From: Robert Zager
Sent: Monday, January 8, 2018 6:58 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Iconix's Comments to NIST Cybersecurity Framework V1.1 Draft 2

Greetings:

Attached please find Iconix's comments in response to your request for public comment on Cybersecurity Framework Version 1.1 Draft 2. As we discuss in the attached, Version 1.1 Draft 2 implements a model of user behavior which, although consistent with FISMA's personnel awareness training mandate, fails to account for actual human behavior. Failing to account for actual human behavior results in a risk assessment system which excludes risks caused by poor usability. We suggest that cybersecurity will improve by adding usability as a cybersecurity risk factor.

Thank you for your consideration of these comments.

Best regards,

Robert Zager
Iconix, Inc.

[*Attachment copied below*]

Document as a whole:

NIST's Visualization and Usability Group observed:[1]

The goal is to build systems that are actually secure not theoretically secure: Security Mechanisms have to be usable in order to be effective.

This observation captures three critical security concepts. First, security is the result of actual practices. Second, rank and file users have a large impact on actual security practices. Third, usability influences the security practices of rank and file users.

Cybersecurity Framework Version 1.1 Draft 2 closely tracks the FISMA mandate of personnel awareness training set forth in 44 U.S.C. § 3544(b):

> (4)security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—
>
> (A)information security risks associated with their activities; and
>
> (B)their responsibilities in complying with agency policies and procedures designed to reduce these risks;

The FISMA model of user behavior assumes that awareness training will result insecure user practices. By adopting this training/awareness model, Cybersecurity Framework Version1.1 Draft 2 perpetuates the myth that personnel will faithfully implement security practices. This assumption (awareness results in desired behavior) is inconsistent with research on human behavior. The Compliance Budget, a concept developed by Beautement, Sasse, and Wonham, describes user security behavior in terms of costs that the user weighs in making security decisions.[2] Under Compliance Budget analysis, security tasks are costs which are charged against the user's individual Compliance Budget. When the cumulative perceived costs of security tasks exceed the Compliance Budget, the result is negative compliance behavior. Beautement, etal. observe:[3]

> Improving system design, and creating a positive security culture, will simultaneously decrease the perceived cost of security tasks, and lower the rate of expenditure of the Compliance Budget. On the other hand increasing sanctions and monitoring will give more weight to the benefits associated with compliance. Both sides of this cycle make a positive compliance decision more likely.

Cybersecurity Framework Version 1.1 Draft 2 adopts three of the four cycle elements (creating a positive security culture, sanctions and monitoring). However, failing to include the fourth (improving system design) excludes a key tool in improving security behavior. In fact, as Beautement, et al. describe, failing to address system design improvements squanders the limited Compliance Budget:[4]

> Spending the budget at a faster rate for example by implementing security tasks that conflict with the business process leads to a lower maximum level of security (we are able to implement fewer security policies before the threshold is reached)…In this scenario security measures are more costly to the user and so at the point that the compliance budget threshold is reached effective security is below that of the other more efficient spending rates.

Cybersecurity is an adversarial engagement.[5] Adversaries exploit the usability of the user interface to induce user behaviors which advance cyberattacks.[6] A common exploit of a malicious abuse of the user interfaceisphishing.[7] For example, when a reporter compromised the FBI Director with a phishing email, the incident exploited the user interface, not a lack of awareness on the part of the FBI Director.[8] As the Ukraine power grid compromise demonstrated, adversaries can abuse the user interface to induce the user to execute a series of actions that ultimately result in compromised systems.[9] Usability is a cybersecurity risk factor.

It is important to address the cumulative impact on the user from compliance requirements promulgated by independent compliance organizations. When each organization independently weighs its own compliance mandates, the impact on the Compliance Budget can be small. But the user is actual manager of the Compliance Budget. As the user goes about daily job tasks, the user is burdened by the cumulative impact of poorly articulated compliance requirements. While each of these tasks may seem trivial in isolation, the cumulative impact of poorly coordinated compliance tasks can take a heavy toll on the Compliance Budget.[10]

Adopting Usability Design incorporates real human behavior into cybersecurity risk analysis.

Specific Comments:

1) Location: line 817-818

Comment: Add a new function, PR.UD, Usability Design. [*A new category within the Protect Function of the Framework Core*]

Rationale: Incorporate usability as a protective strategy.

2) Location: Table 2: Framework Core

Comment: After PR.AC add:

Category: Usability Design (PR:UD): Reducing the conflict between user business requirements and security tasks.

Subcategory: PR:UD-1: Identify and assess all security tasks imposed on users

Informative References: ISO 13407, NIST Interagency/Internal Report (NISTIR) – 7432, NIST Visualization & Usability Group Publications The compliance budget: managing security behavior in organisations[11]

Subcategory: PR:UD-2: User security costs are mitigated through improved usability

Informative References: ISO 13407, NIST Interagency/Internal Report (NISTIR) – 7432, NIST Visualization & Usability Group Publications The compliance budget: managing security behavior in organizations

Rationale: Incorporate usability as a protective strategy.

---

[1] Theofanos, Mary. Poor Usability: The Inherent Insider Threat. Gaithersburg, MD: National Institute of Standards and Technology, 2008. Computer Security Resource Center. NIST, 21 Mar. 2008. Web. 22 Sept. 2017.
<https://csrc.nist.gov/CSRC/media/Presentations/Poor-Usability-The-Inherent-Insider-Threat/images- media/Usability_and_Insider_threat.pdf>.

[2] Beautement, Adam; Sasse, M. Angela; and Mike Wonham. "The compliance budget: managing security behavior in organizations," NSPW'08, September 22–25, 2008, Lake Tahoe, California, USA.

[3] Beautement, et al., fn. 2, p. 54.

[4] Beautement, et al., fn. 2, p. 54.

[5] Chang, Frederick R., Ph.D., Guest Editor's column, The Next Wave, Vol. 19, No. 4, 2012. Web. 27 December 2017.
<https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-nextwave/assets/files/TNW-19- 4.pdf>.

[6] Conti, Gregory and Edward Sobiesk. "Malicious Interface Design: Exploiting the User," WWW 2010, April 26–30, 2010, Raleigh, North Carolina, USA.

[7] Zager, John, and Robert Zager. "Improving Cybersecurity Through Human Systems Integration." Small Wars Journal. Small Wars Foundation, 22 Aug. 2016. Web. 18 Sept. 2017.
<http://smallwarsjournal.com/jrnl/art/improving-cybersecurity-through-human-systems-integration>.

[8] Feinberg, Ashley, Kashmir Hill, and Surya Muttu. "Here's How Easy It Is to Get Trump Officials to Click on a Fake Link in Email." GIZMODO. Gizmodo Media Group, 9 May 2017. Web. 8 Jan. 2018. <https://gizmodo.com/heres- how-easy-it-is-to-get-trump-officials-to-click-on-1794963635>.

[9] Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” WIRED. Conde Nast, 3 Mar. 2016. Web. 25 Dec. 2017. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines- power-grid/>.

[10] Beautement, et al., fn. 2, p. 52.

[11] Beautement, et al., fn. 2.