



How to build a #TETHICAL Company

The power found in good
Data Privacy Policies

Who are we?





Who are we?

Christine Theobald

- Volunteers with Cincinnati CinPA Security SIG
- Infrastructure Engineer
- @ChristineThe7

Micah K Brown

- @MicahKBrown
- Queen City Con
- Co-host ThreatReel Podcast
- Smoker of fine meats and finer cocktails



Disclaimer!

- We are not Lawyers.
- Our thoughts and views should not be considered legal advice.
- Our thoughts and views are that of our own as Independent IT Security Practitioners.
- Talk to your friendly Lawyer(s)!



So, yea have you heard about our Data Privacy Policy?

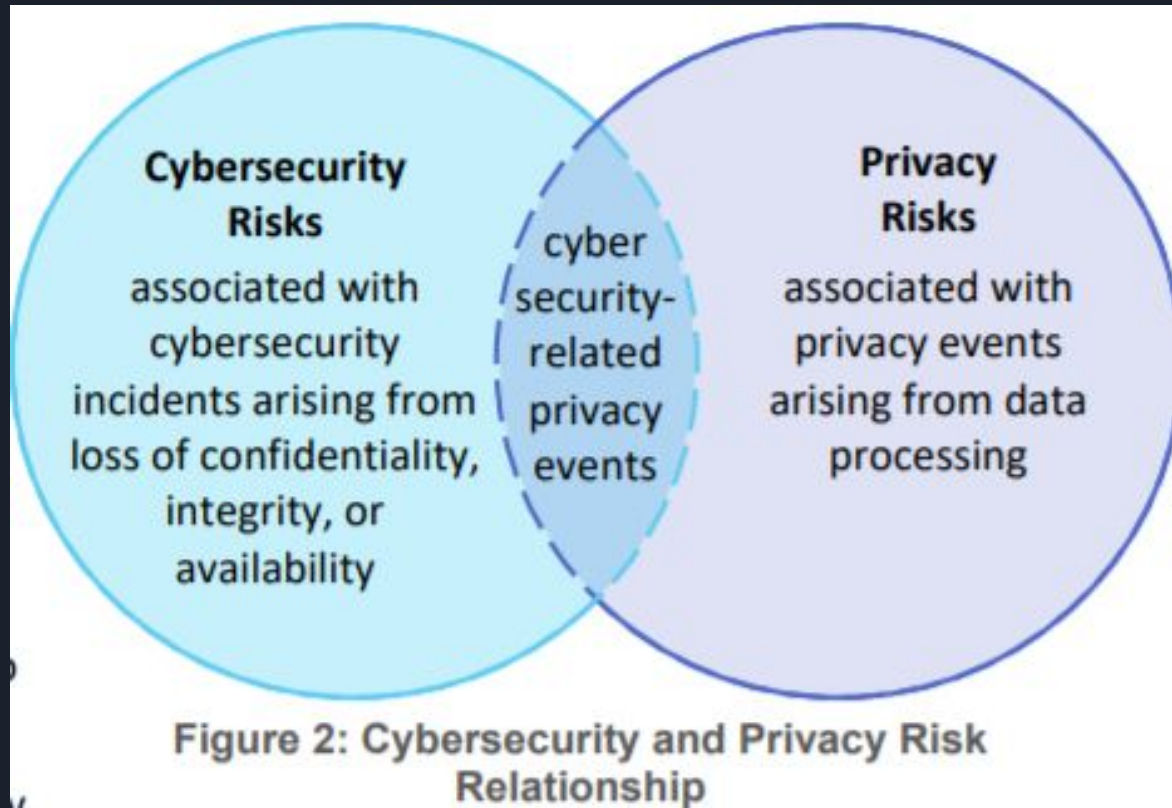




What is Data Privacy?

- Data Privacy is the right to have control over how personal information is collected and used.
- Data Privacy, Information Privacy, Data Protection are sometimes used interchangeably.
- For example, EU refers to Data Privacy as Data Protection while others see Data Protection as the first step of data privacy by first keeping the data from unauthorized disclosure.
- “Data Privacy or Information Privacy is a branch of Data Security concerned with the proper handling of data - consent, notice and regulatory obligations.” Varonis.com
- Privacy Risks can arise unrelated to Cybersecurity related risks.





NIST Privacy Framework Figure 2 (P3)

Why implement formal Data Privacy Program?

Data is one of the most important and valuable assets of a company

Privacy is the right of an individual to be free from uninvited surveillance
- (Varonis.com)

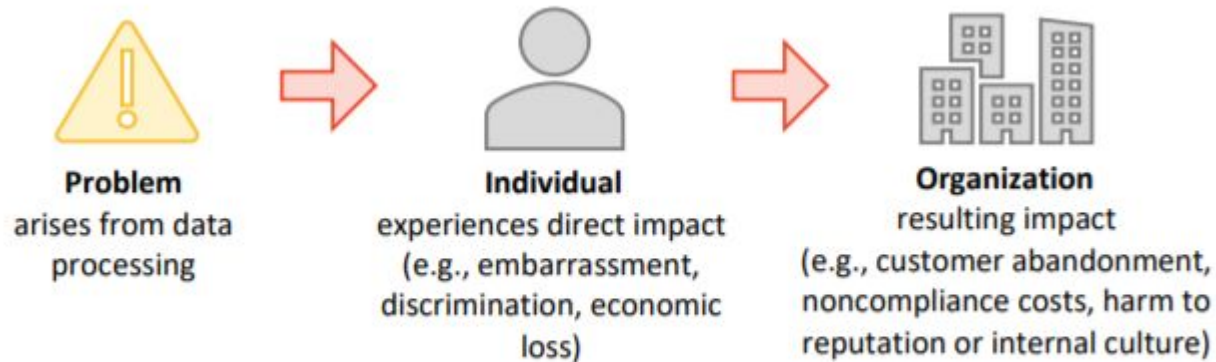


Figure 3: Relationship Between Privacy Risk and Organizational Risk





Should Data Privacy be part of IT Sec?

- Data security or IT Security protects data from compromise by external attackers or malicious insiders
- Data Privacy governs how data is collected, shared, and used
- Data Privacy and data security need to be well connected and collaborating teams



Examples





HIPAA - Health Insurance Portability and Accountability Act of 1996

- Protects PHI or Personal Health Information
- Ensures the CIA of all ePHI
- Protect against anticipated impermissible use or disclosure.
- Applies to Healthcare Providers, Health Plans, Healthcare Clearinghouse, Business Associates.



Photo by [Hush Naidoo](#) on [Unsplash](#)





FCRA - Fair Credit Reporting Act

- Protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services.





ECPA - Electronic Communications and Privacy Act

- Protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers
- Applies to email, telephone conversations, and data stored electronically





GDPR - General Data Protection Regulation

- Applies to residents of EU
- Lots of rights
- Right to rectification
- Right to erasure 'right to be forgotten'
- Right to data portability
- Right to object





NYDFS - New York Department of Financial Services Cybersecurity Regulation

This regulation imposes strict cybersecurity rules on covered organizations, such as banks, mortgage companies, and insurance firms. The regulation requires financial companies to install a detailed cybersecurity plan, enact a comprehensive cybersecurity policy, and initiate and maintain an ongoing reporting system for cybersecurity events.

The NYDFS Cybersecurity Regulation requires institutions to adopt a robust cybersecurity program ideally aligned to five core functions set forth by the NIST Cybersecurity Framework (CSF)





CCPA - California Consumer Privacy Act of 2018

- Applies to CA residents
 - Right to know
 - Right to delete
 - Right to opt out of sale
 - Right to non-discrimination for exercising CCPA rights
- Personal Information under CCPA includes:
 - Name, SSN, Email
 - Records of purchases, Browsing history
 - Geolocation data
 - Fingerprints
 - Inferences - A profile created from other personal info about your preferences and characteristics






CPRA - California Privacy Rights Act of 2020

- CPRA Approved Nov. 3, 2020
Proposition 24
- California Privacy Rights Act of 2020
- Establishes a stand alone privacy regulator - the first state to do so
- CCPA will be incorporated into CPRA Jan 1 2023
- Establishes new consumer right - The right to correct inaccurate personal information (i.e. the right to rectification)
- It is limited on the nature and purpose of the processing of PI
- Establishes a subcategory of PI as sensitive personal information
- Govt issued identifiers
- Financial info
- Precise geolocation
- biometric/genetic info
- Racial, ethnic origin, religious/philosophical beliefs, union membership
- PI concerned health, sex life, sexual orientation
- Contents of mail, email, text messages unless the business is the intended recipient of the communication



Why build a Data Privacy Framework?






Show leadership in privacy by adopting the Privacy Framework to support:

- Building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole
- Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and
- Facilitating communication about privacy practices with individuals, business partners, assessors, and regulators.
- <https://www.nist.gov/privacy-framework/new-framework/adoption>





How to get started – Enter NIST Data Privacy Framework

- What is the NIST Data Privacy Framework?
- It is structured with the same Core, Profiles, Implementation Tiers as the Cybersecurity Framework in order to facilitate use of both frameworks together
- It is intended to help organizations build better privacy foundations by bringing privacy risk into parity with their broader enterprise risk portfolio





How to Implement NIST Data Privacy Framework?

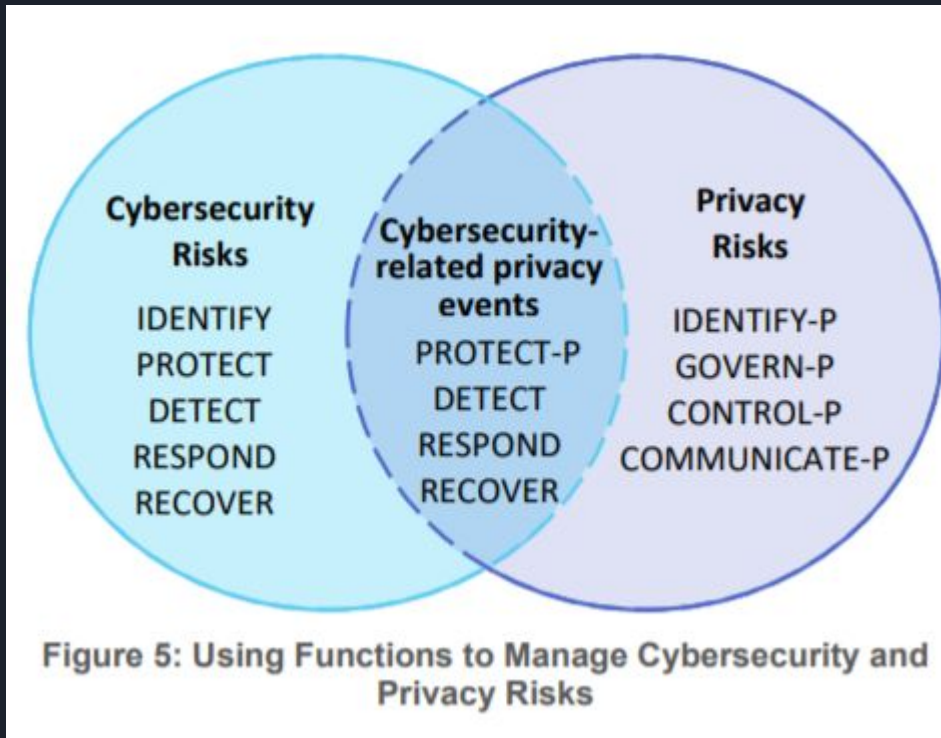
Core - the dialogue about important privacy protections activities and desired outcomes

Unique:

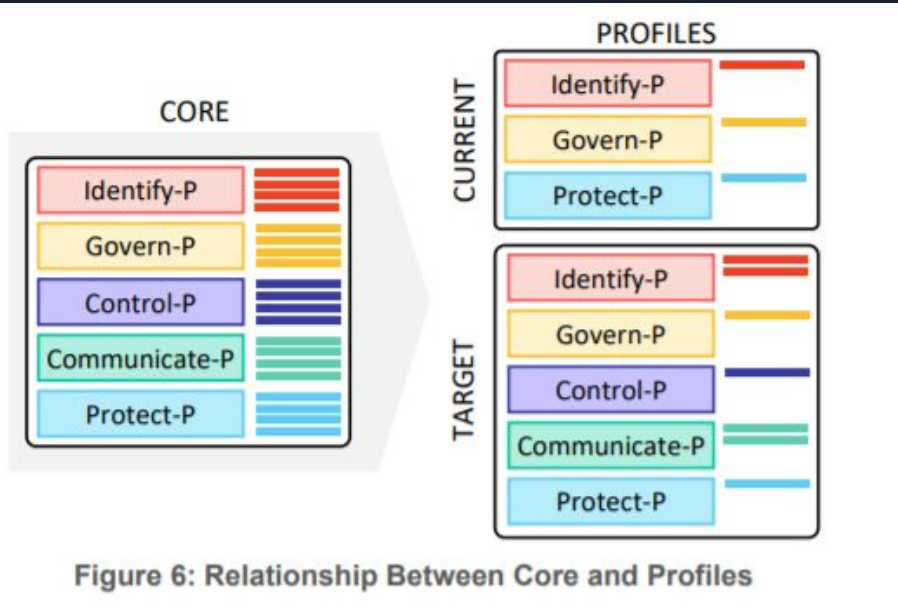
- Identify-P
- Govern-P
- Control-P
- Communicate-P
- Protect-P

Shared:

- Protect-P
- Detect
- Respond
- Recover



Profiles



- The prioritization of the outcomes and activities that best meet organizational privacy values, mission or business needs, and risks
- Prioritizing the outcomes based on individuals needs
- Also represents current privacy activities and/or desired privacy activities and outcomes - Current → Target



NIST Privacy Framework Figure 6 (P8)



Implementation Tiers

- Decision-making and communication about the sufficiency of organizational processes and resources to manage privacy risk
- Action steps and feedback loop - Is the process working? Is this action meeting our goals?
- When considering Target profiles, what tiers can be used to achieve the target profile



Table 1: Privacy Framework Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>



DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Functions from NIST Cybersecurity Framework

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>






Russ: Are you telling me I can dodge lawsuits?
Christine: When you have good Data Privacy,
you might not need to!



Function - Protect - P

- Develop and implement appropriate data processing safeguards
- Covers data protection to prevent cybersecurity related privacy events, one of the overlaps between privacy and cybersecurity risk management





Category - Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.


Subcategory - PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

- How is this being accomplished? Do you have a process for verifying that credentials are updated and least privilege is applied.

Subcategory - PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).

- How is this being accomplished? VLANs? Trunking? Pruning the switches? Protecting against VLAN hopping? NAC?





Category - Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.

Subcategory - PR.DS-P2: Data-in-transit are protected.

- How is this being accomplished? What encryption algorithms are being used? VPN or Remote desktop? What about data transmitted over voice or video?

Subcategory - PR.DS-P5: Protections against data leaks are implemented.

- How is this being accomplished? Do you have a Data Classification system? Do you have DLP? Is it working? Are you inspecting your internet egress traffic? Are you enforcing web proxy / CASBY / SASE? Can users bypass your controls? How are you sure it is functioning as planned?





Function - Control - P

Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks

- **Category** - Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).
 - Subcategory - CT.DM-P3: Data elements can be accessed for alteration.

This will be required for compliance with CPRA and the right to correct inaccurate data about an individual. Is this capability built into the software development life cycle?






Getting Started - Ready, Set, Go

Getting Started Guide

<https://www.nist.gov/system/files/documents/2021/01/13/Getting-Started-NIST-Privacy-Framework-Guide.pdf>

1. Ready - use the Identify-P and Govern-P functions to get 'ready'
2. Set - Set an action plan based on differences between current and target profiles
3. Go - Go forward with implementing an action plan





Why you should consider a building a Formal Data Privacy Program!

Data Privacy is not the same as Data Security.

Data Privacy includes the right to be make decisions about the use of your personal information.

The Privacy Landscape is constantly changing with new rules, laws, and regulations.

Start small - Pick 1 function to start developing.

The Framework can be used dynamically.

- Starting with the Action Steps and mapping back to the Cores
- Starting with the Cores and mapping down to the Action Steps





Who are we?

Christine Theobald

- @ChristineThe7
- Volunteers with Cincinnati CinPA Security SIG
- Infrastructure Engineer

Micah K Brown

- @MicahKBrown
- Greater Cincinnati ISSA
- Queen City Con
- Co-host ThreatReel Podcast
- Smoker of fine meats and finer cocktails



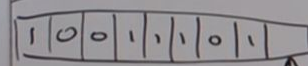
02MOG020V

$$u(x) = \min_{p: u(p) = x} |p|$$

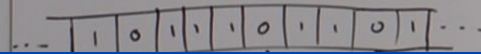
OPTIMIZE OVER programs SYMBOLICALLY

$p: S_1, S_2, S_3 \dots$
 $\uparrow \quad \uparrow \quad \uparrow$
 Integrals

SOLÉNOÏDE INDUCTION



$$P(x_n | x_1, \dots, x_{n-1}) = \sum_{\substack{p: p \text{ int} \\ x_1, \dots, x_{n-1}, x_n}} 2^{-|p|}$$


$$\# [K(X)] \approx H(X)$$

8.223 GB

SENT

\neq ?
8.2176

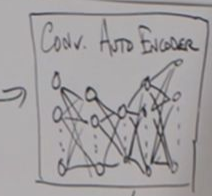
RECEIVED

277

~~max~~
~~bits~~
~~message~~
 $x \leftarrow \text{chat message}$
 $c(x) \leftarrow \text{m/o compress}$
 $c(x) \leftarrow \text{encrypted}$
 $c(x) \leftarrow \text{AI compressed?}$

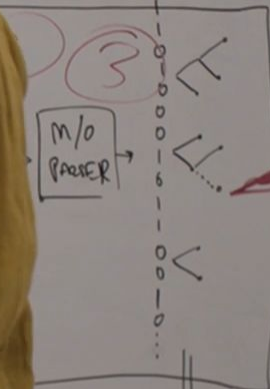
RECOVERED
MESSAGE
("...")

MASSIVE DATASET
A.bnp
AA.bnp
⋮



R.H.

FILE x12



FILE. PA

Thank you! Questions?