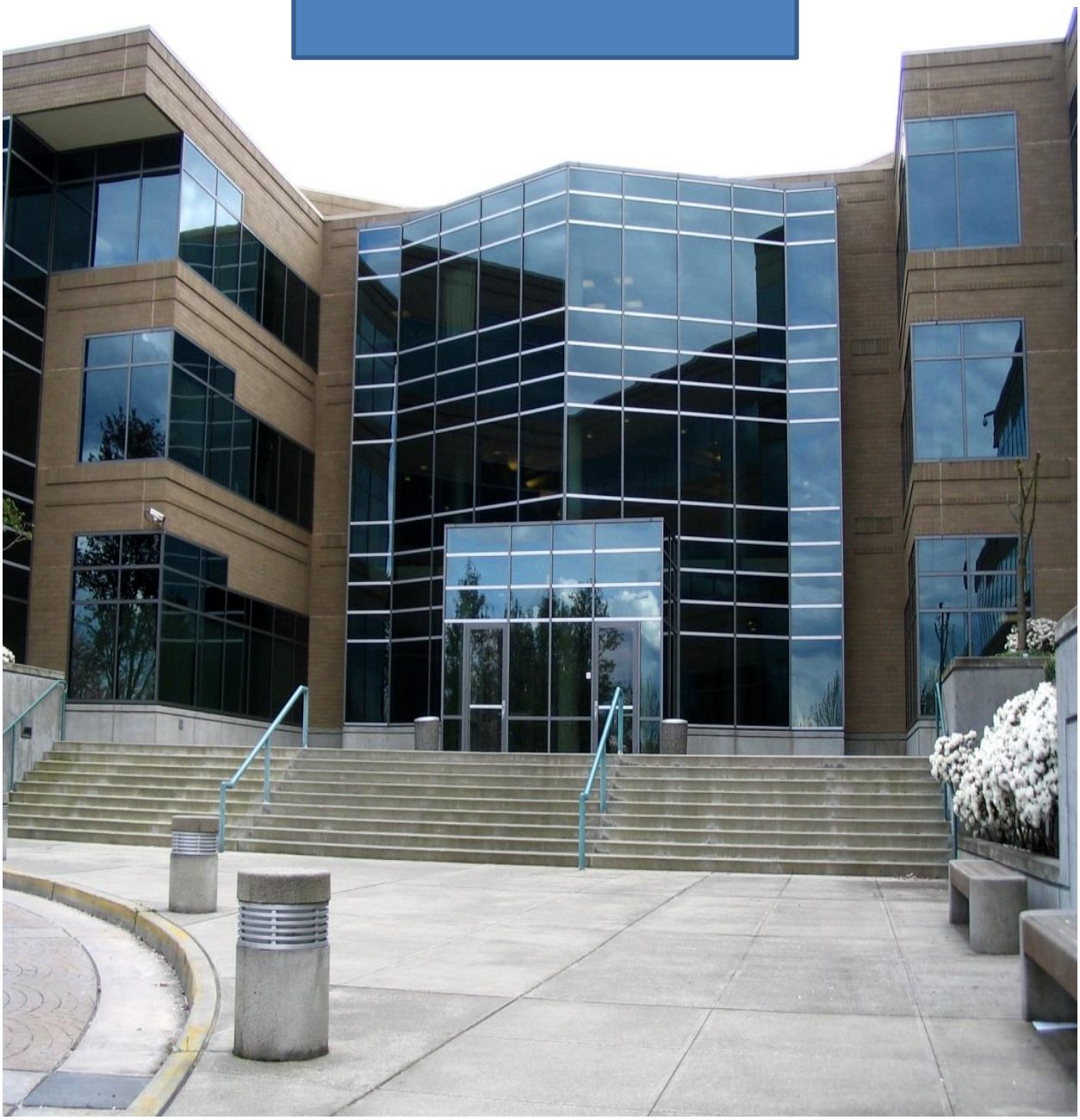
It's important to note that the Framework casts the discussion of cybersecurity in the vocabulary of risk management ***– Stating it in terms Executive leaders and board members understand.***

OutSecure Inc

The NIST framework is a risk based framework based on leading cybersecurity standards – It is valuable for

ALL

Businesses.



OutSecure Inc

NIST Cybersecurity Framework

Critical infrastructure

US Presidential Policy Directive 21 defines critical infrastructure as the following 16 sectors:

- Chemicals
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food & agriculture
- Government facilities
- Healthcare & public health
- Information technology
- Nuclear reactors, materials, & waste
- Transportation systems
- Water & wastewater systems

Source: Department of Homeland Security, Critical Infrastructure Sector

While the ***NIST Cybersecurity Framework*** targets organizations that own or operate critical infrastructure, adoption may prove advantageous for businesses across virtually all industries[1].

The Framework does not introduce new standards or concepts; rather,it leverages and integrates industry-leading cybersecurity practices that have been developed by organizations like NIST and the International Standardization Organization (ISO).

The Framework is the result of a February 2013 Executive Order titled ***"Improving Critical Infrastructure Cybersecurity"*** and 10 months of collaborative discussionswith more than 3,000 security professionals.[2] It comprises a risk-based compilation ofguidelines that can help organizations identify, implement, and improve cybersecuritypractices, and creates a common language for internal and external communication ofcybersecurity issues.

The Framework is a reiterative process designed to evolve in sync with changes in cybersecurity threats, processes, and technologies. It will be revised periodically toincorporate lessons learned and industry feedback. In effect, the Framework envisions effective cybersecurity as a dynamic, continuous loop of response to both threats and solutions.

The Framework provides an assessment mechanism that enables organizations to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining cybersecurity programs. It comprises three primary components: ***Profile, Implementation Tiers,*** and Core.

The Profile component enables organizations to align and improve cybersecurity practices based on their individual business needs, tolerance for risk, and available resources. To do so, organizations create a Current Profile by measuring their existing programs against the recommended practices in the Framework Core. These practices include processes, procedures, and technologies such as asset management, alignment with business strategy, risk assessment, access control, employee training, data security, event logging and analysis, and incident response plans.

To identify a Target Profile, organizations employ the same Core criteria to determine the outcomes necessary to improve their cybersecurity posture.

Unique requirements by industry, customers, and business partners can be factored into the Target Profile. Once completed, a comparison of the Current and Target Profiles will identify the gaps that should be closed to enhance cybersecurity and provide the basis for a prioritized roadmap to help achieve these improvements.

Implementation Tiers help create a context that enables organizations to understand how their current cybersecurity risk-management capabilities stack up against the characteristics described by the Framework. Tiers range from Partial (Tier 1) to Adaptive (Tier 4) (Figure 1.). NIST recommends that organizations seeking to achieve an effective, defensible cybersecurity program progress toTier 3 or Tier 4.

Figure 1: Tiers of cybersecurity maturity

Tier 1	Partial	Risk management is ad hoc, with limited awareness of risks and no collaboration with others
Tier 2	Risk Informed	Risk-management processes and program are in place but are not integrated enterprise-wide; collaboration is understood but organization lacks formal capabilities
Tier 3	Repeatable	Formal policies for risk-management processes and programs are in place enterprise-wide, with partial external collaboration
Tier 4	Adaptive	Risk-management processes and programs are based on lessons learned and embedded in culture, with proactive collaboration

The Framework Core defines standardized cybersecurity activities, desired outcomes, and applicable references, and is organized by five continuous functions: Identify, Protect, Detect, Respond, and Recover. (Figure 2.) The Framework Core, in effect, describes the continuous cycle of business processes that constitute effective cybersecurity.

Figure 2: Five core functions of effective cybersecurity

Functions	Definition	Categories
IDENTIFY	An understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities	Asset management, business environment, governance, risk assessment, risk management strategy
PROTECT	The controls and safeguards necessary to protect or deter cybersecurity threats	Access control, awareness and training, data security, data protection processes, maintenance, protective technologies
DETECT	Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events	Anomalies and events, continuous monitoring, detection processes
RESPOND	Incident-response activities	Response planning, communications, analysis, mitigation, improvements
RECOVER	Business continuity plans to maintain resilience and recover capabilities after a cyber-breach	Recovery planning, improvements, communications

Benefits beyond improved cybersecurity

For most organizations, whether they are owners, operators, or suppliers for critical infrastructure, the NIST Cybersecurity Framework may be well worth adopting solely for its stated goal of improving risk-based security. But it also can deliver ancillary benefits that include effective collaboration and communication of security posture with executives and industry organizations, as well as potential future improvements in legal exposure and even assistance with regulatory compliance.

"U.S. Securities and Exchange Commission SEC)'s Office of Compliance Inspections and Examinations (OCIE) cybersecurity examinations of registered entities include questions outlined in the NIST Cybersecurity Framework."

It's important to note that the Framework casts the discussion of cybersecurity in the vocabulary of risk management. With good reason: Executive leaders and board members typically are well-**versed in risk management, and framing cybersecurity in this context will enable security leaders to more effectively articulate the importance and goals of cybersecurity.**

The Framework has already been suggested as a potential "baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes. At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines—and whether more may be needed." If SEC or other proposed federal regulation of cybersecurity becomes a reality, implementing the Framework could be a mandatory exercise. By choosing to act now, organizations have the benefit of more flexibility in how they implement the Framework.

Call OutSecure (203)81608061 and schedule a free initial assessment to determine how your business can benefit from adopting the NIST cybersecurity framework.

OutSecure Inc