Demystifying the Privacy Landscape for the Cybersecurity Professional

ABOUT ME

Ken leads Lowenstein Sandler's information security and data privacy programs. He has more than 20 years of experience implementing and supporting secure, complex information technology infrastructures. Ken's detailed knowledge of security and network methodologies, techniques, and best practices enables him to thoroughly assess and remediate cybersecurity threats and vulnerabilities.

He is President of the New Jersey Chapter of $(ISC)^2$, and is also a member of the Executive and Threat Intelligence Committees of the Legal Services Information Sharing and Analysis Organization (LS-ISAO), a member-driven community providing a secure framework for sharing actionable threat intelligence and vulnerability information.

Ken is a volunteer with the Cybersecurity Workforce Alliance (CWA), which mentors high school and college students who are breaking into the cybersecurity field.

He hold several cybersecurity and privacy certifications including the CISSP, CIPP/US, CIPT, CIPM, CISM and CCSP.

Agenda

1. Why should I care?
2. How did we get here?
3. Understanding the Privacy landscape
4. What types of jobs are available?
5. What resources are there?

WHY SHOULD I CARE?

Privacy laws are gaining ground in the U.S. and around the world

Many cybersecurity officers need to be responsible for privacy as well

Heavy fines and/or penalties for non-compliance

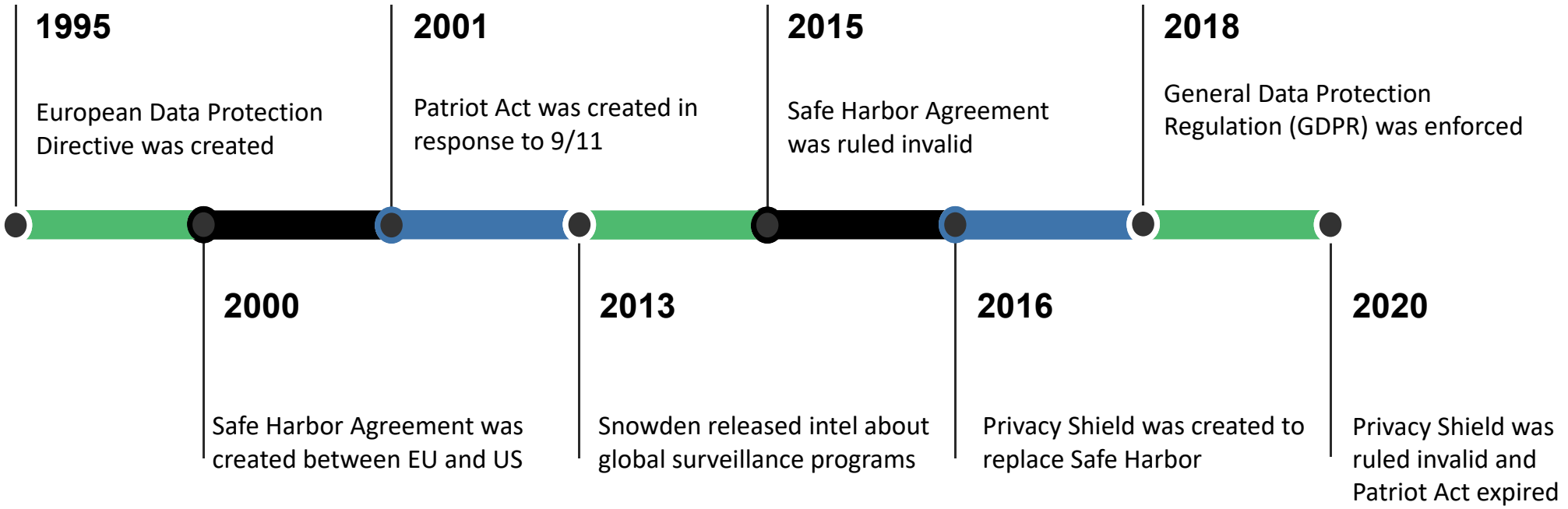
Privacy cannot exist without adequate security

It is one of the fastest growing fields in the U.S.

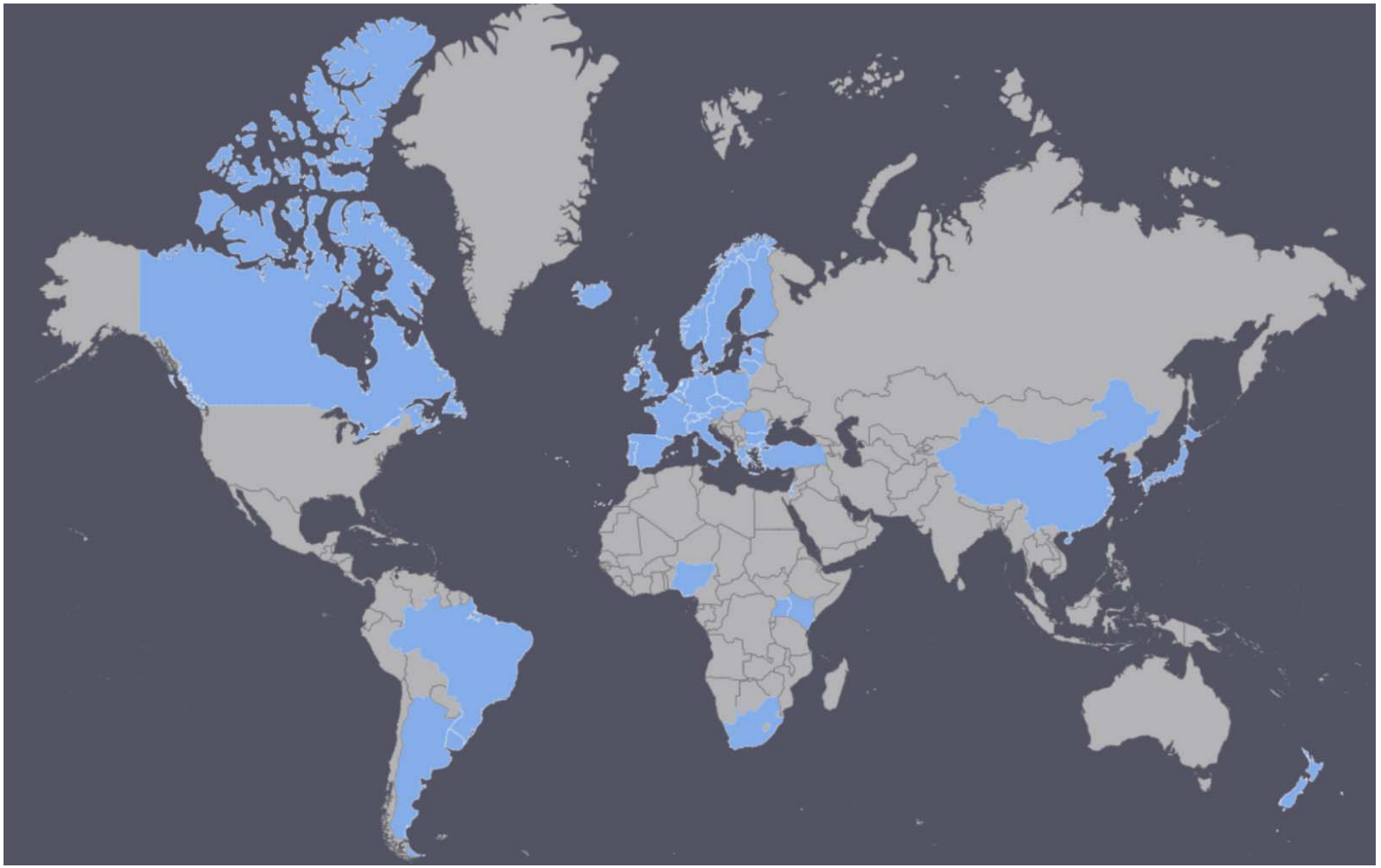
HOW PRIVACY COULD IMPACT A CYBERSECURITY PROFESSIONAL

1. A customer/client requests to be removed from your systems
2. Backups are restored that have customer info that was already removed from your systems
3. A web form requests personal info without explaining why they need it or who has access to it
4. Development is outsourced to third-parties, who use personal data when testing
5. Cookies are tracking more information than what your privacy notification states
6. Your company has decided to enter a new market in another region
7. Time card systems uses biometrics

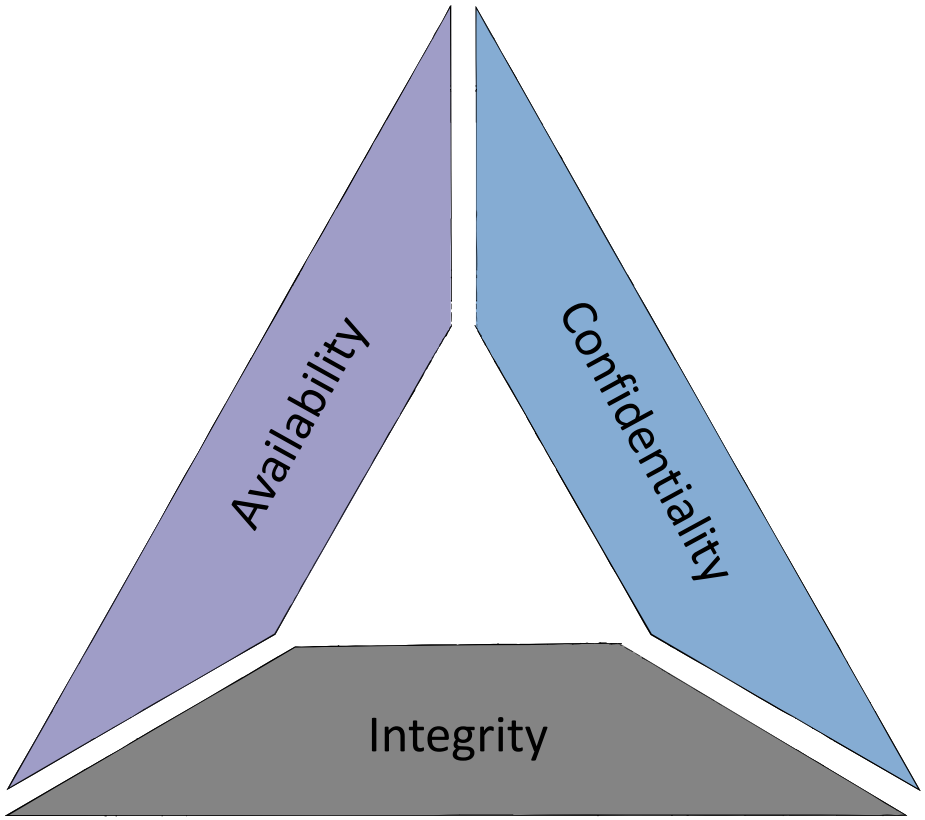
HOW DID WE GET HERE?



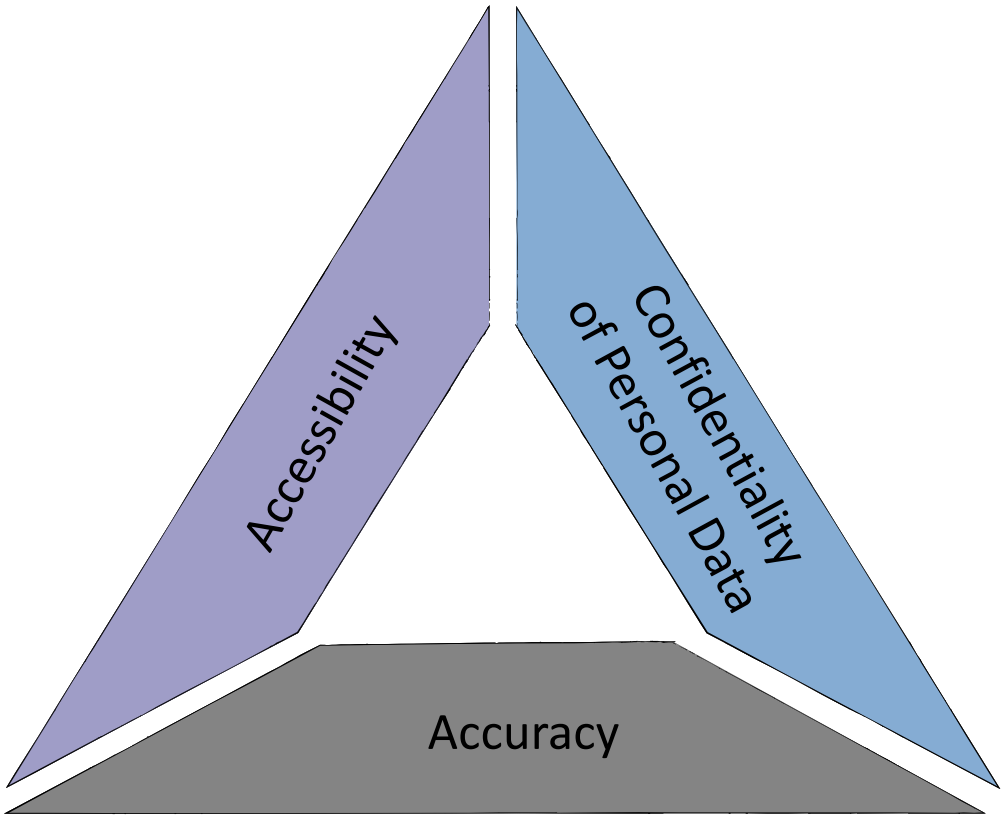
COUNTRIES WITH COMPREHENSIVE PRIVACY LAWS



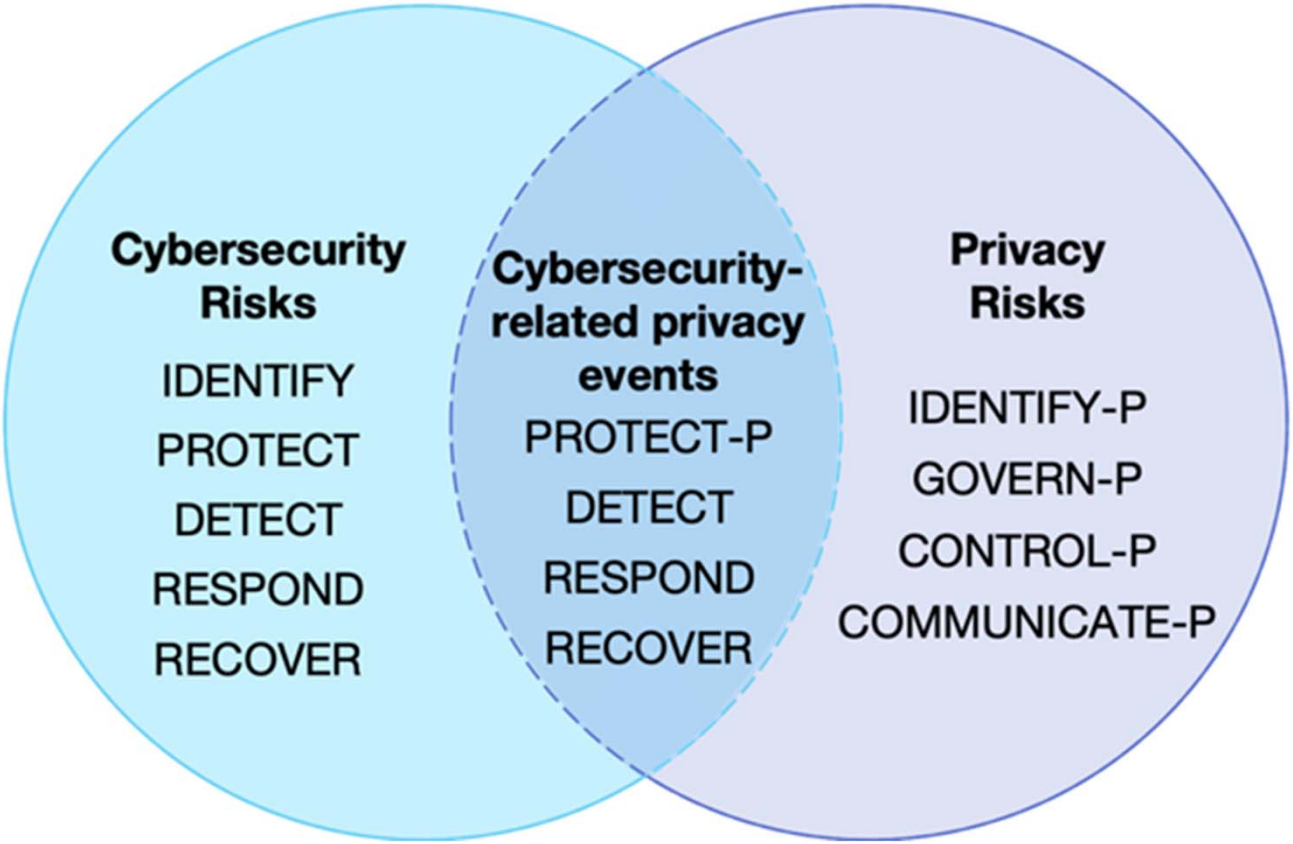
CYBERSECURITY TRIAD AND THE NIST CSF FUNCTIONS



PRIVACY TRIAD AND THE NIST PRIVACY FRAMEWORK FUNCTIONS



WHY CYBERSECURITY IS AN ESSENTIAL PART OF PRIVACY



TAXONOMY CHALLENGES WITHIN PRIVACY LAWS

HIPAA	GDPR	CCPA	VCDPA/CPA	In Plain English
Covered Entity	Controller	Business	Controller	The Company Who Is Responsible For Your Data
Business Associate	Processor	Service Provider	Processor	Vendors That Were Given Permission to Process Your Data
Individual	Data Subject	Consumer	Consumer	You

WHAT DATA SHOULD I BE CONCERNED ABOUT?

Personally Identifiable Information (PII)	Protected Health Information (PHI)	Personal Data (GDPR)	Sensitive Data (GDPR)
SSN#	Medical Records	Online identifiers	Race / ethnic origin
Email address	Medical Billing Information	Biometrics	Trade-union membership
Phone number	Health Insurance	Video surveillance	Sex life or sexual orientation
Drivers license		Potentially any information that relates to an identifiable person	Political opinions
Bank account number		Data obtained directly or indirectly	Religious beliefs

COMMON PRIVACY PRINCIPLES

Notice

What data is used, how is it used and the purpose for collecting. Should be transparent

Choice and Consent

Right to opt-in / opt-out. Data should not be given to third-parties without consent

Access and Participation

Access rights and control of data from owners

Relevancy

Is the data being used for its original purpose and should be obtained lawfully

Security and Accuracy

Are adequate safeguards in place

Enforcement

Owners or custodians of data should be held accountable

COMMON INDIVIDUAL PRIVACY RIGHTS

Data Subject Rights	In Plain English
Right to be informed	What are they doing with my data and are other companies using it?
Right to access	Can I see my data?
Right to rectification	Can they fix my data if it's wrong?
Right to erasure	Can I have them erase my data?
Right to data portability	Can I have my data?
Right to object	Can I object that they have my data?
Right to restrict processing	Can I stop them from using my data?
Personal data breach rights	Can I be notified if my data is stolen?
Right to avoid automated decision-making	Can they stop having a computer determine if I qualify for a loan?

NO CONSENSUS ON CYBERSECURITY FRAMEWORKS

ISO 27001:2013

CIS Controls

NIST

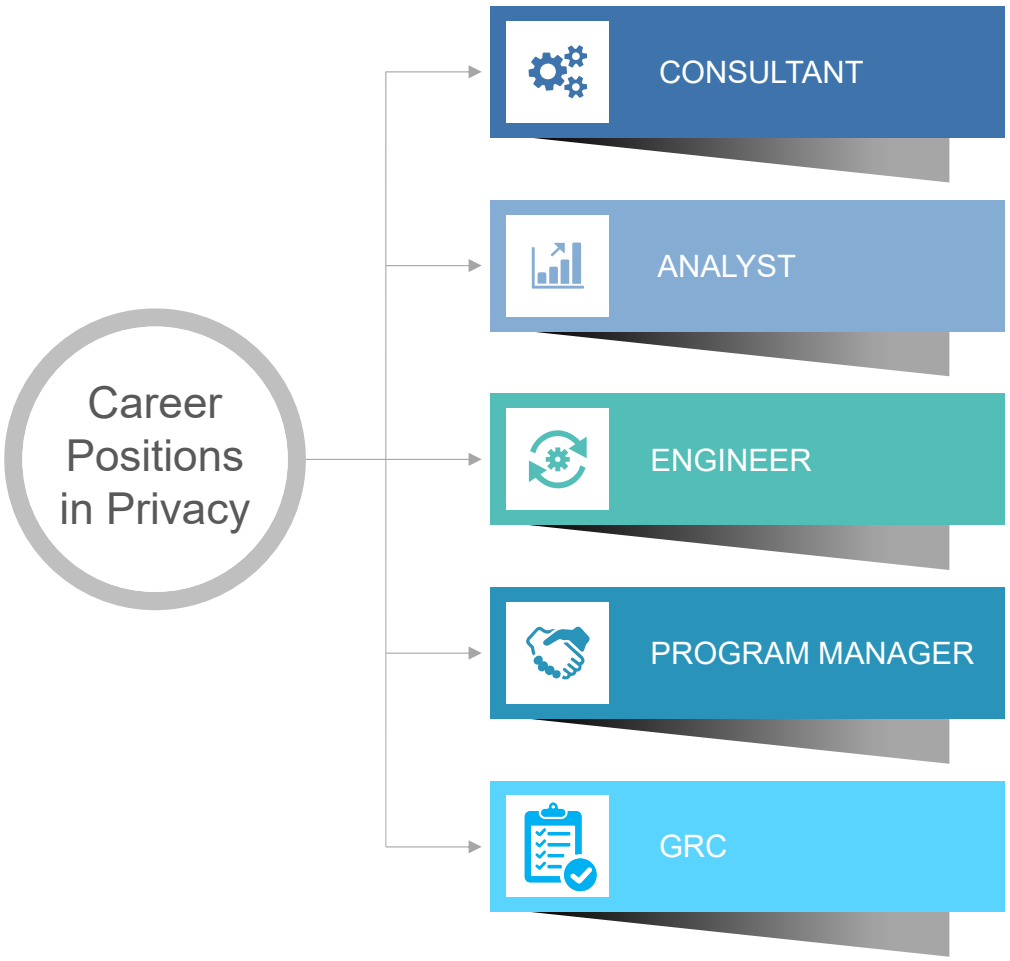
National Institute of Standards

Special Publication 800-53

HOW DO I START DEVELOPING A PRIVACY PROGRAM?

1. Determine scope of assessment and understand your regulatory requirements and client/customer obligations
2. Inventory your data that is in scope
3. Identify the inherent privacy risks of your organization
4. Perform a Privacy Impact Assessment on each system or database
5. Develop Gap Assessment and Risk Register identifying the necessary preventive and corrective controls to implement

WHAT NON-LAWYER PRIVACY JOBS ARE AVAILABLE?



PRIVACY RESOURCES

- IAPP – Conferences, Meetups, Newsletters, Certifications, Podcasts
- NIST Privacy Framework
- ISO 27701 Privacy Framework
- Webinars from OneTrust and TrustArc
- CPO Magazine
- LinkedIn
- Blogs from law firms that have privacy practices

KEY TAKEAWAYS

- The privacy field isn't just for lawyers
- Tremendous momentum in protecting an individual's privacy rights is happening throughout the world
- It is a very dynamic field that is evolving quickly
- More cybersecurity professionals are needed to understand the privacy landscape

Any Questions