RSM

INTERSECTION OF SECURITY AND PRIVACY: HOW A CPO/CISO SUCCESSFULLY WORK TOGETHER

October 3, 2023

Speakers

Chip Stewart

Director, Security and Privacy, RSM US LLP

Baltimore, MD

chip.stewart@rsmus.com

Laura Gomez-Martin

Director, Security and Privacy, RSM US LLP

Pittsburgh, PA

laura.gomez-martin@rsmus.com

Charles Barley Jr

Principal, Security and Privacy, RSM US LLP

McLean, VA

charles.barleyjr@rsmus.com

© 2022 RSM US LLP. All Rights Reserved.

Agenda

- Introductions
- Overview of Security & Privacy
  - How there are different and
  - Where they intersect
- Overview of Chief Privacy Officer role
- Overview of Chief Information Security Officer role
- Bringing it all together, panel discussion
- Audience Q & A

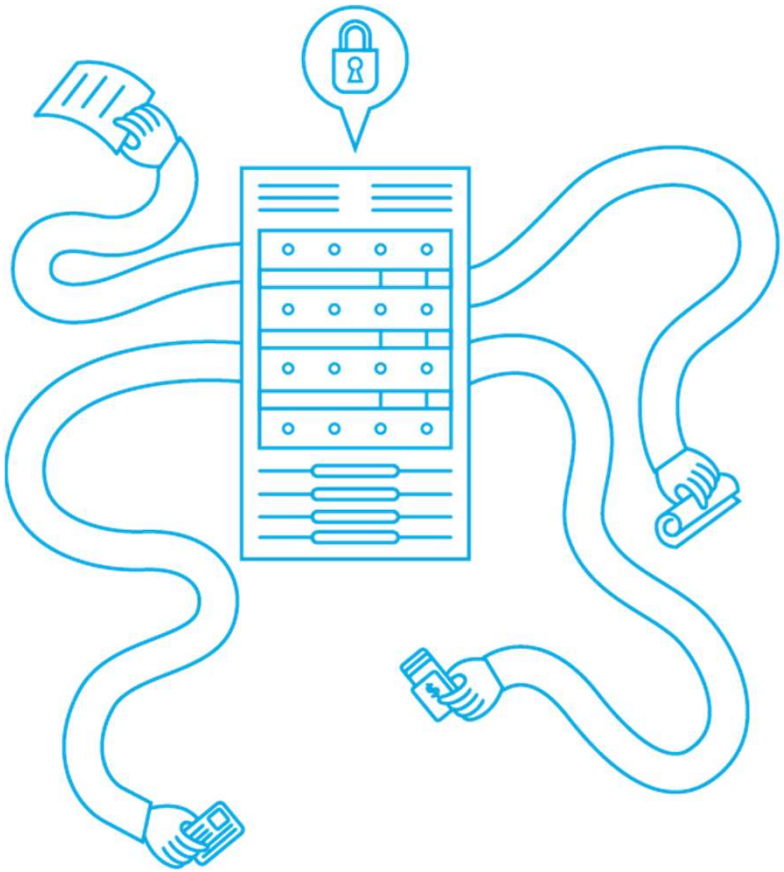
© 2023 RSM US LLP. All Rights Reserved.

RSM

Privacy versus security

Privacy is about…

- Transparency
- Trust
- Individual Rights
- Privacy by Design
- Personal Data

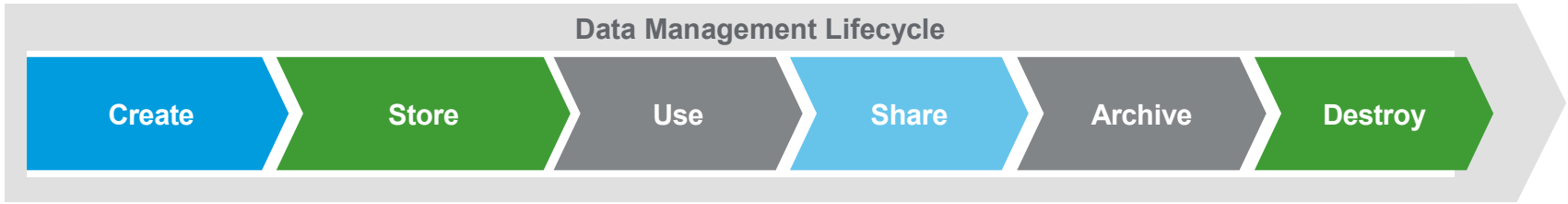


Security is about…

- Confidentiality
- Integrity
- Availability
- DevSecOps
- All data types and environments

© 2023 RSM US LLP. All Rights Reserved.

Convergence of privacy and security



	Create	Store	Use	Share	Archive	Destroy
Privacy	• Privacy by Design • Proper collection of information	• Retention policy • Data Minimization	• Use in line with original consent	• Privacy implications communicated to third-parties	• Retention policy • Data Minimization	• Proper destruction of information • Proper destruction or return from third-parties
Security	• Security by Design	• Adequately protect information according to sensitivity • Implement effective security controls	• Secure Access Management	• Security responsibilities communicated to third-parties	• Adequately protect information according to sensitivity • Implement effective security controls	• Proper destruction of information • Proper destruction or return from third-parties

© 2023 RSM US LLP. All Rights Reserved.

Chief Privacy Officer (CPO) Overview

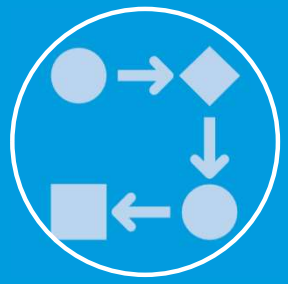
- The CPO role increasing within many organizations
  - Private
  - Non-profit
  - Government

- Within different organizations, the CPO can report to:
  - General Counsel
  - Compliance Team
  - CEO

- In charge of setting and enforcing policy and strategy reflecting privacy principles:
  - Consent
  - Data Limitation
  - Purpose Specification

© 2023 RSM US LLP. All Rights Reserved.

The importance of privacy



Operational Risks

Privacy today is more than just a compliance obligation; it impacts strategic growth, decision making, and operational effectiveness.

Organizations need to manage personal data as it would any other company asset and instill a company culture that respects privacy.

Reputational Risks

Transparency and trust are paramount in the global economy amongst consumers, employees, and business partners.

The impact to a company's brand could be substantial in terms of perception about ethical personal data practices.

Financial Risks

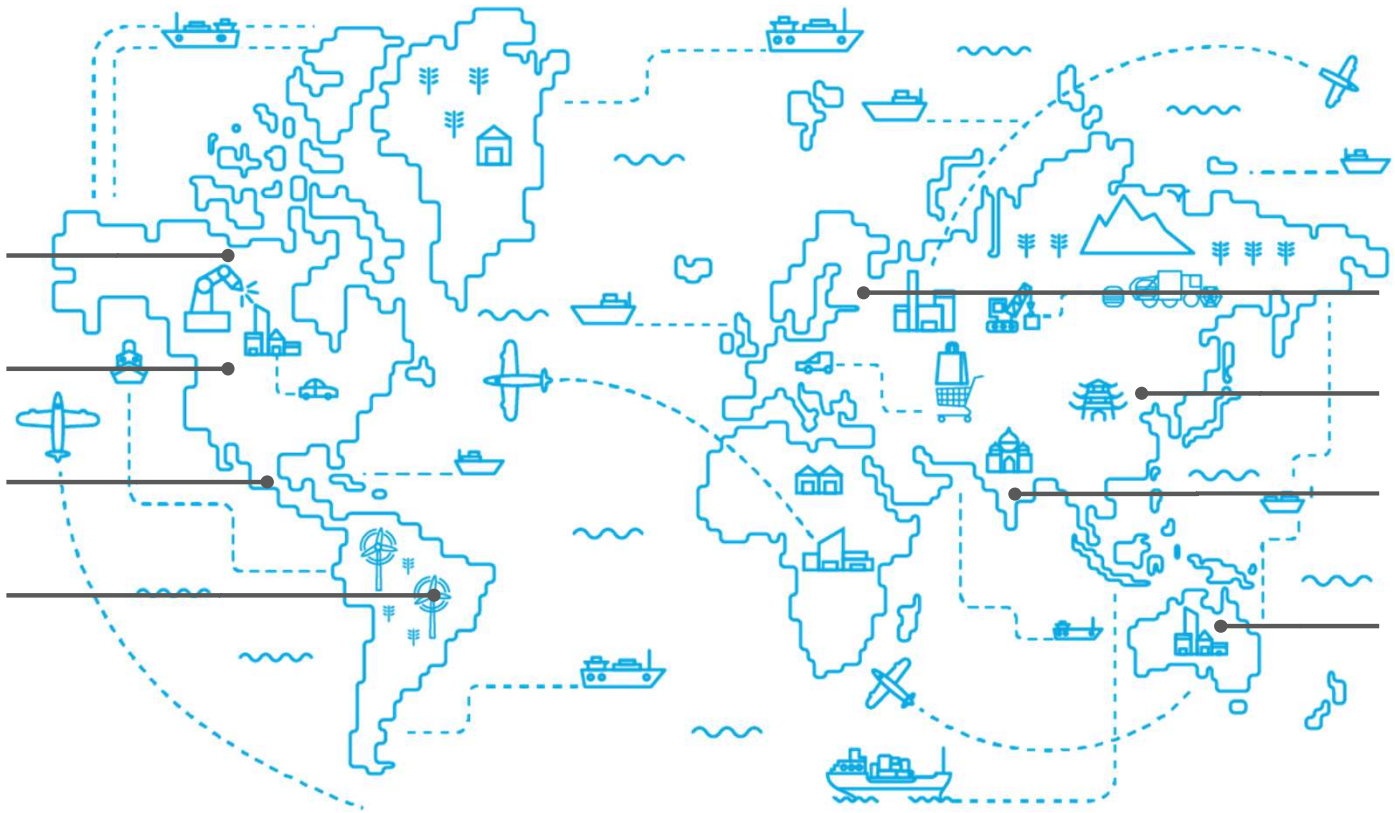
Loss of trust may result in loss of current and future business opportunities.

Enforcement actions from regulatory and supervisory authorities can be costly; or in some instances result in further private legal action from individuals and their attorneys.

Privacy is important as a business and marketplace differentiator.

© 2023 RSM US LLP. All Rights Reserved.

Keeping pace with global privacy requirements



Canada and Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial specific laws and regulations

United States and the federal by industry and state mandated laws and regulations for privacy and breach notification

Mexico and the Federal Law on the Protection of Personal Data Held by Private Parties

Brazil and General Law for Data Protection or Lei Geral de Proteção de Dados Pessoais (LGPD)

European Union and the General Data Protection Regulation (GDPR)

China and the Personal Information Protection Law (PIPL) and Cybersecurity Law

India and the Digital Personal Data Protection Act (DPDP Act)

Australia and the Federal Privacy Act and the Australian Privacy Principles (APPs)

This slide is intended to be illustrative and is not representative of all global laws and regulations for privacy and personal data protection.

© 2023 RSM US LLP. All Rights Reserved.

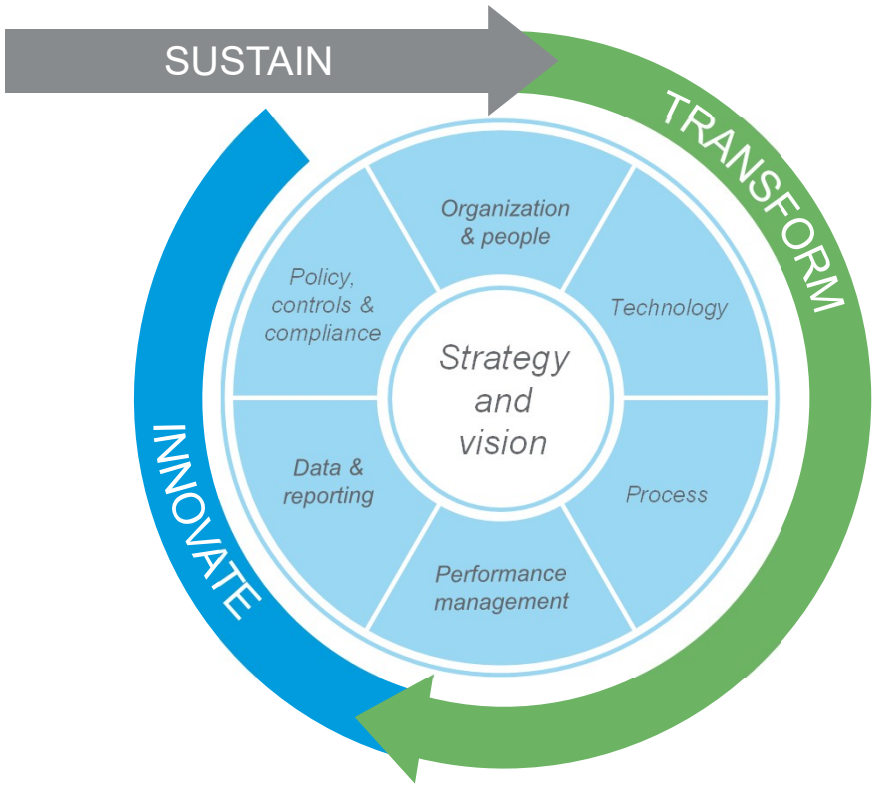
Privacy trends in an evolving landscape

	**Keeping pace with the patchwork of privacy requirements**	**Be anticipatory and future-proofed in the approach**
	**Establishing and sustaining personal data governance**	**Derive business value from sustainable governance**
	**Understanding applicable roles and responsibilities**	**Know the compliance obligations by business impact**
	**Designing and implementing a privacy function that is right-sized**	**Say yes to Privacy by Design (PbD) and integrate methodologies**
	**Having access to the right subject matter expertise**	**There is a talent shortage causing a competitive landscape**
	**Addressing EU-US cross-border transfers after Data Privacy Framework (DPF)**	**New EU-US privacy framework permits data transfer to US under new DPF principles.**

© 2023 RSM US LLP. All Rights Reserved.

Chief Information Security Officer (CISO) overview

Similar to the advocacy of cybersecurity professionals, **privacy must be built in** - not bolted on at the end.



© 2023 RSM US LLP. All Rights Reserved.

Chief Information Security Officer (CISO) overview

46%

Of cybersecurity incidents resulted in the exfiltration of PII

As more organizations create a dedicated CPO, **integrating privacy into all aspects of security**, including incident response.

© 2023 RSM US LLP. All Rights Reserved.

Chief Information Security Officer (CISO) overview

Year	% with CISO	% with CPO
2023	73%	52%
2020	70%	48%
2015	65%	37%
2010	55%	26%
2005	25%	10%
2000	10%	5%

© 2023 RSM US LLP. All Rights Reserved.

Chief Information Security Officer (CISO) overview

14%

Of boards have a member with **privacy** expertise.

51%

Of boards have a member with **cybersecurity** expertise.

As more companies add a member to their board with cybersecurity expertise, **organizations should consider adding a member with privacy expertise**.

© 2023 RSM US LLP. All Rights Reserved.

BRINGING IT ALL TOGETHER

Common themes for privacy and security

Risk Management

- Integrate privacy and cybersecurity considerations into risk management process.
- Visibility into personal data holdings which drives applicability of privacy laws and regulations.
- Ensure that adequate cybersecurity controls are considered and implemented to minimize attack surface.

Incident Response

- Communication and escalation between the two roles.
- Recognition of separation of duties and joint responsibilities.

Policy and Governance

- Ensure that policy and governance documents align with one another – especially those associated with Incident Response.
- Maintaining a consistent lexicon within these documents and in internal and external communication.
- Managing compliance objectives is a joint effort – privacy relies on security for many of its objectives.

© 2023 RSM US LLP. All Rights Reserved.

RSM

PANEL DISCUSSION

Led by: Charles Barley
Featuring: Chip Stewart and Laura Gomez-Martin

QUESTIONS AND ANSWERS

RSM

THANK YOU FOR YOUR TIME AND ATTENTION

RSM US LLP

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2022 RSM US LLP. All Rights Reserved.

RSM