DOI:10.1145/3267354

Peter Swire

▸ **Carl Landwehr,** Column Editor

# Privacy and Security
# A Pedagogic Cybersecurity Framework

*A proposal for teaching the organizational, legal, and international aspects of cybersecurity.*

"REAL" CYBERSECURITY TODAY devotes enormous effort to non-code vulnerabilities and responses. The Cybersecurity Workforce Framework[a] of the National Initiative for Cybersecurity Education lists 33 specialty areas for cybersecurity jobs. Ten of the specialty areas primarily involve coding, but more than half primarily involve non-code work (15 areas, in my estimate) or are mixed (eight areas, per my assessment).

This column proposes a Pedagogic Cybersecurity Framework (PCF) for categorizing and teaching the jumble of non-code yet vital cybersecurity topics. From my experience teaching cybersecurity to computer science and other majors at Georgia Tech, the PCF clarifies how the varied pieces in a multidisciplinary cybersecurity course fit together. The framework organizes the subjects that have not been included in traditional cybersecurity courses, but instead address cybersecurity management, policy, law, and international affairs.

The PCF adds layers beyond the traditional seven layers in the Open Systems Interconnection model ("OSI model" or "OSI stack"). Previous writers have acknowledged the possibility of a layer or layers beyond seven, most commonly calling layer 8 the "user layer."[b] The framework proposed here adds three layers—layer 8 is organizations, layer 9 is governments, and layer 10 is international. This column explains how the new framework would benefit cybersecurity students, instructors, researchers, and practitioners. Layers 8–10 classify vulnerabilities and mitigations that are frequently studied by non-computer scientists, but are also critical for a holistic understanding of the cybersecurity ecosystem by computing professionals.

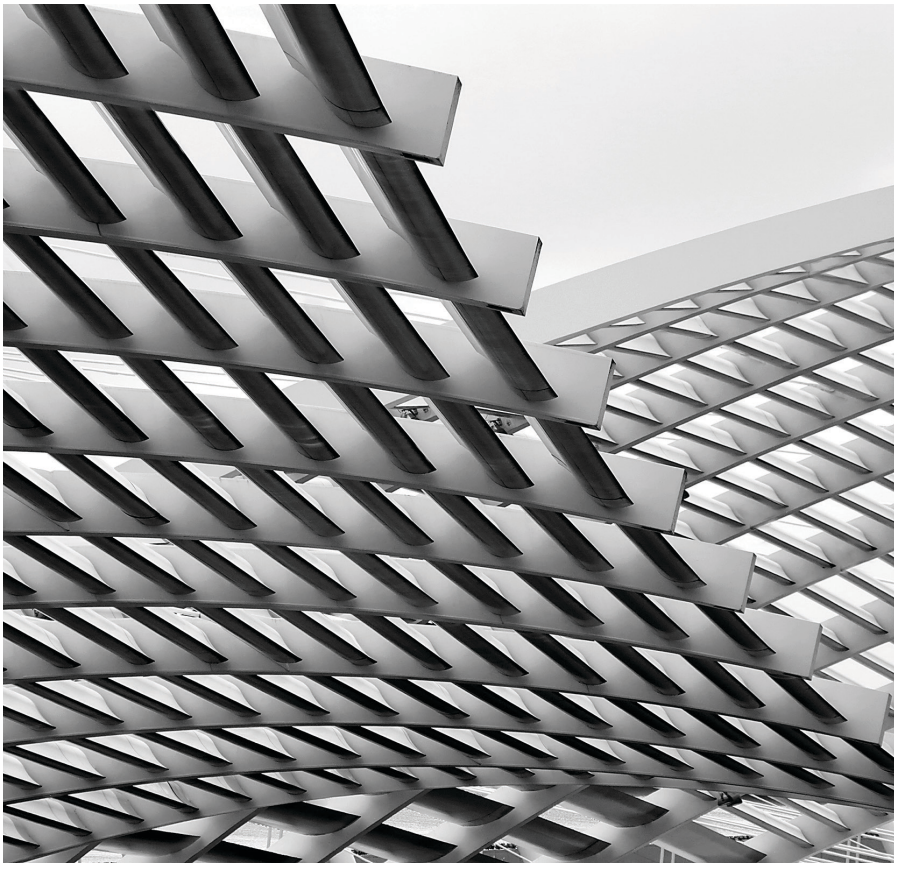

IMAGE BY UNCONVENTIONAL

a https://bit.ly/2McPRB3

b Varying previous definitions of higher layers of the OSI Model are available at https://en.wikipedia.org/wiki/Layer_8.

**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<br>B: Sub-contractors with weak cybersecurity; lack of information sharing<br>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<br>B: Badly drafted cybercrime laws (for example, prohibiting security research)<br>C: Excessive government surveillance |
| 10. International | A: Nation-state cyberattacks<br>B: Lack of workable international agreements to limit cyberattacks<br>C: Supranational legal rules that weaken cybersecurity (for example, some International Telecommunications Union proposals) |

**Table 2. The pedagogic cybersecurity framework.**

| Layer of the Expanded OSI Stack | A: Risk Mitigation Within an Organization or Nation | B: Relations with Other Actors | C: Other Limits from This Level | Protocol Data Unit |
|---|---|---|---|---|
| **8: Organization** | **8A: Internal policies or plans of action** to reduce risk within an organization (for example, incident response plans). | **8B:** Vulnerability management in **contracts with other entities**, like vendors (for example, cyber-insurance). | **8C: Standards** and limits **originating from the private sector** (for example, PCI DSS standard, led by the PCI Cyber Security Standards Council). | Contracts |
| **9: Government** | **9A: Laws** that govern what **an individual** or **organization** can or must do (for example, HIPAA Security Rule). | **9B: Laws** that govern **how organizations and individuals interact** (for example, Computer Fraud and Abuse Act). | **9C:** Government **limits on its own actions** (for example, Fourth Amendment, limits on illegal searches). | Laws |
| **10: International** | **10A: Unilateral actions by one government directed at one or more other nations** (for example, U.S. Cyber Command launching a cyberattack on a hostile nation). | **10B:** Formal and informal **relationship management with other nations** (for example, the Budapest Convention's provisions about cybercrime and Mutual Legal Assistance). | **10C: Limits** on nations **that come from other nations** (for example, the United Nations and international law). | Diplomacy |

## The Abstraction Layers of the OSI Model

The PCF builds on the Open Systems Interconnection model (OSI) stack familiar to most computer scientists. It treats the stack primarily as a conceptual framework for organizing how we understand computing systems, particularly in the security domain. The OSI model describes abstraction layers that enable the student or practitioner to focus on where a problem may exist, such as the physical, network, or application layer. While retaining the abstraction layers from the OSI model, the PCF does not emphasize the role of the OSI model as a standardizing model. Instead, it broadens students' understanding by focusing attention on the critical domains that introduce well-documented and well-understood risks from management, government, and international affairs. I provide supplemental materials online that further discuss the relationship of the PCF to the OSI model and expand other points made in this column.[c]

As a conceptual framework for understanding computer systems, the seven traditional layers apply intuitively to cybersecurity risks, as discussed by Glenn Surman in his 2002 article "Understanding Security Using the OSI Model."[2] Surman concluded: "The most critical thing you should take from this paper is that for every layer there are attacks being created, or attacks awaiting activation as a result of poor defence." Bob Blakley from Citicorp assisted with these illustrations of vulnerabilities that exist at each of the seven layers, and I have added vulnerabilities existing at layers 8, 9, and 10.

As a way to introduce layers 8 through 10, each horizontal layer highlights important types of cybersecurity vulnerabilities. At layer 8, organizations face a wide range of cyber-risks, and take many actions to mitigate such risks. At layer 9, governments enact and enforce laws—good laws can reduce cybersecurity risks, while bad laws can make them worse. At layer 10, the international realm, no one nation can impose its laws, but treaties or discussions with Russia and China, for instance, may improve cybersecurity. As shown in Table

c Supplementary materials on the framework are available at https://bit.ly/2MJCrZq

1, the vulnerabilities in these new layers are further organized by institutional form—whether the vulnerability arises within the organization (or nation), between organizations (or nations), or from other institutions at that layer.

In addition to categorizing vulnerabilities, the PCF builds on another aspect of the OSI model, the "protocol data unit," such as bits for the physical layer, packets for the network layer, and data for the application and other top layers. These protocol data units "describe the rules that control horizontal communications," within a single layer of the OSI stack.[d]

At layer 8, for organizations, I suggest the controlling rules come from contracts. The much-cited law and economics scholars Jensen and Meckling have defined corporations as a "nexus of contracts."[1] Contracts are the governance structure for relations between corporations, such as data-use agreements between an organization and its contractors. Less intuitively for non-lawyers, contracts also govern arrangements within a corporation, governing the roles and actions of the board of directors, management, and employees. Contracts are thus the protocol data unit for layer 8, providing the rules within that layer.

At layer 9, the controlling rules for government—the protocol data units—are laws. Governments enact and enforce laws, requiring actions from the organizations within the government's jurisdiction. The international realm of layer 10 operates where no binding law applies. Actors at layer 10 interact through diplomacy (or lack of diplomacy), such as negotiating a cyber-related treaty, and sometimes through declared or undeclared war.

Put another way, the traditional seven layers concern protocols expressed in machine language; layers 8 to 10 concern protocols (contracts, laws, diplomacy) expressed in natural language. The layers operate in a way familiar from the OSI stack: organizations at layer 8 select the applications at layer 7. Governments at layer 9 set laws to govern organizations. Actions at layer 10 affect the governments at layer 9, and apply when no single government can set the law.

d https://bit.ly/2x40Aoj

**I have often encountered practitioners (and researchers) who believe "real" cybersecurity involves writing code.**

### The 3x3 Institutional Matrix

Universities have traditionally studied the three non-code layers in different departments. In general, business schools focus on managing companies and other organizations. Law schools are the experts in law. International relations programs study international affairs. These different university departments are organized based on the institutions they primarily study: companies, laws, and transnational institutions.

By contrast, my experience is that computer scientists often group all of these issues into the general term "policy." Traditionally in computer science, this soft realm of "policy" is the generic term for everything not expressed in machine language. But public policy departments do not intensively cover all aspects of management, law, and international relations, so the computer science use of "policy" creates confusion for the other departments that increasingly teach and research on cybersecurity. The proposed framework matches the typical departmental organization in universities, and provides a visual representation of the key dimensions for what computer scientists have often simply called "policy."

As an additional way to organize the many non-code cybersecurity-concerns, the PCF employs a 3x3 matrix that refines which institutions are involved in each area of cyber-vulnerability or response. Table 2 portrays the matrix. In Figure 2, each layer (row) is defined by the institutions that make decisions affecting cybersecurity. Layer 8 applies to organizations facing cyberattacks. Layer 9 applies to governments writing and enforcing laws about cybersecurity. Layer 10 applies where there is no government to issue laws. Study of layer 10 thus includes both state and non-state actors that have transborder effects.

In the matrix, each of the three columns refines the sorts of institutions making the decisions. For each layer, column A contains issues arising within the institution—the organization or nation. Each "issue" identifies cyber vulnerabilities or mitigating activities. Column B contains issues defined by relations with other actors at that level. Column C contains issues where other limits arise from actors at the same layer of the stack.

This three-column approach becomes clearer as applied to layer 8, the organizational layer. Column A includes cybersecurity activities within a single organization. A company (or other organization that faces cybersecurity attacks) takes numerous actions to reduce cyber-risk. It develops incident response plans and other internal policies, and trains its employees. One way to conceptualize cell 8A is to think of the responsibilities of a CISO in managing cyber-risk within the organization.

Column B in layer 8 (cell 8B) concerns the organization's relations with other actors. First, a company creates data-use agreements and other contracts with vendors and other entities. Flawed management of these relations can expose a company to risk, such as if it hires a subcontractor to manage systems or data and the contractor does so badly. Another much-discussed aspect of cybersecurity is information sharing between organizations, such as through an Information Sharing and Analysis Center.

The third column, cell 8C, concerns other limits that originate in the private sector. The PCI DSS standard is a well-known example, governing security at the point of sale. This standard has a powerful effect on the cybersecurity of millions of merchants. The contractual standard originates in the private sector, led by the PCI Security Standards Council. If the standard is designed and implemented well, then cybersecurity improves; if done badly, cyber-risks and costs increase.

Looking at layer 8 as a whole, the simple point is that overall cybersecurity significantly depends on how well an organization handles risk within its organization (8A), its contracts and relations with other actors (8B), and standards and norms that come from the private sector (8C).

Governments, for purposes of the PCF, create laws. Cell 9A contains laws that govern what an individual or organization can do. For instance, using U.S. examples for illustration, the HIPAA Security Rule sets requirements for medical providers. As a different example, consider legislation that would prohibit the use of strong encryption or require a backdoor. I have opposed such legislation, but it illustrates how a government law, applying to each organization, can affect cybersecurity risk.

Cell 9B contains laws that govern how organizations and individuals interact. Some of the HIPAA requirements fit here, such as the business associate requirements of HIPAA that govern contracts with outside parties. An important example in cell 9B is the Computer Fraud and Abuse Act, the anti-hacking law that defines when it is criminal to access computer systems without authorization.

Whereas cells 9A and 9B primarily concern government laws affecting the private sector, cell 9C applies to government limits on government action. The limit on illegal searches in the Fourth Amendment is one example. More broadly, cell 9C concerns the controversial topic of government surveillance. Surveillance sometimes aids security, such as when a criminal is detected, and sometimes hurts security, such as when government actions create backdoors or other vulnerabilities.

The international layer applies to actions taken within one nation that are intended to have cyber effects in other nations. Cell 10A concerns unilateral actions by one government, such as the U.S. The government, for instance, may decide that U.S. Cyber Command should launch a cyberattack on a hostile nation.

Cell 10B involves relations with other nations, which is the main task of diplomacy. There are formal treaties that affect cybersecurity, such as the Budapest Convention's provisions about cybercrime and Mutual Legal Assistance. More generally, cell 10B applies to the range of possible cooperation with other nations on cyberattack or defense.

**The PCF provides a parsimonious way to identify and develop a response to a growing number of non-code cybersecurity risks.**

Finally, cell 10C applies to limits on nations that come from other nations. For instance, some countries have proposed to set cybersecurity rules through the International Telecommunications Union, associated with the United Nations. If such rules are implemented, then supranational laws could govern cyber actions that have transborder effects.

## Applying the Framework

Adding layers 8, 9, and 10 to the OSI stack in the PCF brings important advantages to the study and practice of cybersecurity. I have personally experienced the framework's usefulness in teaching cybersecurity at my own institution: my cybersecurity classes cover every topic mentioned in this column. The PCF provides students with invaluable context for how all the issues fit together, to ensure they understand the "big picture." The framework also clarifies the scope of a cyber-curriculum. Some classes, for instance, focus primarily on how a CISO or company should manage a company's risks (layer 8). Others are mostly about international affairs (layer 10), perhaps with discussion of national cybersecurity laws (cell 9A). The PCF enables program directors and students to concisely describe the coverage of a cybersecurity class or curriculum.

The 3x3 matrix clarifies a research agenda for those seeking to identify and mitigate non-code cyber problems. For example, cell 8B raises legal and management issues of how to design and manage cybersecurity contracts: How should cybersecurity be treated in outsourcing or insurance contracts? Cell 9A concerns legal and political science issues of how laws get drafted and implemented. Cell 10C calls on international relations expertise to discuss the role of supranational institutions. Few individuals are expert in all of this literature. Researchers can develop an issue list for each cell, along with canonical readings to assign in general examinations.

For cybersecurity practitioners, I have often encountered practitioners (and researchers) who believe "real" cybersecurity involves writing code, perhaps with some vague acknowledgment of the need for "interdisciplinary" study. The sheer volume of issues identified in the 3x3 matrix emphasizes the growing significance of non-code issues—bad decisions in any part of the matrix can negatively affect cybersecurity. As with the existing seven layers of the stack, organizations can identify their vulnerabilities by systematically examining layers 8 to 10. Organizations can then better identify and mobilize expertise for these non-code cyber issues.

In sum, the PCF provides a parsimonious way to identify and develop a response to the growing number of non-code cybersecurity risks. The 3x3 matrix visually categorizes and communicates the range of non-code cybersecurity issues. No longer can "real" cybersecurity refer only to technical measures. Instead, a large and growing amount of cyber-risk arises from problems at layers 8, 9, and 10. Extending the stack to these 10 layers results in an effective mental model for identifying and mitigating the full range of these risks. C

**References**

1. Jensen, M.C. and Meckling, W.H. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics 3*, 4 (Oct. 1976), 305-360.
2. Surman, G. Understanding security using the OSI model. GSEC Practical Version 1.3 (Mar. 29, 2002); https://bit.ly/2BaJGrV.

**Peter Swire** (Peter.Swire@scheller.gatech.edu) is the Elizabeth & Tommy Holder Chair of Law and Ethics in the Scheller College of Business and Associate Director for Policy in the Institute for Information Security and Privacy at Georgia Institute of Technology in Atlanta, GA, USA.