November 3, 2023

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: NIST Cybersecurity Framework 2.0 & Examples for the NIST CSF 2.0

Dear NIST,

BlackBerry appreciates the opportunity to provide input on the Cybersecurity Framework 2.0 (Framework) and offer suggestions for additional relevant examples. For nearly 40 years, BlackBerry has invented, created, and built security solutions to give people and businesses the ability to stay secure and productive. Today, BlackBerry's trusted security protection can be found everywhere – from cars, to mobile devices, to laptops, based on our industry proven secure software development practices. BlackBerry develops credible, secure solutions, which e.g. are certified against ISO/IEC standards including 27001 and have adopted OpenChain ISO/IEC 5230:2020[1].

We believe that the Framework can be helpful guidance to enterprises that are establishing their cybersecurity risk management systems from scratch. At the same time, the flexible design of the functions will enable enterprises that have already established and been managing their own risk management systems to overlay the Profile to review and improve their existing risk management process.

Below, you will find our comments and suggestions.

1. NIST Cybersecurity Framework 2.0

A NIST resource on Developing Cyber-Resilient Systems (NIST SP 800-160, Volume 2 Revision 1)

Lines 735-740 of the Framework list examples of resources specific to an organization's technology. We support the resources listed.

PR.IR-03 identifies the following subcategory: "Mechanisms are implemented to achieve resilience requirements in normal and adverse situations". NIST SP 800-160, Vol. 2, Rev. 1[2], includes representative cyber resiliency techniques in normal (i.e., non-adverse) situations. By considering resiliency techniques proactively, it can be expected that fewer cyber breaches will occur. BlackBerry recommends that the Framework refer to this NIST resource, e.g. as follows (proposed addition to lines 735-740 is underlined, below):

> Since the Framework is technology-neutral, organizations should also look for resources that are specific to their technologies, such as:
>
> - …
> - Cyber techniques to increase resiliency: SP 800-160, Vol. 2, Rev. 1, *Developing Cyber-Resilient Systems*

[1] BlackBerry Certifications, https://www.blackberry.com/us/en/company/certifications
[2] NIST SP 800-160, Vol. 2, Rev. 1, https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

PR.AA-07 doesn't exist

It is stated that subcategory PR.PT-04 was moved to PR.AA-07. We assume this to be an editorial mistake as PR.AA-07 doesn't exist. Note that PR.AA-06 does refer to PR.PT-04 as a former subcategory.

2. Examples for the NIST CSF 2.0

DE.CM-03: Detect comprised accounts using behavior analytics software

DE.CM-03's example Ex1 correctly advises the use of behavior analytics software to mitigate insider threats. However, the same technology can also be used to detect compromised accounts i.e., not limited to insiders. We recommend enhancing example Ex1 accordingly:

> **Ex1:** Use behavior analytics software to detect anomalous user activity to mitigate insider threats or compromised accounts

DE.CM-09: Detect comprised devices using behavior analytics software

An unlocked device may be compromised when the user leaves it behind in a restaurant or a ride-share. Such compromises may be detected by observing the location of the device coupled with usage patterns, or compared with locations of other devices registered to the same user. We recommend adding an example accordingly:

> **Ex:** Use behavior analytics software to determines anomalous / unsafe or even typical behavior based on numerous factors, including location information, biometric signatures, and other contextual information associated with a user's endpoints

DE.CM-09: Offline malware detection

Many malware detection solutions need a connection (e.g., to the cloud) to remain relevant or seek assistance in convicting actual malware. Enterprises seeking to protect their resources against malware should consider whether relevant protection is needed when a resource's connection to the Internet is absent, disrupted or impaired. Note that malware is evolving quickly, especially with growing access to Generative AI-based malware factories. We recommend adding the following consideration when seeking protection against malware:

> **Ex:** Use technologies providing relevant protection even when connectivity is absent, disrupted or impaired

PR.AA-03: Use multifactor authentication judiciously

PR.AA-03's example Ex1 correctly requires the use of multifactor authentication. However, it should be noted that frequent use of multifactor authentication can interrupt the normal workflow and cause "security fatigue"[3]. We recommend enhancing example Ex1 to suggest risk-informed activation of multifactor authentication e.g., when a risk score fails to meet a certain threshold:

> **Ex1:** Implement multifactor authentication and activate it judiciously

[3] NIST, https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly

PR.IR-03: Achieve resilience requirements in normal situations

All three current examples (Ex1, Ex2, and Ex3) of PR.IR-03 increase availability via redundancy and agility when a system is experiencing degradation e.g., through compromise or failure of a component, or during periods of high load. Each of the three examples reflect good engineering practices but have predictable outcomes.

These measures do not necessarily detect or slow down adversaries "silently" performing discovery and network mapping efforts i.e., prior to exploiting any (yet-to-be) discovered weaknesses. Implementing principles of moving target defense – including deception, dynamic positioning, and non-persistence techniques – frustrate and expose adversaries. We recommend adding the following example of achieving resilience in "normal" situations:

> **Ex:** Randomize and automate moving target defense to detect and deter attackers, decrease successful exploitations of vulnerabilities, and prevent sustained mapping of target infrastructure

RS.CO-02: Incident notification

When developing an incident response plan, enterprises should consider that normal communication channels may be severed. A dedicated and separate secure notification system can act as a single source of truth, preventing ambiguity during moments of crisis. We recommend adding the following example:

> **Ex:** Ensure notifications can be trusted and do not cause ambiguity; consider that normal communication channels may be severed or compromised

3. Conclusion

The proposed enhanced Cybersecurity Framework Profile and its accompanying resources are helpful guidance and can serve to improve existing risk management processes. BlackBerry recommends enhancing or adding examples of achieving further resilience, including resilience against compromised or even severed communication channels, and resilience during day-to-day operations when adversaries may be preparing to launch an attack. Furthermore, modelling of behaviors may detect compromised accounts or devices. We believe this is the surest path to benefit from adhering to the Framework.

We appreciate the opportunity to offer our input. Mr. John-Luc Bakker [redacted] is available to respond to any questions concerning BlackBerry's response.

Respectfully submitted,

J.H.L. Bakker

John-Luc Bakker
Director, Standards

BlackBerry Corporation
[redacted]