WAVESTONE

NIST Request for Comments

Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity – Draft #2

Response of Wavestone

January 19, 2018

Introduction

Private and public entities' exposure to cyber threats has faced a rapid acceleration over the past several years, with a steady increase of the number and impact of attacks targeting specific organizations.

While threats are becoming more frequent, more sophisticated, and more widespread, the data and devices to be protected are increasing in volume and complexity with new behavioral or technical trends such as BYOD, work from home, IOT, SaaS, and various cloud services.

Beyond the operational risk faced by financial institutions, regulators are expanding their scrutiny to focus more attention on cybersecurity. Europe and the United States are currently developing specific regulations that are expected to be enforced in the coming years, the latest example being the NYS-DFS 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies released in February 2017.[1] On February 15, 2018, covered entities are required to submit their first Certification of Compliance to the superintendent.

Several frameworks have been developed to structure and support the risk mitigation approach at the organization level. All major advisors or standards organizations pushed for their own solutions. As a result, IT departments, compliance divisions, legal representatives, and senior executives struggle to select the appropriate strategy to efficiently mitigate risk and align with growing regulatory requirements.

Senior Management and board of directors came to embrace the management of cyber risks with the same kind of scrutiny applied to other business risks. This evolution is either the results of regulatory constraints or the awareness of cyber events' impact. Therefore, cyber risks left the IT world to become an enterprise priority.

Relying on the NIST Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Cybersecurity Framework" or "Framework"), Wavestone proposes to unify the efforts and the governance of cybersecurity around the risks faced by the organization. Therefore, the momentum is ensured between the major stakeholders (e.g., Board, Business Lines, Compliance, Legal, IT, IT Security, Third Party Risk Management, Human Resources, Business Continuity Management, Corporate Communications), each with their own agenda.

Wavestone welcomes the opportunity to contribute once again to the development of the NIST Cybersecurity Framework that became a cornerstone of the worldwide cybersecurity landscape.

In response to the latest NIST request for comments (RFC),[2] Wavestone relies on its past successes and management consulting expertise to provide feedback on the recently released draft #2 of the Framework version 1.1.[3] Our experts are available to answer any questions the RFC reviewers will have. Note: For more feedback relating to the Framework version 1.1, please refer to the previous response of Wavestone[4] to the NIST request for comments of January 25, 2017.[5]

Wavestone is eager to pursue its contribution to industry developments regarding cyber risk management and would be pleased to participate in any future developments of the Framework.

[1] http://www.dfs.ny.gov/about/press/pr1702161.htm
[2] https://www.nist.gov/sites/default/files/documents/2017/12/05/fact_sheet_framework1.1_and_roadmap_12_5_2017.pdf
[3] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf
[4] https://www.nist.gov/sites/default/files/documents/2017/04/21/2017-04-10_-_wavestone.pdf
[5] https://www.federalregister.gov/documents/2017/01/25/2017-01599/proposed-update-to-the-framework-for-improving-critical-infrastructure-cybersecurity

Table of Contents

Wavestone's Interest in the Framework

Wavestone is an international management consulting organization with 2,500 consultants across 4 continents.[6] The firm provides consulting services to various industries with a focus on financial institutions in the United States, specializing in areas such as:

- Strategy & Operations;
- Risk Management & Regulatory Compliance;
- Technology Strategy.

Our teams rely on several frameworks (either available on the market or developed internally) to improve the cybersecurity maturity of organizations, with transformations impacting the Board, and management and operational levels.

With 400 cybersecurity experts, Wavestone provides extensive cybersecurity management capabilities on topics such as assessing cyber risks, assessing cyber risk management maturity, defining cyber risk management strategy, developing and deploying governance, building multi-year cybersecurity roadmap of initiatives, conducting cyber risk workshops to identify controls in place, developing cybersecurity regulatory and industry watch capabilities in partnership with compliance departments, and jump-starting initiatives covering topics such as data loss prevention, identity and access management, data assessment and classification, cyber resilience management, and cybersecurity internal awareness.

The NIST Cybersecurity Framework is a major step forward to support companies develop or reinforce a cybersecurity program based on industry best practices.

Due to the evolving nature of the cybersecurity landscape and available frameworks, and due to the improvement opportunities observed, we work with our clients on tailored/customized frameworks. Most engagements leverage multiple industry recognized best practices/frameworks beyond the NIST Cybersecurity Framework, including country-specific frameworks such as:

- FFIEC Cybersecurity Assessment Tool[7];
- COSO Enterprise Risk Management – Integrated Framework[8];
- ISO/IEC ISO 27k – Information Security Management System Family of Standards[9];
- SANS Institute CIS Critical Security Controls[10];
- BIS-IOSCO Guidance on cyber resilience for financial market infrastructures[11];
- CSA Cloud Controls Matrix Working Group[12];
- HKMA Cyber Resilience Assessment Framework,[13] or;
- MAS Technology Risk Management Guidelines[14].

[6] https://www.wavestone.com/en
[7] https://www.ffiec.gov/cyberassessmenttool.htm
[8] http://www.coso.org/erm-integratedframework.htm
[9] https://www.sans.org/critical-security-controls
[10] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[11] https://www.bis.org/cpmi/publ/d138.htm
[12] https://cloudsecurityalliance.org/group/cloud-controls-matrix
[13] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf
[14] http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx

1 Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity ecosystem (threats, vulnerabilities, risks, practices, technological approaches), including those developments in the Roadmap items?

The update of the NIST Cybersecurity Framework is a welcome addition to the cybersecurity landscape. It shows the U.S. public administration continues to support public and private institutions in their cybersecurity efforts, and that the Framework is a living tool that institutions can leverage on the long haul.

Moreover, the active involvement of the private sector during the review process reinforces the Framework's relevance for private institutions and the fact that it includes industry best practices from a broad range of actors (e.g., solution vendors, security services providers, management consulting firms).

However, the new version does too little, and too late. Almost 4 years after the release of the first version and numerous workshops, requests for information, and requests for comments, the version 1.1 is still to be released. Besides continuous increase of the level of cyber threats, the Framework falls short with respect to several key areas such as:

- Promoting consistent assessment and alignment of cybersecurity practices across industries and geographies;
- Guiding institutions from an operational standpoint to put theoretical concepts into practice;
- Providing guidance for interconnected institutions with worldwide entities and global/local risks and controls.

This update is unlikely to significantly impact the recognition and adoption of the Framework. Only a broader update of the Framework, especially addressing the need for objective evaluation criteria and proposing a standardized approach for implementation, will have the potential to reinforce its position as global reference to address cybersecurity. On that topic, Wavestone continues to believe that support and involvement in the Framework development by international organizations recognized in other zones (i.e., EMEA and APAC) should be reinforced.

The Framework remains too theoretical. The Framework describes the Profile as "the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization," and a way to "establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities." It suggests assessing the organization's maturity level for each of the Framework Core's Functions, Categories and Subcategories, defining target maturity levels based on "desired cybersecurity risk management goals," and developing a prioritized plan to achieve them. While the idea of assessing a current state, defining a target, and developing a roadmap to achieve this target is rather easy to apprehend, it is difficult to put into practice in the context of cybersecurity when it needs to account for business specifics.

The Framework currently leaves the door open to interpretation on how to conduct such effort. Additional clarity is needed to help organizations go through those step by themselves, with objective evaluation and prioritization criteria, as the exercise usually proves rather difficult and time consuming.

As an example, questionnaires developed in the Baldrige Cybersecurity Excellence Builder – Key questions for improving your organization's cybersecurity performance[15] bring significant value. A similar type of resource would be very helpful when combined with the Profile.

Wavestone recommends considering the following initiatives to foster greater cyber preparedness across public and private sector:

/ **Structure a certification model to accompany organizations.** Wavestone believes the development of a NIST Cybersecurity certification for 3rd parties would foster more consistent and effective deployment of the Framework. It could follow a similar model as what currently exists in the field of accounting. Such certification would require training, exercises, and exams on how to implement the Framework while accounting for institutions' specifics: creating a current profile, conducting a risk assessment, creating a target profile, prioritizing gaps, etc.

/ **Develop operational guidelines on how to implement the Framework.** The NIST Cybersecurity Framework – Manufacturing Profile[16] released in September 2017, is a great example of guideline that should be made available for other sectors and distributed to a broader audience. By providing tailored business/mission objectives, a prioritization of the Core's subcategories to support those objectives, and target profile criteria by system impact level, the document helps institutions move from theoretical to concrete actions. Guidance on tracking and managing achievement of Target Profiles is essential to ensure full deployment of the NIST Cybersecurity Framework. Specifically, criteria and thresholds for assessing achievement of a Target Profile is critical as part of institutions' cybersecurity programs.

/ **Propose implementation examples including materials and tools used.** Wavestone believes it would be beneficial to provide concrete examples of the usage of the current and target profiles for the definition of a roadmap, and would not limit the flexibility for implementing the Framework in any way. Including materials and tools such as templates or other reference documents to jump start this effort would also help institutions focus more on results rather than spending too much effort on developing their own specific approach.

/ **Develop standard measures and metrics.** Wavestone frequently works with clients to develop tailored cybersecurity metrics and dashboards for reporting at the operational and management levels within an IT security department and up to the Board, by leveraging the Framework Core's Functions and Categories for categorization. Those dashboards are always deemed very valuable for managing cybersecurity. While the version 1.1 introduces new guidelines regarding the measure of cybersecurity in Section 4.0 *Self-Assessing Cybersecurity Risk with the Framework*, it does not address the need to provide standard measures and metrics, including calculation methods, as a basis for measuring trends over time, internally and externally. Informative references currently available are not sufficient to easily define and implement appropriate measures and metrics. Wavestone therefore recommends the addition of an initiative dedicated to the development of standard measures and metrics as part of the NIST Roadmap. The resulting materials should be developed and incorporated as part of the Framework, or as a separate reference document if the Framework clearly refers to it.

[15] https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf
[16] https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile

2 For those using Version 1.0, would the proposed changes affect their current use of the Framework? If so, how?

As a user of the version 1.0, Wavestone does not foresee any significant impact on the usage of the NIST Cybersecurity Framework with the release of the version 1.1. Adjustments will mainly include:

- **Review of Current and Target Profiles based on changes to the Framework Core.** While the Functions are maintained, the new and updated categories and subcategories will require re-assessment of Current Profiles and the update of Target Profiles. Updated informative references will also have to be reviewed to identify any additional best practices to consider for the roadmap.

- **Review of the Implementation Tier based on new supply chain risk management practices and adjusted Integrated Risk Management Program practices.** The changes in the Implementation Tiers will need to be reviewed to ensure that the selected Implementation Tier remains appropriate. As changes are consistent with usual practices generally observed at a given level for our clients, Wavestone believes that no change should occur in most cases.

- **Reinforce efforts to measure cybersecurity effectiveness.** Most organizations already leverage metrics or measures to assess the effectiveness of their cybersecurity program over time, especially at the technical level. The addition of the Section 4.0 reinforces the importance of such activities to be able to effectively steer and prioritize cybersecurity efforts. However, while the Framework version 1.1 Draft #1 brought interesting concepts and examples to pursue this effort, the Draft #2 takes a step back and remains quite theoretical. By recommending organizations to be "thoughtful, creative, and careful," the Framework does little in helping them focus on "rational, effective, and valuable cybersecurity investments."

3 For those not currently using Version 1.0, would the proposed changes affect their decision about using the Framework? If so, how?

Though the NIST Cybersecurity Framework version 1.0 already brought strong value. Today, Wavestone believes the update to version 1.1, and more regular updates moving forward, are important to encourage further adoption, but also insufficient to tackle today's challenges. The Framework needs to be more thoroughly maintained on a recurring basis to answer the evolving cybersecurity landscape (i.e., best practices, guidelines, other frameworks, regulatory requirements, etc.)

Wavestone believes that this new version 1.1 of the NIST Cybersecurity Framework is beneficial in promoting broader adoption among public and private institutions, mainly thanks to the incorporation of supply chain risk management guidance in Section 3.3 *Communicating Cybersecurity Requirements with*

Stakeholders and as part of the Framework Core. The new guidance fills a major omission in the version 1.0 and is aligned with other recent guidance materials such as the FFIEC Appendix J: Strengthening the Resilience of Outsourced Technology Services,[17] the NYS-DFS Update on Cyber Security in the Banking Sector: Third Party Service Providers,[18] and the FINRA Report on Cybersecurity Practices.[19]

As previously explained, the Framework leaves room for improvement in certain areas and does not fully address today's cybersecurity needs of public and private institutions. Indeed, it leaves space for subjective interpretation in the definition of Current and Target Profiles and Implementation Tiers, preventing a fully consistent approach within the same firm, industry, or across industries.

[17] https://www.ffiec.gov/press/PDF/FFIEC_Appendix_J.pdf
[18] http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf
[19] https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Wavestone U.S. Contact Information

Cyril Korenbeusser
Senior Manager

M +1 (929) 245-5747
cyril.korenbeusser@wavestone.com

Cyril Korenbeusser is leading Wavestone Cybersecurity & Data Protection group in the US. He is promoting cyber excellence as a speaker and contributor in various forums.

Jean-Jacob Dreyfus
Senior Consultant

M +1 (646) 724-2695
jean-jacob.dreyfus@wavestone.com

Jean-Jacob Dreyfus is a Cybersecurity & Data Protection strategy expert. He is managing the Cyber Regulatory Watch for the US and develops cyber accelerators to ease business-to-technology risk mitigation.