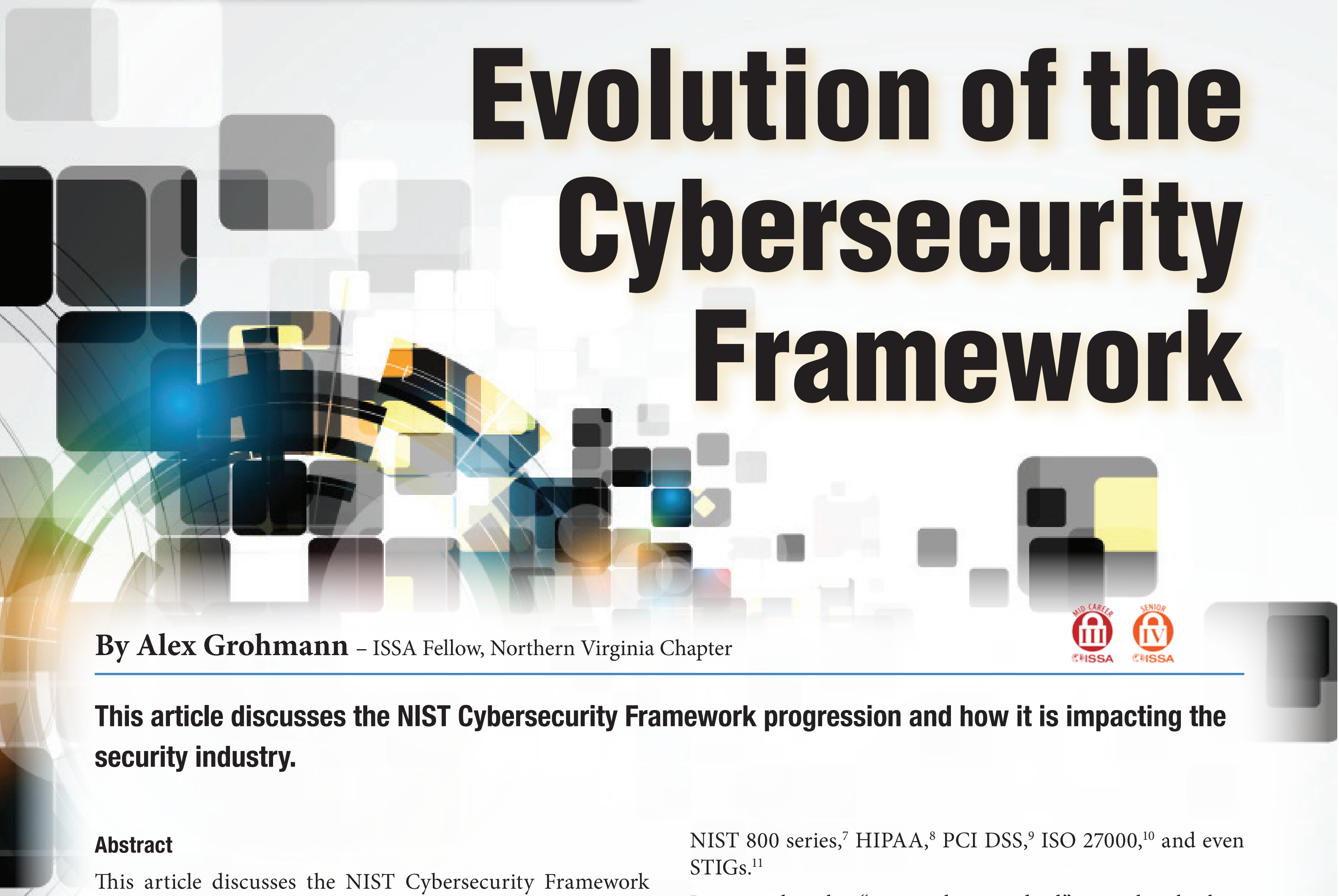

Evolution of the Cybersecurity Framework

By Alex Grohmann – ISSA Fellow, Northern Virginia Chapter

This article discusses the NIST Cybersecurity Framework progression and how it is impacting the security industry.

Abstract

This article discusses the NIST Cybersecurity Framework progression and how it is impacting the security industry. For the last four years the framework has proven to be a solid framework for risk management across all types of industries throughout the entire globe. It has just received its first update but still proves to be a valuable resource in the planning and building of a successful cybersecurity program.

Andrew Tanenbaum, author and computer science professor, is famously quoted as saying "The nice thing about standards is that you have so many to choose from." And so it is with the cybersecurity industry. Auditors have standards and guidelines from places like the FFIEC,[1] PCAOB,[2] ISACA,[3] IIA,[4] and COSO,[5] and cybersecurity professionals can choose from standards such as COBIT,[6] NIST 800 series,[7] HIPAA,[8] PCI DSS,[9] ISO 27000,[10] and even STIGs.[11]

It was within this "yet another standard" mentality, back in 2014, that the Cybersecurity Framework (CSF) [7] was initially introduced. This publication from the National Institute of Standards and Technology (NIST) quickly differentiated itself, however, because it was not just another detailed set of standards and guidelines around specific security processes and procedures but was the high-level strategy framework that had always been missing. This was the frame to the puzzle in which any set of standards could be fit, and the details of the framework requirements could be set by the CISO and driven by business needs instead of the old one-size-fits-all checklist.

For four years NIST's CSF has sat atop of the cybersecurity landscape as the framework for integrating standards into an overall strategy, and in that time many practitioners have been using the CSF in some form or fashion. The CSF was

[1] FFIEC - Federal Financial Institutions Examination Council – https://www.ffiec.gov/.

[2] PCAOB – Public Company Accounting Oversight Board –https://pcaobus.org/.

[3] ISACA – https://www.isaca.org.

[4] IIA – The Institute of Internal Auditors – https://na.theiia.org.

[5] COSO – Committee of Sponsoring Organizations of the Treadway Commission – https://www.coso.org.

[6] COBIT - Control Objectives for Information and Related Technologies – http://www.isaca.org/cobit.

[7] NIST 800 series – https://csrc.nist.gov/publications.

[8] HIPAA - Health Insurance Portability and Accountability Act of 1996 – https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[9] PCI DSS - Payment Card Industry Data Security Standard – https://www.pcisecuritystandards.org/pci_security/.

[10] ISO 27000 – International Organization for Standardization, 27000 family, Information Security Management Systems – https://www.iso.org/isoiec-27001-information-security.html.

[11] STIGs - Security Technical Implementation Guides – https://iase.disa.mil/stigs/Pages/index.aspx.

originally intended to be an optional tool for the creation, management, and refinement of security programs and to provide the basis for any company or entity to create a strategy of how to approach information security [2]. It was this initial version of the CSF that famously came up with the identify-protect-detect-respond-recover cadence, which allows for the neat integration with the NIST risk management framework [4].

In December 2016, the White House Cybersecurity Commission Report [1] called for the CSF to be the dominate strategy framework used by federal CISOs, and in May of 2017 an executive order [3] was issued that did just that by mandating, among other things, protection of federal networks using the NIST CSF. In April of 2018, after long series of drafts and open discussions, NIST released version 1.1 of the CSF, which strengthened the framework by reinforcing some of its existing concepts (such as authentication and identify proofing) and adding some new ones (including supply chain risks, self-assessments, and vulnerability disclosure). The use of the CSF has since grown to be used across industries and academia as well as by the governments of different states and multiple nations.

How the framework works

While the CSF is a framework for detailed standards, it is not a small document, nor a small undertaking to implement. The "core" of the CSF is broken down into five general functions of cybersecurity: Identify, Protect, Detect, Respond, and Recover.

Function: ID	Categories
Identify: ID	Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management
Protect: PR	Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology
Detect: DE	Anomalies and Events, Security Continuous Monitoring, Detection Processes
Respond: RS	Response Planning, Communications, Analysis, Mitigation, Improvements
Recover: RC	Recovery Planning, Improvements, Communications

Table 1 – Cybersecurity Framework Functions and Categories

In the original version of the CSF, the five functions were then broken down into 22 categories and 98 subcategories, but with the release of version 1.1, a 23rd category was added that focuses on supply chain risk (table 1).[12] In addition to the five subcategories that were added to support the new supply chain category (table 2), there were new subcategories added to clarify and improve the requirements for identity proofing, multifactor access control, integrity checking, resilient mechanism design, and vulnerability disclosures, adding a total of 10 new subcategories, bringing the overall total to 108 subcategories. Each of these subcategories needs to be evaluated by the security team to define how they wish to address the requirement by using COBIT, NIST, ISO, ISA, or one of many other control definitions available in their industry, or by even defining their own custom solutions. Each subcategory includes what NIST has labeled "informative references" that map the specific controls from these different controls documents to the subcategory level, giving the implementation team an understanding of what the different control documents advocate for the possible control implementation for each subcategory.

The CSF is not intended to say how to meet the requirement—only what the requirements are—and allows the dif-

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	**D.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	COBIT 5…
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	COBIT 5…
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	COBIT 5…
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	COBIT 5…

Table 2 - Supply chain risk management subcategories and sample informative references

[12] Images and tables are reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce.

ferent control documents to drive the how, which will be determined by the individual organization (by defining it based on their understanding of the risk and their accepted risk posture). This is an important distinction; it is the organization that defines what level they expect the control to meet, based on the level of risk that they are willing to accept, which is driven by applying a cost-benefit analysis to their own situation. In other words, the security leadership can customize their controls by building a common control framework that meets their specific requirements and risks. This concept can give the CISO the opportunity to take some of the checklist-mentality away from the auditor and ensure that they are being audited on the control levels that they have set for themselves, customized for their own environment.

This allows senior management…to give direction on security settings based on their understanding of business priorities.

However, while the core functions of the CSF have caught on, there are two other components that are intended to support the core functions: tiers and profiles. These are not as well-known as the CSF's main core component. NIST has defined a four-level tier structure with the purpose of describing "…an increasing degree of rigor and sophistication in cybersecurity risk management practices" [7]. These tiers are intended to be signposts as to the state of each of the cybersecurity subcategories. Though NIST explicitly calls out that this tier structure (from level 1 – partial to level 4 – adaptive) is not a maturity level, the increase in levels is clearly the result of a more mature level of processes that may be worth attaining if it provides a "…cost-effective reduction of cybersecurity risk" [7]. In an ideal setting, senior management would dictate what tier level they would like to operate each subcategory at (based on risk and cost-benefit), with a supporting team to translate the assigned tier level to appropriate technical control implementations. This allows senior management, who may not be familiar with the details of security language and technology, to give direction on security settings based on their understanding of business priorities.

This prioritization of the subcategories by tier can be a major undertaking, which is why NIST decided to integrate profiles in with tiers. In the original version of the CSF, target profiles were pre-canned implementation risk-level recommendations for a specific sector, business, or industry. This allowed supporting organizations to publish the priority of subcategories that they thought should be put in place for a specific group of businesses. For example, NIST has published a target profile for the manufacturing industry to highlight which subcategories were of higher importance based on the business objectives common to the manufacturing industry [8]. In this situation, under the business objective of "Maintain Human Safety" in the category of Asset Management, the subcategories of ID.AM-1 (physical device inventory) and ID.AM-5 (resources are prioritized) would be considered a priority in the target profile.

In version 1.1, this concept of profiles was expanded to include tiers, where the characteristics of a target profile would be reflected to support the desired tier level. As in the above example, management might feel that the implementation of physical device inventory should be a tier-four control because of the high risk of injury associated with manufacturing equipment, which would lead to extensive processes of checks and balances to ensure that the physical device inventory was rigorously maintained at all times. This would likely be a time-consuming and expensive set of processes but considered worth the potential cost based on the calculated benefits and priority within the organization. In contrast, Asset Management subcategory ID.AM-2 (software inventory) is a lower priority in the profile and might only rate a tier-one investment in a control solution (relying on a much looser and informal process for tracking). For each of the 108 subcategories, once a target profile was established, a current profile would need to be developed based on the current state of the control, followed by a gap analysis between the two, and a remediation plan—all part of the CSF seven-step process to improve the cybersecurity program.

Future of the framework and next steps

NIST has stated that the CSF is a living document and has published a road map [6] of the next topics to be addressed, including "international aspects, impacts, and alignment" and "small business awareness and resources." NIST plans on addressing privacy engineering, cybersecurity workforce, and the life cycle of cyber attacks in future updates, with the option to add or reprioritize topics as they gain or lose importance. As with the version 1.1 update, it is likely that the core of the CSF will remain relatively static so that while any new version will offer some new features, it will also allow the continued use of previous versions without impact.

It is therefore incumbent on the organization to start to integrate some type of risk management framework into their environment. In order to be successful in this regard, the organization needs to understand its own regulatory requirements and be able to address specific industry priorities. It is here that pre-built profiles by industry experts would be a huge step forward—published either by NIST or by separate independent industry specialists. In addition, the organization needs to have an understanding of its industry's risk environment in order to consider unique risks that they may be facing. In the long run, perhaps this is something that the industry-specific information sharing and analysis centers (ISACs) would be better equipped to manage and maintain across their specialty sectors. Lastly, an organization needs to understand what its current level of maturity is in these different cybersecurity areas to be able to know where to move toward. NIST has tried to bridge this gap by teaming with the Baldridge Performance Excellence Program to create a set of resources that can assist the management team in defining their overall cybersecurity strategy and mapping the current and future state of their cybersecurity program [5].

Conclusion

The Cybersecurity Framework is an elegant document that provides the skeleton on which a solid cybersecurity program can be built. Meeting all the requirements of an individual control document can be a cost-prohibitive project that absorbs countless man-hours with little return on investment in many of the control areas, so being able to build a customized set of controls that is specifically adapted to meet the needs of an organization is both cost effective and maximizes risk reduction.

References

1. Commission on Enhancing National Cybersecurity, "Report on Securing and Growing the Digital Economy," (December 1, 2016) – https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.
2. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," US Federal Register (February 12, 2013) – https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
3. Executive Order 13800, " Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Federal Register (May 11, 2017) – https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.
4. Joint Task Force Transformation Initiative, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," NIST (updated 6/5/140 – https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final.
5. [NIST, "Baldrige Performance Excellence Program," National Institute of Standards and Technology (March 2017) – https://www.nist.gov/baldrige.
6. NIST, "Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1," National Institute of Standards and Technology (December 5, 2017) – https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf.
7. NIST, "Framework for Improving Critical Infrastructure Cybersecurity (version 1.1)," National Institute of Standards and Technology (April 16, 2018) – https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
8. Stouffer, K., et al, "NISTIR 8183: Cybersecurity Framework Manufacturing Profile," National Institute of Standards and Technology (September 2017) – https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

About the Author

Alex Grohmann, CISSP, CISA, CISM, CIPT, is an independent consultant and information security professional with nearly 25 years of experience. He is an ISSA Fellow and a member of the Honor Roll. He may be reached at grohmann@sicherconsulting.com.