Expanding the OSI Stack to Describe Categories of Privacy Tasks

Professor Peter Swire

Georgia Tech Scheller College of Business

Alston & Bird LLC

NIST Privacy Framework Conference

May 12, 2019

Georgia Tech | Ernest Scheller Jr. College of Business

Introduction

- Warm welcome to this conference, with its focus on **managing privacy risk**
- Privacy governance, historically, has often begun with lawyers
  - **Engineers** and others then become **increasingly important** to transform the vague rules/standards into actual practices
- This presentation:
  - **Build on published research** about the non-code aspects of cybersecurity
  - Apply that framework to **privacy governance**
  - **Categorize skill sets/disciplines** that apply to different tasks
    - What disciplines relevant for the privacy team

https://bit.ly/2MJCrZq

Published 9/26/18

Theme of CACM Article: Growth in Non-Code Cybersecurity

- **"Real" cybersecurity** today devotes enormous effort to **non-code** vulnerabilities and responses.
- The Cybersecurity Workforce Framework of the National Initiative for Cybersecurity Education lists **33 specialty areas** for cybersecurity jobs. **Ten** of the specialty areas primarily involve code, but **more than half** primarily involve **non-code work** (15 areas, in my estimate) or are mixed (eight areas, per my assessment).
- CACM article seeks to **categorize** the non-code aspects of cybersecurity
  - Expand the OSI stack to new layers 8, 9, 10
  - Define for each **problems, disciplines, and team membership**

Seven Layers of the OSI "Stack"

Technical Engineering				
	Host Layers	7. Application	Data	High-level APIs, including resource sharing, remote file access
		6. Presentation		Translation of data between a networking service and an application; Including character encoding, data compression and encryption/decryption
		5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth trasmissions between two nodes
		4. Transport	Segment (TCP) / Datagram (UPD)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
	Media Layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
		2. Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
		1. Physical	Bit	Transmission and reception of raw bill streams over a physical medium

In my experience, these seven layers are well known to knowledgeable computer people who work on cybersecurity. Intuitively, they also know that cyber-attacks can happen at any of these 7 levels.

Table 1. Vulnerabilities at each layer of the expanded OSI stack.

As discussed in the column, for layers 8–10, "A" refers to vulnerabilities and risk mitigation arising within the organization or nation; "B" refers to vulnerability and risk mitigation in relation with other actors at that level; and "C" refers to other limits created by actors at that level.

Layer	Vulnerability
1. Physical	Cut the wire; stress equipment; wiretap
2. Data link	Add noise or delay (threatens availability)
3. Network	DNS and BGP attacks; false certificates
4. Transport	Man in the middle
5. Session	Session splicing (Firesheep); MS SMB
6. Presentation	Attacks on encryption; ASN-1 parser attack
7. Application	Malware; manual exploitation of vulnerabilities; SQL injection; buffer overflow
8. Organization	A: Insider attacks; poor training or policies B: Sub-contractors with weak cybersecurity; lack of information sharing C: Weak technical or organizational standards
9. Government	A: Laws prohibiting effective cybersecurity (for example, limits on encryption); weak laws for IoT or other security B: Badly drafted cybercrime laws (for example, prohibiting security research) C: Excessive government surveillance
10. International	A: Nation-state cyberattacks B: Lack of workable international agreements to limit cyberattacks C: Supranational legal rules that weaken cybersecurity (for example, some International Telecommunications Union proposals)

Layers 8, 9, and 10: Natural Language

Layer 10	**International**	**Natural language**	**Diplomacy**
Layer 9	**Governmental**	**Natural language**	**Law**
Layer 8	**Organizational**	**Natural language**	**Contracts**
Layers 1-7	**OSI stack**	**Computer Code**	**Various protocols**

Examples from Cybersecurity

- MGMT/CoC/PubPol 4726/6726 “Information Security Strategies and Policy”
  - Required for Masters in Cybersecurity
  - How do all the pieces of this course fit together? Now – 3 parts of the course
    - **Layer 8: Corporate cybersecurity policies and governance** – e.g., draft ransomware policy for a hospital group
    - **Layer 9: Government laws/regulations** – e.g., proposed state legislation to govern IoT cybersecurity
    - **Layer 10: Nation state and international** – e.g., draft National Security Council memo on cyberthreats from Russia and policy options to respond
  - For each, **what skill set needed on the team**, to effectively manage risks?

Create a 3x3 Matrix: Institutional Sources of Governance of Risk

- Horizontal layers
  - Layer 8: organizational
  - Layer 9: government
  - Layer 10: international
- Vertical columns
  - Column A: actions within an organization or nation
  - Column B: relations with other actors
  - Column C: other limits from that layer
    - Layer 8: limits on private sector from private sector
    - Layer 9: limits on government from government
    - Layer 10: limits on nation from other nations

Layer 8: Privacy within Organizations: Contracts

	Within the Organization	Relations with Other Actors	Other Limits on Private Sector
Examples of privacy law and policy **For each, what skill set on the team?**	• **Roles,** such as **CPO, lawyers** and **privacy engineers** • **DPIAs/PIAs** & other internal policies • **Training** • Access and other **data subject rights** • **Users'** precautions	• **Vendor** & other contracts & management • More broadly, rules on **data dissemination**, including to **researchers** • **Breach insurance**	• DAA and other **self-regulatory standards** • **Technical standards** such as W3C ad IETF

Layer 9: Government Layer: Law

	Within the Organization	Relations with Other Actors	Limits on Government
Examples of privacy law and policy **For each, what skill set on the team?**	• GDPR, HIPAA, GLBA, and other **privacy laws** (100+ countries) • **Data breach** laws spreading • Rules limiting strong **encryption** • **De-identification** rules (fewer limits where not PII/personal data)	• **Business associate/processor** rules • **Data broker**/public record rules • Rules on data acquisition **dissemination**	• Constitutional and statutory **limits on what the state can do**, such as 4th Amendment, ECPA, FISA, or other illegal surveillance

Layer 10: International Layer: Diplomacy

	Within the Nation	Relations with Other Nations	Other Limits on Nations
Examples of privacy law and policy **For each, what skill set on the team?**	• **Limits on cross-border transfer**, such as prohibit export to nations that lack "adequate" protections • **Data localization requirements**, to protect citizens or enable law enforcement access	• **Non-binding** international approaches, such as OECD Privacy Guidelines • **Formal agreements**, such as EU/US Privacy Shield or EU/Japan adequacy • **Cooperation** with other nations, such as coordinated privacy enforcement	• Possible **supra-national rules**, such as by UN • **European Convention on Human Rights** (Strasbourg Court) • Council of Europe **Convention 108** and Budapest Convention

Where do Users fit?

- Focus of 3x3 matrix on **managing privacy risks** for organizations, governments, and internationally
  - A user is not an organization, government or international actor
- **I suggest part of Layer 8**
  - **Private sector actors range** from individual users/sole proprietorship to modest size to large organizations
  - EU law – individuals retain privacy rights when acting in business capacity
- Users lack an IT department, a general counsel, and face lots of risks
- **8A: "Within the household"** – how individual/family manages privacy risks
- **8B: "Relations with other actors"** – Terms of service, identity theft insurance, hire Geek Squad
- **User protection** is a big concern at **9A** (government regulation of business), such as GDPR, HIPAA

Implications for Managing Privacy Risk

- Computer scientists/engineers are used to thinking about layers 1 to 7
- CACM: Pedagogic Cybersecurity Framework (PCF)
- Today: **Privacy Institutions Risk Management Framework (PIRM Framework)** (Suggestions for other title?)
- The expanded OSI stack helps privacy engineers and others:
  - Spot the **risks and mitigations** for each part of layers 8 to 10
  - Define the **skill sets** needed for your team
    - Draw on the relevant expertise in technology, organizational behavior, law, and international relations as needed

Research Agenda for Managing Privacy Risks

- Each cell in the 3x3 matrix has characteristic research questions
  - 8B – how to **design** (law/business) and **implement** (privacy engineering) contracts for data acquisition and dissemination?
  - 8C and 9A – law and political science questions of **mix of markets, regulation, and self-regulation** to protect privacy
  - 10C – role of **supranational** institutions (international relations)

Potential for the Privacy Curriculum

- Helps describe what topics are done in each course:
  - Mostly corporate governance for CPOs (layer 8)
  - Mostly design of state/national laws (layer 9)
  - Mostly international relations, for global interoperability (layer 10)
  - An overall curriculum could determine how full the coverage is of the 3x3 matrix

PIRM Framework and Possible Integration with NIST Privacy Framework:

- Highlights ways that management of privacy risks goes beyond 8A (compliance within an organization)
- An Enterprise Risk Risk Management Tool
- Schrems II, project for company considering how to respond to risk of EU cutting off flows of personal data to the U.S.

Conclusion: Contributions of the 10-layer stack

- **Parsimonious structure** to organize the jumble of issues now crowding into cyber law, policy, and business courses
  - In my class, we discuss every issue in 3 charts
  - For students, teachers, and practitioners, a way to keep the many issues straight
- **Attacks can happen at layers 8, 9, and 10**, if the company has bad policies, the nation has bad laws, or the international community does not prevent attacks
  - **Vulnerabilities** at layers 8, 9, and 10 thus **fundamentally similar** to vulnerabilities at layers 1 to 7
  - Computing & business students, by end of the course, agree that a large part of the current cyber threat is at these layers
- In short, we need this **new theory of the non-code aspects of cybersecurity, to help students, teachers, researchers, practitioners, and policy-makers**