[redacted]
[redacted]
Subject: EXT :FW: Supply Chain Governance
Date: Thursday, March 9, 2023 1:45:01 PM
Attachments: image001.png

CAUTION: This email originated from **outside** your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

FYI

[redacted]
Sent: Wednesday, February 15, 2023 10:50 AM
To: cyberframework <cyberframework@nist.gov>
[redacted]
Subject: Supply Chain Governance

Hi,

Thank you for holding the workshop and leading this critical work.

Few comments from Kevin and Jon prompted me to send some thoughts on supply chain risk management from a governance point of view. I will not be able to attend the supply chain panel.

Governance can also play a key role in managing and mitigating third party risks. It starts by tiering your suppliers by risk presented to your organization (if they are down or compromised)

1. For critical suppliers, at a minimum, have full visibility into their critical dependencies, their third parties (fourth parties). Including use of industry utilities.
2. Set risk metrics / thresholds that can be used to assess suppliers in those tiers. And ensure contractually that the third parties are obligated to report to you on those metrics.
3. Examples of metrics could be -
    a. Do they have / use a CSF or equivalent framework
    b. Do they have / test their Disaster Recovery and Business Continuity capability and does that include cyber
    c. Do they have good cyber hygiene …to deal with phishing, social engineering, weak passwords, and timely patching of vulnerabilities. Do they train their employees.

Governance can ensure that your third parties are obligated to not just report to you but periodically join your BCP/cyber exercises.

Best,
Sumeet

Sumeet Chabria
Founder and CEO, ThoughtLinks Group


ThoughtLinks
POWERING THE WORLD OF NEW IDEAS