[redacted]
Subject: EXT :FW: Comment on Proposed Significant Updates to the CSF 2.0 [Ali Chadli]
Date: Monday, March 20, 2023 11:24:07 PM

[redacted]
Sent: Saturday, March 18, 2023 2:19 AM
To: cyberframework <cyberframework@nist.gov>
[redacted]
Subject: Comment on Proposed Significant Updates to the CSF 2.0 [Ali Chadli]

Name: ***Ali Chadli***
Company: ***Glotario LLC.***
Date: ***03/13/2023***

Hi,

I would like to submit the following two items below towards developing the NIST CSF 2.0 special publication.

1. Identify Sources of Privacy & Cybersecurity Requirements

1.1) Problem Statement:

Throughout past experiences, some organizations get surprised or even shocked when they have overlooked some requirements sources and discovered them at the last minute. Some examples:

- Company A makes OTT (Over the Top) communications services. They were already launched in the US market and they were planning to launch in Europe. The last minute when they tried to upload their mobile up to the Apple Store, they got blocked because they needed pre-approval from local authorities as all encrypted communications under that jurisdiction need to go through a specific process with the authorities in order to be allowed in the country. So the launch didn't go

as planned. Had they had the relevant role in the organization, they could have foreseen the issue and made the proper arrangements in-time.

- Company B provides services that ultimately will be collecting PII (Personally Identifying Information) of EU (European Citizens). If the GDPR law is applicable to the organization services, they would be hit with very hefty fines up to 3% of their global turnover.

- Company C makes products that they intend to provide to the US government. If they have the right roles in their organization, they can start tailoring security requirements to meet NIST SP 800-171 for example based on the product security profile educated guess.

1.2) Discussion and Solution:

All entities (businesses small or large, agencies etc..) have to be aware of what cybersecurity and privacy mandates or choices that are the source of their cybersecurity and privacy requirements. Some examples are:

- Government: NIST/DoD, FedRAMP, 800-53, 800-218 etc..
- Industry Vertical Specific: HIPAA, PCI DSS
- Industry Standards Organization: ISO, ANSI, IEC, SOC
- Privacy Laws: GDPR, California CCPA,
- Country Specific laws and regulations
- Survival Security (just to stay afloat)

Organizations need not only to identify these sources that apply to them but they also should have in their governance the right roles who are responsible for identifying the proper sources and lining up the organization's objectives to meet the relevant requirements.

Having the right roles in place will ensure that organizations know what they should be and how to get there without losing the path.

2. Feedback Loop

2.1) Problem Statement:

I have witnessed with several clients and employers the fact that some issues; even when identified and thought to be mitigated; re-appear again and again. Sometimes they are not isolated incidents but rather can be seen as patterns. My analysis is that

patterns always emerge and it is a huge waste of time, resources and even credibility. This calls for process improvement.

2.2) Discussion and Solution:

Repeat offenders call for a traceable path all the way to the requirements. Patterns emerging and repeating means somewhere along the line there are irregularities; let's call them process weaknesses. If these weaknesses are not properly rectified, then the requirements have to change in a way to produce consistent and quality results.

So the recommended feedback should loop from the identified weaknesses to the requirements in form of:

- Lessons learned from high profile failures should be considered as opportunity to self review; especially from outside the organization (high profile breaches)
- Repeat failures should produce requirements review and update
- Improvement actions to continuously improve security process quality and performance

Thanks and regards
ali