From:	Barzan Ahmed
To:	cyberframework
Subject:	Feedback and Suggestions on the NIST Cybersecurity Framework 2.0 Draft
Date:	Monday, August 14, 2023 11:48:14 AM
Attachments:	image001.png image003.png

Hello NIST CSF Team,

I hope this email finds you in good spirits. I'd like to start by commending the incredible work that has gone into the evolution of the NIST Cybersecurity Framework over the years. As a passionate follower and user of the framework, I've appreciated the strides made in refining and optimizing it to address current cybersecurity needs.

Having reviewed the latest draft of the NIST Cybersecurity Framework 2.0, there is much to praise. The renaming, enhanced focus on governance, better integration of NIST's Privacy Framework, and emphasis on people, processes, and technology are particularly commendable.

However, there are a few points I'd like to highlight:

1. Awareness and Training Controls: Roger Grimes, Data-Driven Defense Evangelist at KnowBe4, has articulated concerns about the reduction of Awareness and Training controls. The continuous surge in social engineering and phishing attacks underscores the paramount importance of this aspect of cybersecurity. While the proposed consolidated controls in the new draft are concise, I share the concern that it might inadvertently reduce the urgency and focus organizations place on comprehensive awareness training. The recommendations provided by Grimes, including monthly security awareness training and simulated phishing campaigns, are particularly salient and worth considering.

2. Governing in the Cloud: It's vital to have more pronounced controls addressing governance in cloud environments. As cloud adoption accelerates, the risks associated with misconfigurations and other cloud-specific vulnerabilities also rise. Misconfigurations in the cloud have, alarmingly, become one of the root causes of breaches in cloud environments. Additional controls, guidelines, or examples highlighting best practices for cloud governance would be of immense value.

Emphasizing the need for routine reviews and assessments of cloud configurations is pivotal. This proactive approach can significantly mitigate the risks posed by overlooked misconfigurations and ensure organizations maintain a secure cloud posture.

The evolution and success of the NIST Cybersecurity Framework have always been a collaborative effort, with feedback from various stakeholders playing a pivotal role. In that spirit, I sincerely hope that my feedback, along with that of other experts in the field, will be taken into account to ensure the Framework remains as effective and pertinent as ever.

Thank you for your tireless dedication to strengthening our cybersecurity landscape. I eagerly await the official release of the NIST Cybersecurity Framework 2.0 and am confident in its positive impact.

Kind Regards,

Barzan Ahmed
Security Analyst
[redacted]
merchantsfleet.com | Great Place to Work
electrifyfleet.com – Join us on the Road to Electrification