# Modalities for Cyber Security and Privacy Resilience: The NIST Approach

**Janine S. Hiller**
Virginia Tech
jhiller@vt.edu

**Roberta S. Russell**
Virginia Tech
rrussell@vt.edu

**ABSTRACT**

Cybersecurity was a major topic of discussion at the 2015 World Economic Forum in Davos - the Sony attack; huge data breaches at Target and Adobe; a 91% increase in targeted cyber-attacks; annual losses of over $400 billion; the exposure of 904 million personal data records; cyber-attacks on a Finnish bank, a South Korean credit bureau, a German factory's industrial controls, and the Ukrainian government; as well as increased general anxiety over critical infrastructure exposure (Tobias 2014; WEC 2015). These incidents highlight the risks inherent in a world increasingly complex, interconnected, and cyber-based. Much like thinking in other fields of disaster and crisis management, creating an impenetrable boundary or eliminating cyber risk entirely has given way to building cyber resilience. Cyber resilience is a social, economic and national security issue. This paper examines one approach, the NIST Cybersecurity Framework, in terms of building resilience in both cybersecurity and privacy..

**Keywords**

Cybersecurity, privacy, resilience, risk, framework, NIST

## INTRODUCTION

Information systems are important in times of crisis management; therefore, maintaining the security of those systems is important. Furthermore, cyber attacks or intrusions may, themselves, be considered a crisis when the systems upon which a society depends, critical information infrastructures, are rendered dysfunctional. During a crisis, privacy issues, or personal integrity issues, can sometimes be overlooked. Yet both security and privacy are fundamental to the survival of a civilized and democratic society. If an information system disaster plan also includes privacy considerations, then the resilience of the system can provide for the resilience of privacy. The problem is that privacy principles as they have traditionally been identified are not amenable to being incorporated into system design. This short paper describes how the recent NIST approach to designing cyber secure systems does this by incorporating privacy considerations into cybersecurity metrics. The NIST Draft arguably moves from a privacy by design concept to an evolving privacy engineering model. Lastly, the paper uses the resiliency lens to analyze the NIST framework to protect critical information infrastructures and privacy.

## REGULATORY FRAMEWORK FOR CYBER INFRASTRUCTURE IN U.S.

Early in the discussion of how actors in cyberspace would be governed, Larry Lessig famously described four regulatory modalities; norms, market mechanisms, architecture (technology, or code as Lessig called it) and law. All of these modalities are used to secure cyberspace today in an interrelated and fairly

unstructured, dynamic manner. There may, however, be tensions between public and private regulators about the province of each and the role of mandatory standards or self-regulatory frameworks. In past research we described the different mixes of modalities for regulation and the impact of different approaches taken in the United States and the European Union (Hiller et al. 2013). Whether security measures should be required by regulation, or whether they should be voluntary, is part of the comparison. The European Union has also provided leadership in this field through its Cybersecurity Strategy, proposed directive on network and information security, and through work by ENISA, the European Union Agency for Network and Information Security. We limit discussion to the NIST framework in this short paper, while anticipating discussions and comparisons of these two approaches.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" required NIST to address cyber vulnerabilities, "one of the most serious national security challenges," by developing a voluntary framework to reduce cyber risks to critical infrastructure in a "collaboratively develop[ed] and implement[ed] risk-based" approach. Over the next year NIST engaged in consultations, meetings, and discussions with government, interest groups, and private sector representatives, and solicited comments on a proposed draft. Within the past year, it released a Framework for Improving Critical Infrastructure Cybersecurity, a Roadmap for Improving Critical Infrastructure Cybersecurity, and a draft of privacy engineering objectives, each based on industry input and voluntary compliance.

The first part of the NIST framework is the Core; the "Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles." The Core establishes common terminology and divides functions into the identification of assets, protection of assets, detection of threats/vulnerabilities, response to attacks/vulnerabilities, and recovery from attacks/vulnerabilities. The Core further divides and subdivides into categories, and maps to existing standards, norms and guidelines. From this analysis a company can build a current or target Profile of itself that can be a benchmarked to the Core; it can vary based on varying situations faced by the organization. Companies furthermore identify themselves within four Tiers to better comprehend and evaluate how they are meeting the cyber risks. Companies in Tier Four, "Adaptive," are described as "agile and risk-informed," the most developed, while companies in Tier One are labeled "Partial" and are advised to improve their status. Adaptive companies exhibit learning systems, continuous improvement and respond to change. Their cyber security program is integrated, culturally supported, and they engage with the external community and share information. Built upon risk management best practices principles, the Framework is meant to be useful in any industry and by any size organization, including internationally. The NIST framework includes three parts; the Core, Profile, and Implementation Tiers.

The Framework notes that "Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes." The Framework only offers a "general set of considerations" to address privacy concerns as a part of cybersecurity activities. As the organization audits its practices, it would also identify and evaluate how the practices and processes impact individual privacy. It particular, companies should have the people and processes in place to comply with privacy laws and regulations. Access limitation and training should be implemented, and a process should exist to review cyber system defense and response measures for privacy protection NIST also provided that the framework would undergo continuous review and updating in order to "ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risk, and solutions" (NIST 2014a).

The Roadmap, released at the same time as the Framework, seemingly expressed frustration that the Fair Information Privacy Practices (FIPPs), so widely utilized globally, were not a useful source for definitions of privacy or privacy harms, nor did they provide standards, best practices, or metrics. To design the cyber security Framework, NIST drew from existing documents and guidelines for cyber security; in contrast, NIST was required to craft definitions and standards for privacy risk management. Envisioning the creation of privacy engineering along the same lines as security engineering, NIST began by convening a workshop

towards these goals. The first workshop (First Workshop), held in April, 2014, attracted hundreds of attendees from across government, the private sector, civil society organizations, and education. The primary objective of the workshop was to promote privacy engineering concepts and standardized practices so that system developers could use technical approaches and best practices to protect privacy. Miscommunication between the policy side and technical side was a recurring theme from the First Workshop, as was the need to establish a standard vocabulary. Noting that individual privacy concerns persist in the face of fast moving technology developments, the summary of the first NIST Workshop resulted in an important conclusion, that "Process-oriented principles are an important component of an overall privacy framework, but on their own they do not achieve consistent and measurable results in privacy protection" (NIST 2014b).

At a second workshop on September, 2014, NIST provided a draft of Privacy Engineering Objectives and Risk Model (Privacy Framework), as well as a "discussion deck" that set out details of a two-pronged approach that integrates a privacy risk management framework and privacy engineering elements (NIST 2014d). Rather than focus on avoiding external risks as the cyber security Framework did, the Privacy Framework focused on the unintended consequences to privacy from an internal, "normal system behavior" standpoint. Many companies and organizations already have strong privacy protecting processes, especially if they are in an industry that is more specifically regulated than others, such as healthcare. In comparison, the privacy engineering objectives are a new approach. First, the three engineering objectives were defined from the point of the individual user as predictability, manageability, and confidentiality. The "problematic data actions" that could undermine those goals were identified as appropriation, distortion, induced disclosure, insecurity, surveillance, unanticipated revelation, and unwarranted restriction. These problematic data actions could lead to privacy harms. Privacy harms were defined as loss of self-determination, discrimination, loss of trust, and economic loss. NIST then gave examples of how specific problematic data actions at different stages of the data life cycle could lead to privacy harms. The Second Workshop report is not yet available, and NIST is still accepting public comments and discussion of the Privacy Framework. There is still work to be done; NIST reflected that more complete mapping of controls to prevent or respond to the risks would be a future topic. In sum, NIST expressed the Privacy Risk Equation as (NIST, 2014c):

*System Privacy Risk = (Personal information collected or generated + Data actions performed on personal information + Context)*

## DISCUSSION

The NIST work towards creating a cyber security Framework and the integration of a Privacy Framework is important as a means towards planning for resilience from the constant cyber attacks that plague participants at all levels in the current environment. Focusing on the privacy component as an example, the following discussion identifies at a high level the elements of the NIST Framework corresponding with resiliency theory, and deserving of further discussion. Perhaps the most important policy concept of the NIST frameworks is an integration of privacy as a fundamental part of preserving cyber resiliency; it is not a choice between privacy and security. Similarly, from a crisis management viewpoint, the fundamental right to privacy and civil rights can be incorporated as a necessary component to cyber security planning, and not seen only as an impediment. The Privacy Framework can be viewed under the resiliency lens in the following ways.

**System Based:** If resilience is defined as "the capacity of a system to withstand internal and/or external change yet remain within the same regime" (Garmestani, Allen & Benson, 2011), then a large disconnect between privacy protection and resilience is that there is generally no privacy "system" to protect. The FIPPs do not define broader privacy concepts, beyond the focus on personally identifiable information. The NIST Privacy Framework proposed a vocabulary that would allow policy and technical sides to work across perspectives and to "speak the same language." This language and proposed definitions are required in order to implement the systems approach and to eventually instill a risk management framework. The definitions and assumption will most likely evolve further as future consultations and discussions take place. The underlying principles lead to the goals and eventually to the ability to know what risks should be mitigated.

**Risk Management:** The Privacy Framework is built around a risk management model. Placing privacy within the realm of risk management enables it to be

addressed substantively within the management of data systems and operationalized within an organization (Bamberger & Mulligan, 2011). Resilience planning incorporates this type of implementation and internal controls based on evaluation of risk (Matwyshyn, 2011).

**Adaptive Capacity**: The frameworks are meant to continually evolve based on feed back and updating. The risk management framework will allow for continual learning from experience as individual organizations implement the model and update their procedures. Adaptive capability is a hallmark of resilient systems (Ruhl, 2011), and essential to address the dramatic challenges of cyber security. Cyber attacks and vulnerabilities are a fact of life and will continue to occur in the foreseeable future; therefore planning to address them organizationally is essential for resilience.

**Flexibility:** Resilience planning decries a system that is a "cookie-cutter one-size fits-all magic-bullet solution" (Arnold, 2014). The NIST framework can be applied in differing contexts, across industries, and internationally. The Privacy Framework is also built to accommodate context, and although it will incorporate laws and regulations, it does so at a level that allows it to be useful as a planning tool for organizations across the globe.

**Governance:** The NIST Privacy Framework is not centralized or mandatory; it is voluntary, and its creation depended upon the input from all sectors of society. It is not limited in use to one jurisdiction but can be used across global legal boundaries, and it involves organizations in the process and implementation. In this sense it meets the recommendation of some resilience scholars that law should not be hierarchical and inflexible (Humby, 2014).

## CONCLUSION

The NIST frameworks can be viewed through the lens of resiliency and risk assessment for information systems. Integrating privacy into security management by taking a privacy engineering approach is one of its important contributions. Future success in the private sector will likely depend on international acceptance and harmonization across borders.

## REFERENCES

1. Arnold, C.A. (2014) Resilient Cities and Adaptive Law, 50 *Idaho Law Review*. 245.
2. Bamberger. K.A. and Mulligan, D. K. (2011) Privacy on the Books and on the Ground, *Stanford Law Review*, 63, 247.
3. Garmestani, A.S., Allen, C.R. and Benson, M.H. (2013) Can Law Foster Social-Ecological Resilience? *Ecology and Society* 18(2):37.
4. Hiller, J. and Russell, R. (2013) The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison, *Computer Law and Security Review*, 29: 3, 236-245.
5. Humby, T. (2014) Law and Resilience: Mapping the Literature, *Seattle Journal of Environmental Law*, 4, 85.
6. Matwyshyn,A. M. (2011) Resilience: Building Better Users and Fair Trade Practice in Information, *Federal Communications Law Journal*, 63, 391.
7. NIST (2014a) NIST Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0), Washington, DC: National Institute of Standards and Technology, 2-12-15.
8. NIST (2014b) NIST Roadmap for Improving Critical Infrastructure Cybersecurity, Washington, DC: National Institute of Standards and Technology, 2-12-15.
9. NIST (2014c) NIST Update on the Cybersecurity Framework, 12-5-14.
10. NIST (2014d) Privacy Engineering Objectives and Risk Model – Discussion Deck, 9-10-14.
11. Ruhl, J.B. (2011) General Design Principles for Resilience and Adaptive Capacity in Legal System—With Applications to Climate Change Adaption,

*North Carolina Law Review*, 89, 1373.
12. Tobias, S. (2014) The Year in Cyberattacks, *Newsweek*, 12-31-14
14.
13. WEC (2015) Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, Geneva: World Economic Forum, # 301214.