From: Brian Cummings
Sent: Monday, December 17, 2018 12:40 PM
To: privacyframework
Subject: NIST Privacy Framework

Katie:

Some thoughts on the proposed NIST Privacy Framework.

1. Cultural "Will to Protect": Leadership and culture is critical to an entity's privacy governance and execution. An entity must, by decision, choose and act as a prime business directive to protect private information and use the information in an ethical manner. Absent such strong leadership and culture, an entity will struggle to achieve effective privacy protection.
2. Ethical Use of Data: It would be useful for entities to adopt the Data Ethics & Privacy practices of Acxiom Marketing Services (Now owned by IPG). Acxiom presents three categories of increasing restriction on the use of private information: 1) What is technically possible (the broadest category); 2) What is legally permissible (Usually lags how data is made available and used); and 3) What is Acceptable to your customers. Acxiom's Data Ethics & Privacy practices target to achieve "Acceptable" use of data, the most restrictive category.
3. Network Segmentation: As a standard security practice, it is essential to isolate personal information, and perhaps even different categories of information into highly secured (Zero Trust) network segments. The secure segments should fully implement the Top Twenty Critical Security Controls and mitigate the OWASP Top Ten Critical Web Application Security Risks. Many entities continue to allow private information to proliferate across their technical environment, making it impossible to protect or driving an excessively high cost of security.
4. "Aggressive Vigilance": There are notable entities who have for several years avoided being the victim of a security breach by practicing what I call "Aggressive Vigilance." Their Security Operations include a team that focuses on cyber-activity and cyber-attacks. They understand the rhythm and flow of the of the business and network activity, and monitor for anomalies. The "aggression" comes in on anomaly detection, at which time these entities immediately interdict the activity and launch an investigation. Under the "Will to Protect", these entities deem an interruption of a business service as preferable to allowing malicious activity to progress down the cyber-kill chain.