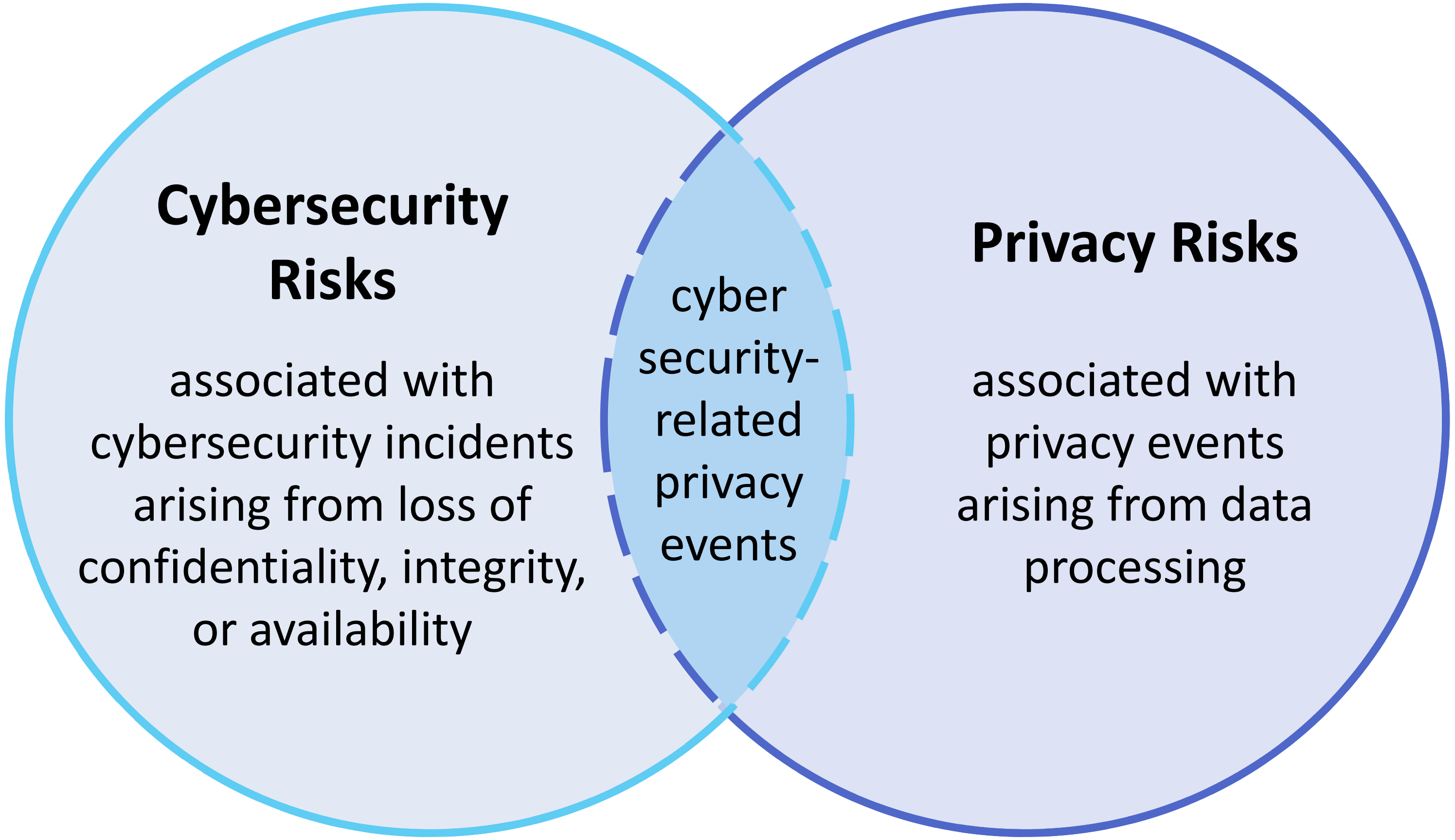
Privacy Considerations: an Overview

Naomi Lefkovitz, Senior Privacy Policy Advisor, Information Technology Lab, NIST

January 26, 2021

Relationship Between Cybersecurity and Privacy Risk



Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

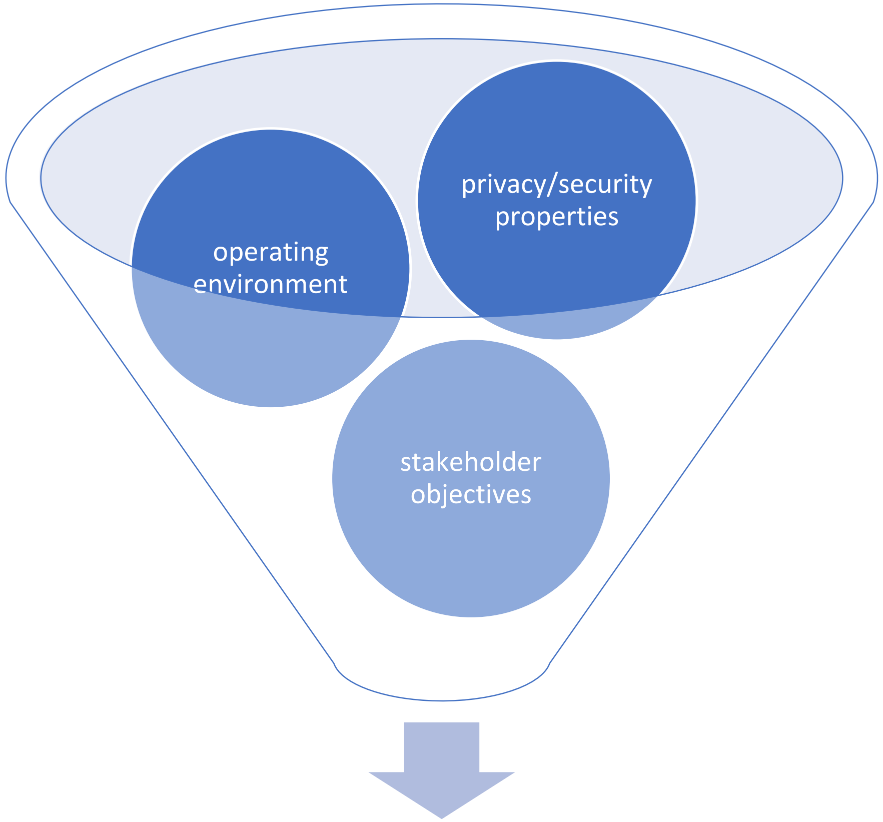
Privacy Framework Profile Extract

NIST Privacy Framework Core			*Capabilities/Policies*
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.	• Privacy policies, processes, and procedures governing the data processing are clearly articulated. At a minimum: o Individuals use of the tool is voluntary (opt-in). o Data processing is minimized (including collection, retention, and disclosure of specific data elements) to the degree necessary to enable individuals to determine if they have been in physical proximity with an infected individual and to receive information about response measures. o Retention periods are established for all collected data. o De-identified, aggregate data may be used for epidemiological purposes. o No other data uses are permitted.
		GV.PO-P2 - GV.PO-P4: …	
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	The tool functions in a manner that complies with any applicable privacy and security legal, regulatory, or contractual requirements.

Privacy Framework Profile Extract (con’t)

NIST Privacy Framework Core			***Capabilities/Policies***
CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Disassociated Processing (CT.DP-P):** Data processing solutions increase disassociability consistent with the organization’s risk strategy to protect individuals’ privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).	State of the art technology to limit the observability and linkability of the data processing with individuals is implemented. o Individuals’ data are stored on their local devices unless contraindicated by the risk assessment conducted under the Risk Assessment Category (Identify Function).
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).	State of the art technology to limit the identification of individual users is implemented. o User-initiated queries are used for infection proximity alerts, rather than system-generated notifications. o Data used for epidemiological purposes are aggregated and de-identified with provably strong confidence

Understanding Tradeoffs



Technology Solution

Resources

Websites

NIST Privacy Framework: https://www.nist.gov/privacyframework

NIST Privacy Risk Assessment Methodology: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources