Cybersecurity Policy Guidebook

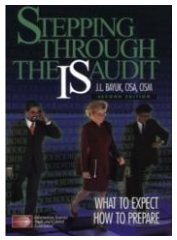
Preview of Second Edition

Jennifer Bayuk

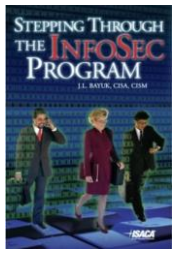
www.bayuk.com

June 11, 2026

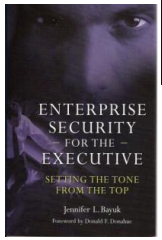
Introduction



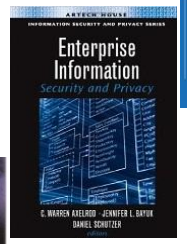
2004



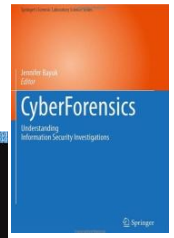
2007



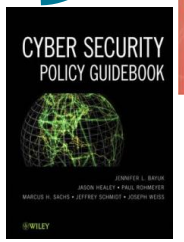
2009



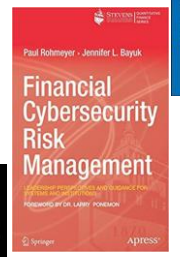
2009



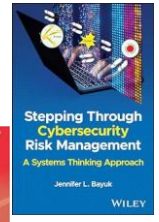
2010



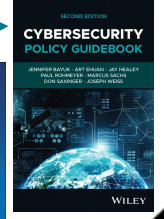
2012



2019



2024



2026

President & CEO
Decision Framework Systems, Inc.

Managing Director, Cybersecurity Risk
JPMorgan Chase

Managing Director, Enterprise Risk
Citi

Independent Technology
Risk Management Consultant

Associate Professor
Stevens Institute of Technology

Senior Managing Director, CISO
Bear Stearns, Inc.

Manager, IS Business Controls
AT&T Capital Corporation

Information Systems Risk Manager
Price Waterhouse

Member of Technical Staff
AT&T Bell Laboratories

PhD Systems Engineering,
Stevens Institute of Technology

Licensed Private Investigator,
State of New Jersey

Certified Information Systems
Security Professional (CISSP)

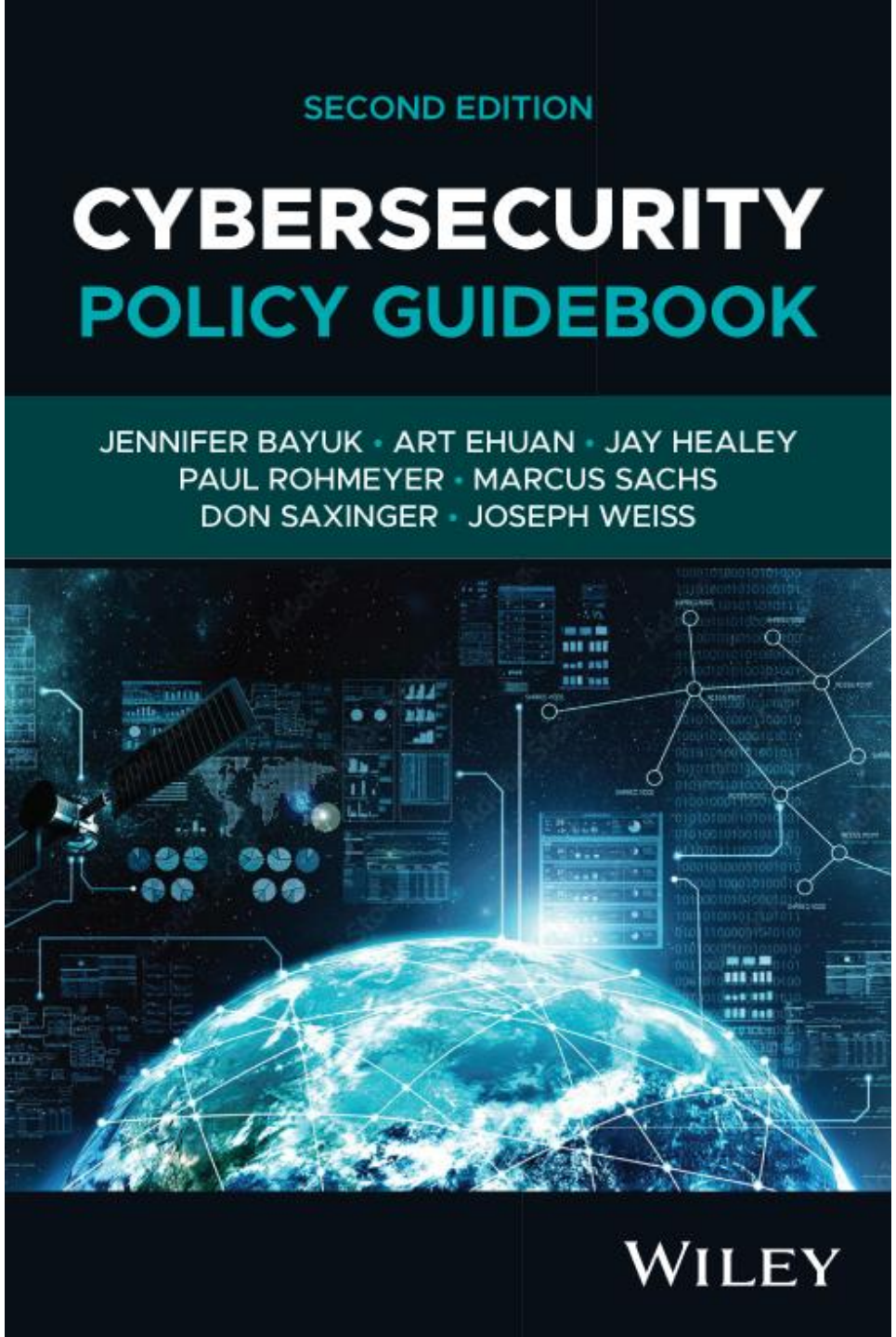
Certified in the Governance
of Enterprise IT (CGEIT)

Certified Information Security Manager (CISM)

Certified Information Systems Auditor (CISA)

MS Computer Science, Stevens Institute of Technology

BA Computer Science & Philosophy, Rutgers College, Rutgers University



Preface Excerpt

The idea for the original edition of this book was sparked by Mike Wynne, the 21st Secretary of the US Air Force, who established considerable capability for cybersecurity in the Air Force, and was at the time single-handedly responsible for raising the awareness of national security-related cybersecurity policy issues. He envisioned a guidebook for congressional staffers and academics that would create awareness of the importance of cybersecurity policy, and while on the Advisory Board of the Stevens Institute of Technology School of Systems and Enterprises, he organized a conference on the topic.

Opinions were solicited from experts in a wide variety of fields who are stakeholders in cyberspace. Many of them spoke at the conference or attended the discussions. Some were unable to attend, but provided their comments in written form. The conference had sessions ranging from security technology investment decisions by venture capitalists to the implications of cybersecurity policy on personal privacy.

Though all speakers were experts in their field and were asked to address cybersecurity policy topics, many instead focused on strategy or technology issues. Even where it was clear that policy was being discussed, policies were often not articulated clearly enough for panelists and audience members to participate in informed debate.

This observation itself became the buzz at the conference and made it clear that cybersecurity policy means different things to different people, even those who work in cybersecurity. As a result, then Stevens professor Jennifer Bayuk recruited a variety of cybersecurity experts to lend their expertise to the first edition of this book.

Second Edition Authors

Art Ehuan is Executive Director of Duke University's Master of Engineering in Cybersecurity and CISO Executive Certificate programs. A former FBI Supervisory Special Agent, he served as cyber expert on breaches at Heartland, Sony Pictures, Target, Anthem, Equifax, Capital One, and Marriott.

Jason Healey is a Senior Research Scholar at Columbia University's School for International and Public Affairs. He founded the Atlantic Council's Cyber Statecraft Initiative and was a founding member of the White House Office of the National Cyber Director.

Paul Rohmeyer, PhD, is an IT management consultant and Information Systems faculty member at Stevens Institute of Technology. He serves on the editorial boards of Computers & Security Journal and Cybersecurity & Cybercrime Journal, with expertise spanning banking, finance, healthcare, and life sciences.

Marcus H. Sachs, PE, is Senior Vice President and Chief Engineer at the Center for Internet Security. A retired US Army officer and former White House appointee, he previously served as CSO of the North American Electric Reliability Corporation and VP for National Security Policy at Verizon.

Donald Saxinger is an independent financial sector regulatory policy consultant. As an FDIC banking supervisor for over three decades, he chaired the FFIEC IT Examination Handbook and Cybersecurity and Critical Infrastructure Working Groups, authored banking industry cybersecurity guidance, led interagency cyber rulemaking, and advised central banks internationally.

Joseph Weiss, PE is Managing Partner of Applied Control Solutions, LLC, an independent control system cybersecurity consultant. An ISA Life Fellow and member of Control's Process Automation Hall of Fame, he has published over 100 papers and holds patents on instrumentation, control systems, and OT networks.

Excerpts from Forward by Dan Geer

A second edition of a book is a testimony to two things, the first edition was valuable and the world has changed. Both characteristics apply here; the first edition proved most valuable and Lord knows the world of cybersecurity is nothing if not rich in change.

...

The book is, to a large degree, encyclopedic, and it expects a lot of you, the reader. Part of that comes from a certain reality:

> decision making under uncertainty is sharper when you not only know a lot about where you are, but also how you got to where you are.

The authors collectively have that history cornered, as their biographies and the chapter on "Cybersecurity Evolution" proves.

...

The culminating chapter is a "Cybersecurity Policy Catalog" that rolls up all the entire rest of the book. It is argumentative (meant as a compliment) as it confronts how differing goals and constraints color what policies can be adopted in the reader's particular setting, which is to say that each proposed policy comes with debate, as well they should given the inherent contradictions in much of what we are talking about. The present author's opinion is that:

> Most important ideas are not exciting
>
> Most exciting ideas are not important
>
> Not every problem has a good solution
>
> Every solution has side effects

In no part of modern life are the above more true than in the interplay around cybersecurity. They are what selecting policies is all about: distinguishing between tolerable and intolerable failure modes. A state of security can be simply described as the absence of unmitigatable surprises, making the goal of security engineering likewise simple: No silent failure. Failure is to be avoided whenever possible, but absolute total avoidance is certain to be diseconomic. And we are back to picking policies that advance such end-goals.

This book will help.

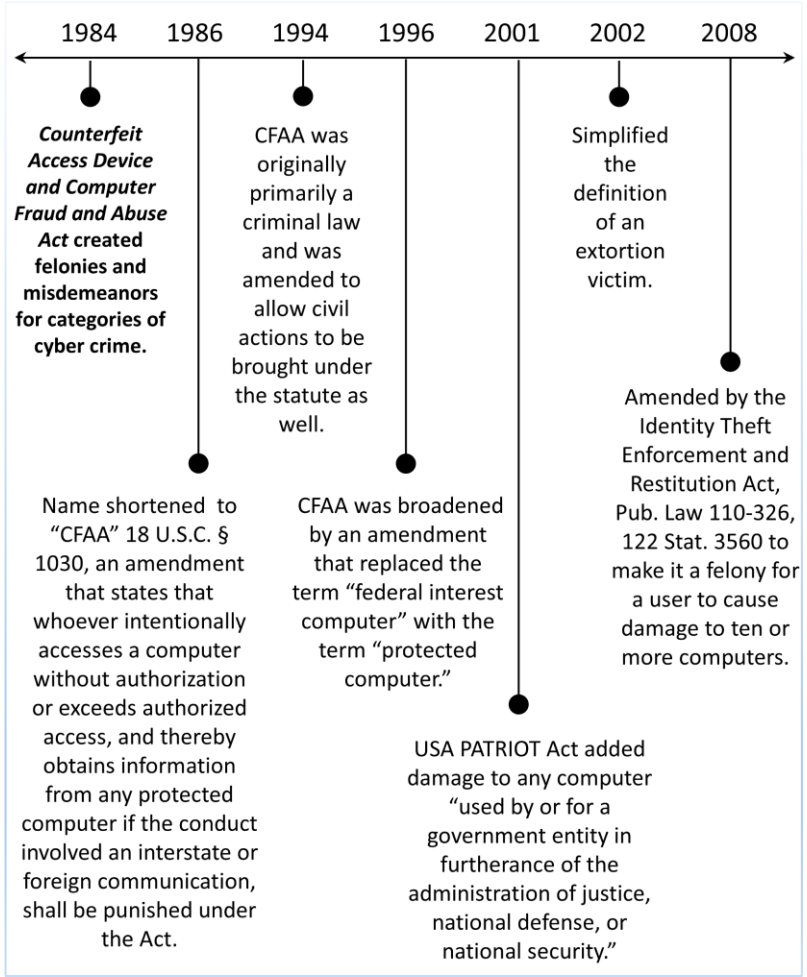
If you use it

Chapter 1: Building Blocks

- **Cybersecurity Goals**
- **Distinction between:**
  - **Information Technology**
  - **Operational Technology**
  - **Industrial Control Systems**
- **Introduction to Policy Domains:**
  - **Individual**
  - **Organizational**
  - **Dependency**
  - **Adversary**
  - **Cyberspace**
  - **Public**
- **Distinction between:**
  - **Technology Security Specifications**
  - **Cybersecurity Policy**
- **Cybersecurity Policy Catalog**
- **Example Cybersecurity Law in Catalog Format**

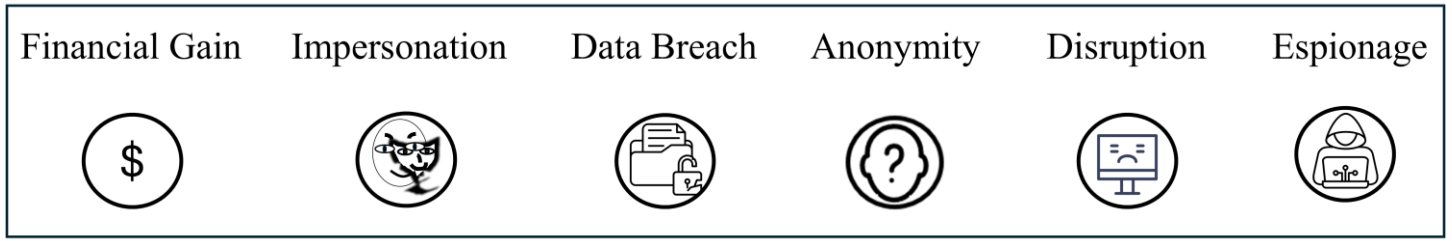
Chapter 1: Catalog Public Policy Example

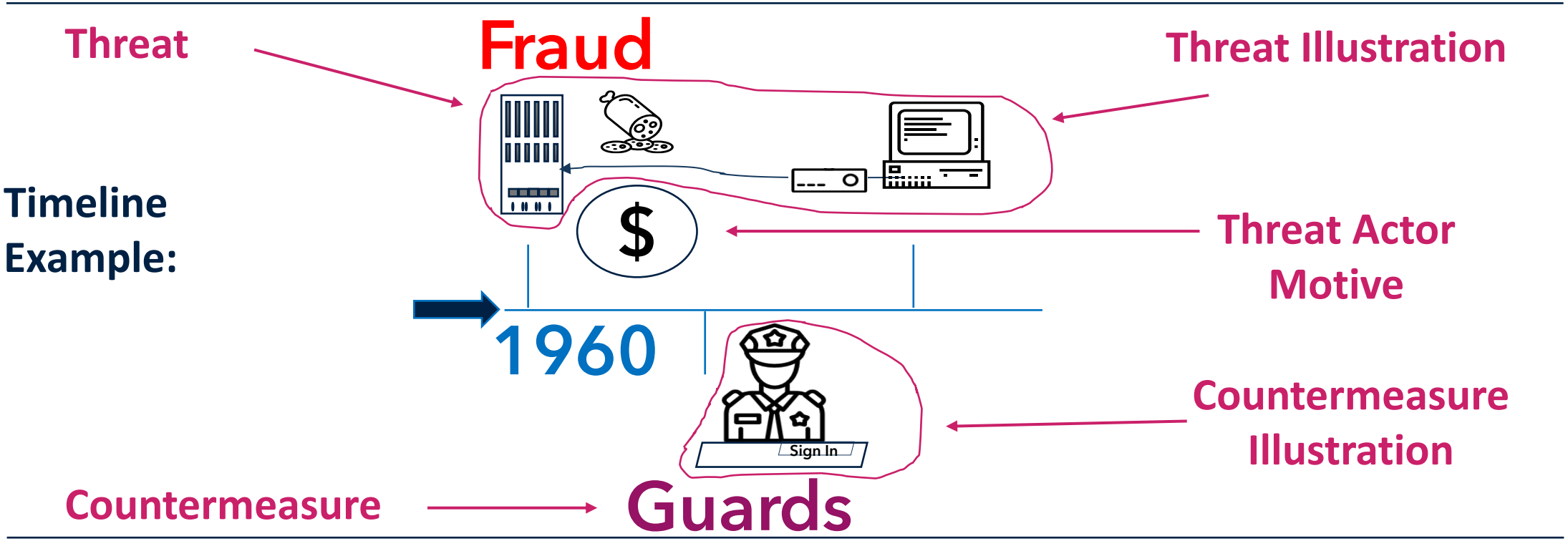
Index	Statement	Objective	Reasons for Controversy
CFAA	Accessing protected computers without authorization, or exceeding authorized access, for the purpose of fraud, financial gain, malicious damage, espionage, or extortion shall be subject to criminal and civil penalties.	This policy is intended to prohibit trespassing into, damaging, or acquiring information from certain categories of computers, assuming the user lacks authorization for that conduct.	• Malicious espionage and data theft is rampant and there are currently no laws that criminalize the fundamental enabler of these crimes, which is hacking • Exploring the internet was a common activity among curious young people and many thought it was harmless.



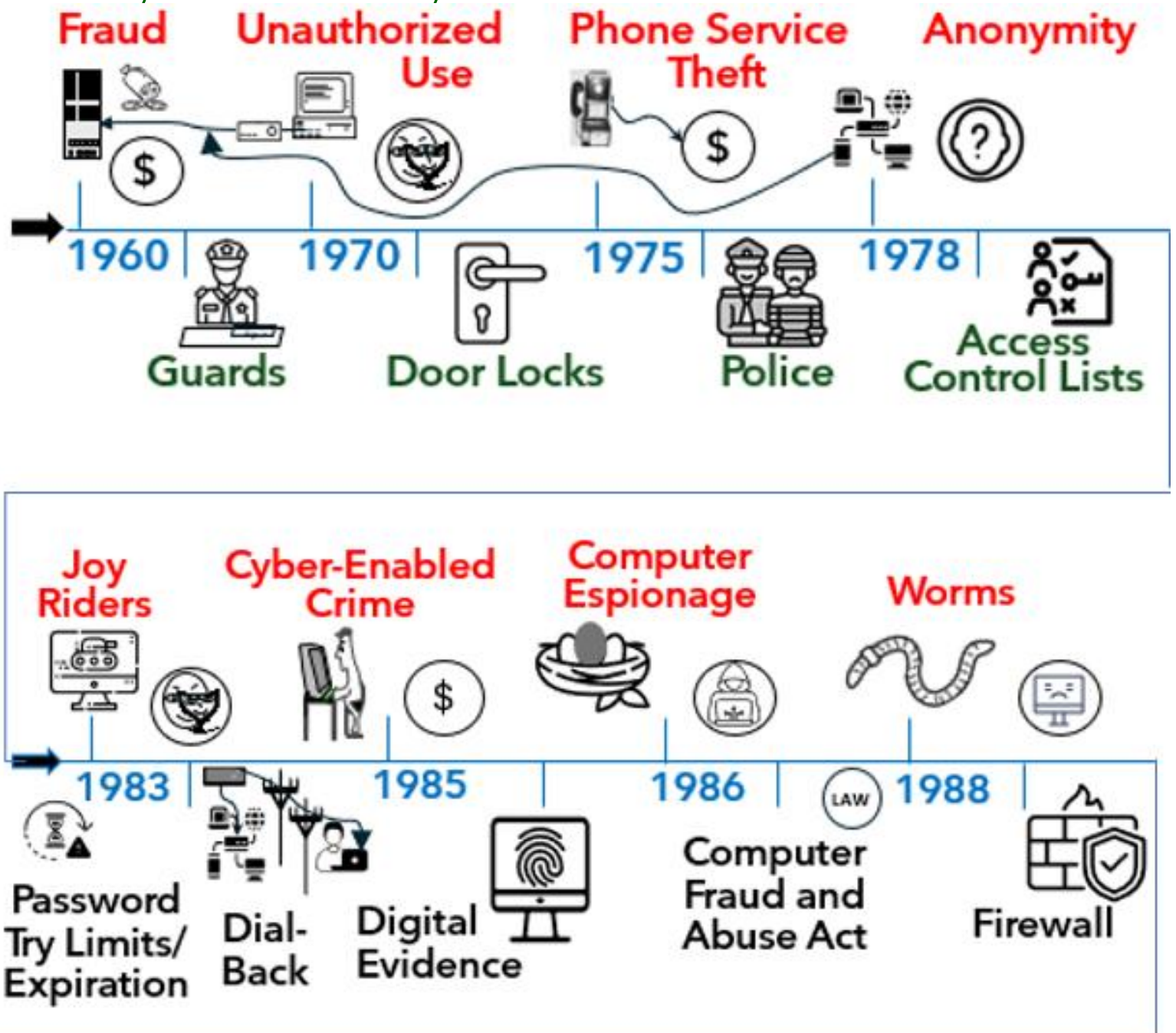
Chapter 2: Cybersecurity Evolution

Key to timeline of cyber threat motivations:

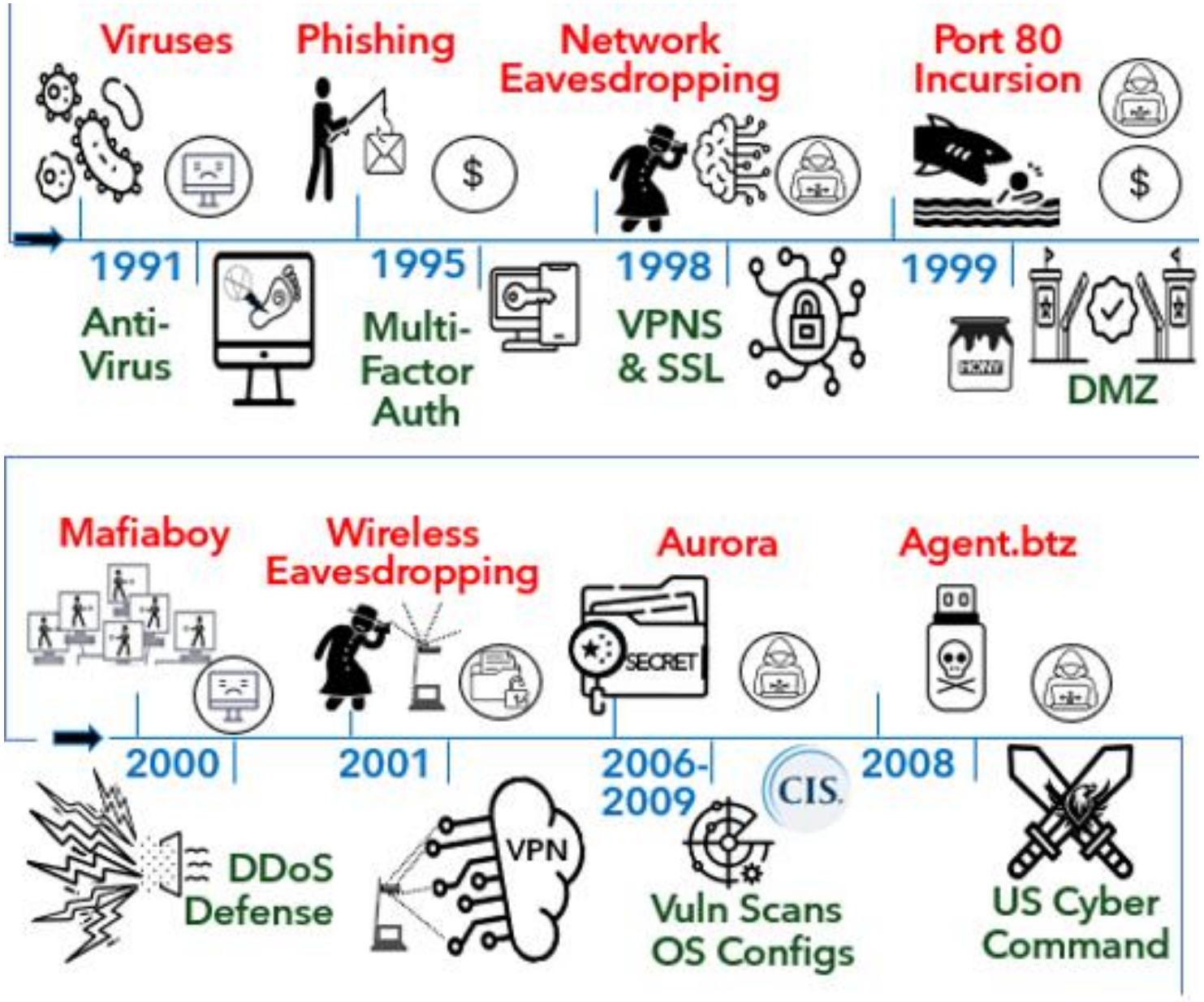




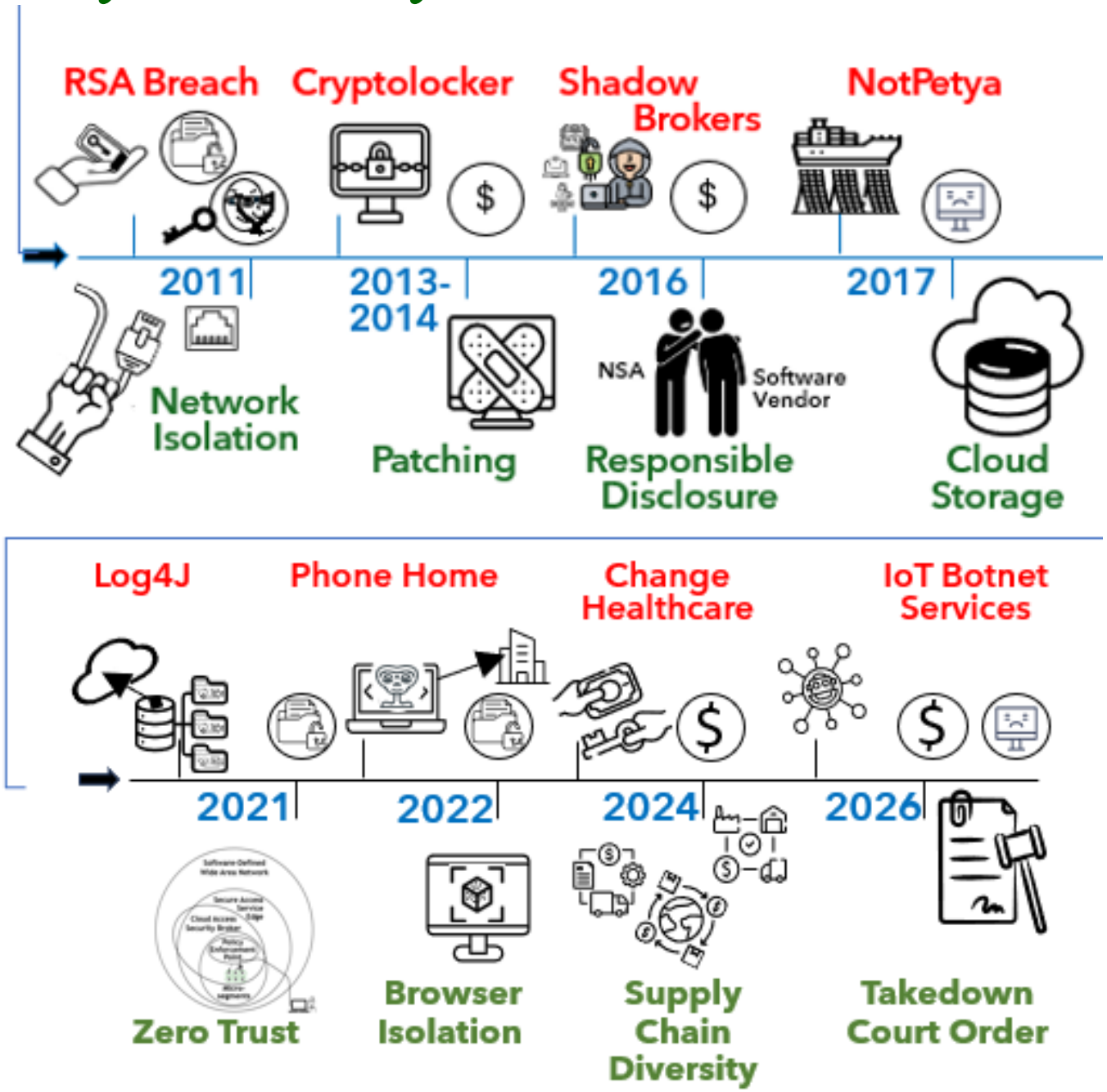
Cybersecurity Evolution 1960-1988



Cybersecurity Evolution 1991-2008



Cybersecurity Evolution 2011-2026



Contributing Factors:

- *Known Exploited Vulnerability* to Ransomware
- *External Threat* from Ransomware Operators
- *Insider Threat* with Ties to Ransomware Operators

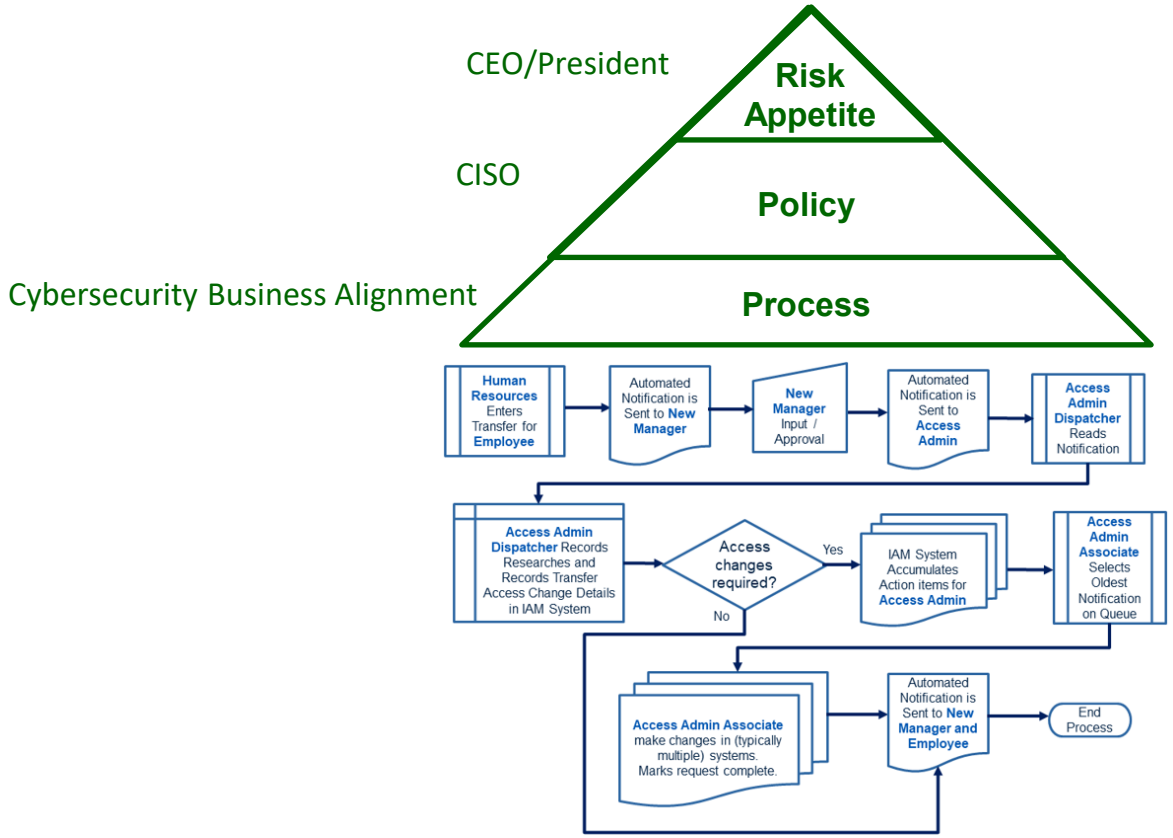
Root Cause: **Organizational inability to prioritize security safeguards**

Risk Issue

Chapter 4: Governance → Start with Tone at the Top

CYBERSECURITY IS A MAJOR CONCERN.

THE ENTERPRISE HAS NO TOLERANCE FOR KNOWN VULNERABILITIES IN ITS SYSTEMS, NO TOLERANCE FOR DATA BREACHES, AND LOW TOLERANCE FOR UNKNOWN VULNERABILITIES.



Section B: Authorized Use

B.1: Business Purpose

All information technology at Firm shall be associated with an "Application." The application is the business purpose of the technology that is recorded in Application Inventory.

B.2: Least Privilege

Where individuals require access to an organization's facilities, operational processes, technology systems, and information ("resources") in order to ensure the success of the enterprise mission, this access shall be:

(i) limited to least privilege with respect to the individual's function; and

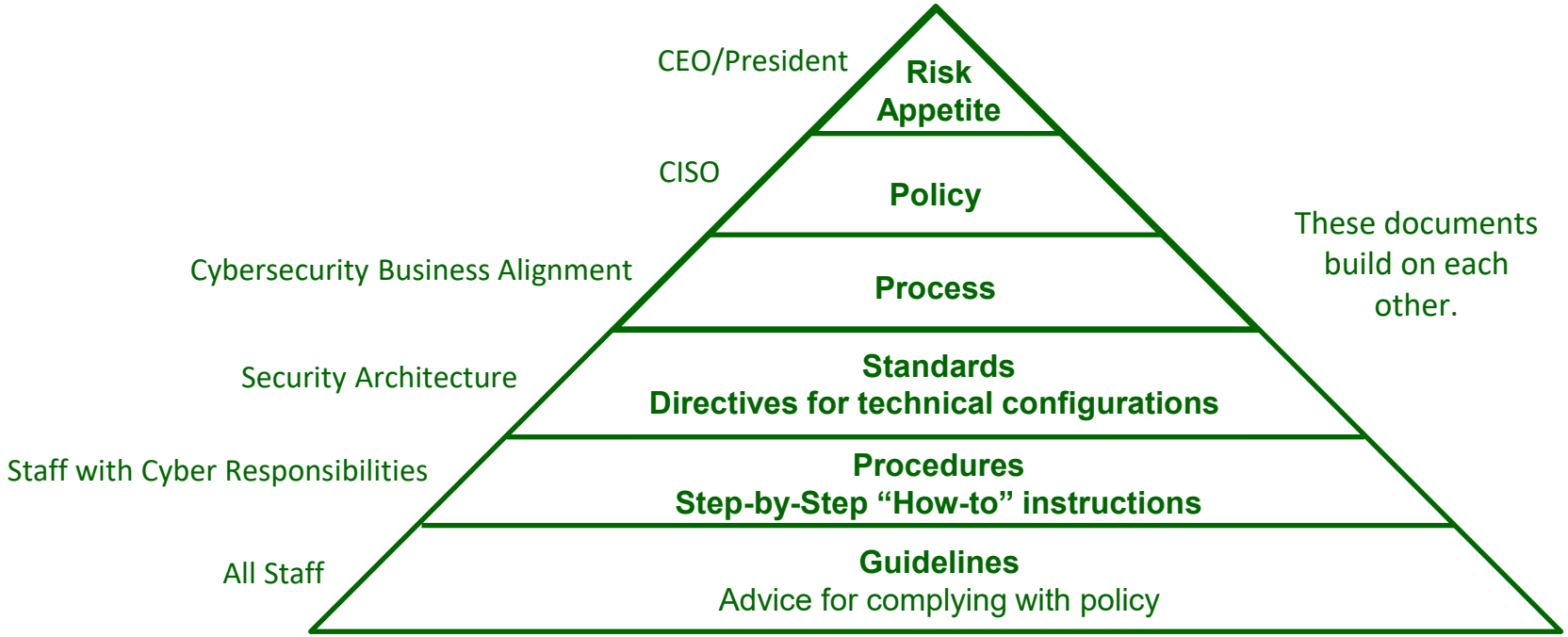
(ii) provisioned only after receipt of a successful background check approved by Legal that may be customized for that function.

B.2.1: User Classification

Responsibility for determining the minimum possible access requirements for an individual's function is allocated based on user classification. Individuals who do not have a business relationship with the enterprise that falls into a defined user classes shall have no authorized access and all individuals who are granted systems access shall endeavor to ensure that such unclassified individuals are unable to access enterprise resources that are not declared by Legal to be publicly accessible (e.g. advertising and corporate investor websites).

B.2.2: Departmental Responsibility

Cybersecurity Risk Management Controls



These documents build on each other.

Awareness and directives at higher levels drive awareness and corresponding activities at lower levels.

Consistency

**Must also be consistent with legal obligations and contractual requirements!*

Case Study Comparison

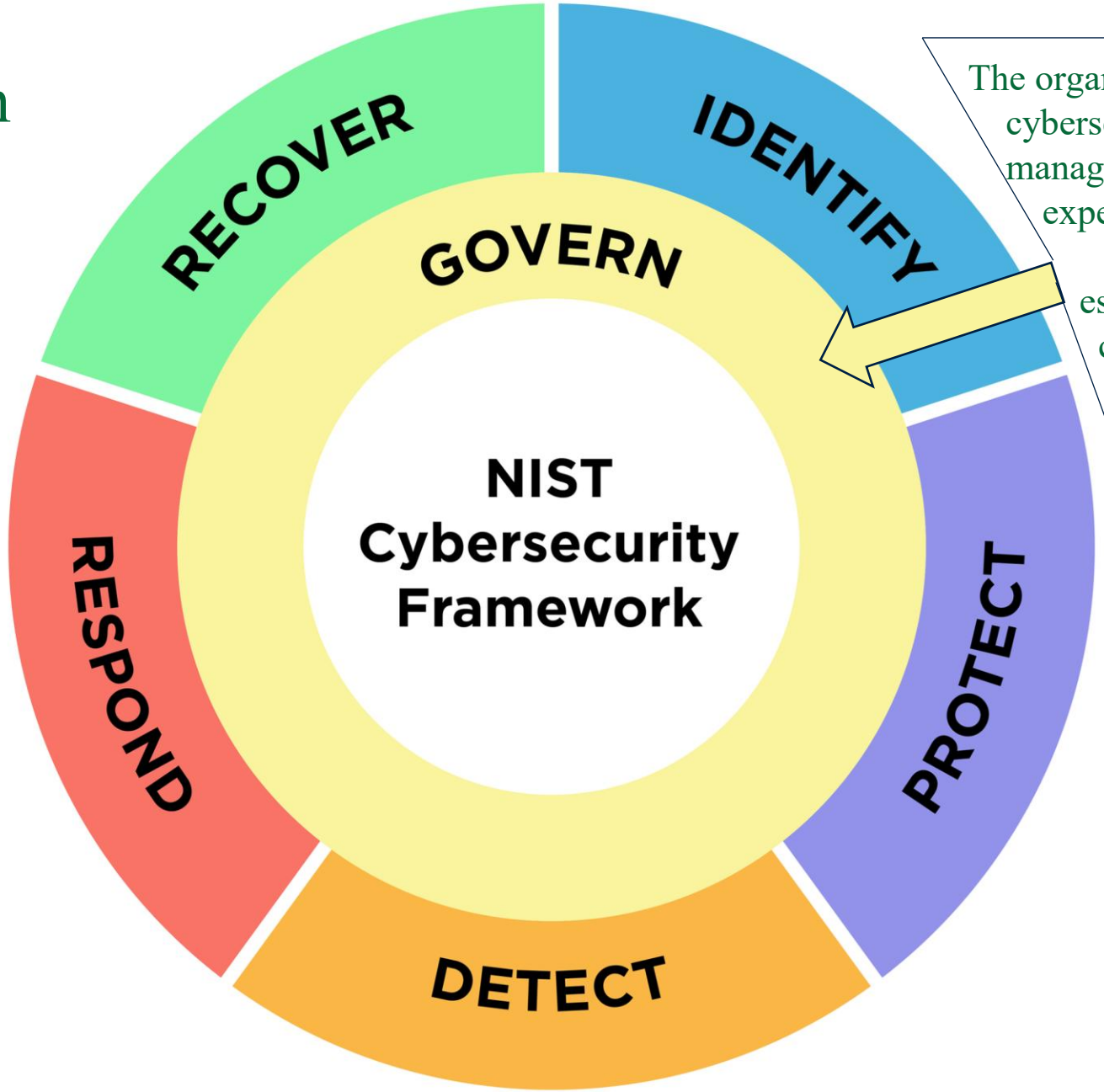
Most Controlled  **Least Controlled**

	Financial Industry	Industrial Control Systems	Technology Platforms	Artificial Intelligence
Primary Cyber Risk	Monetary	Public Safety	Confidentiality, Integrity, Availability	Autonomous Agents
Operating Model	Coordinated Transaction Processing	Physical System Automation	Marketplace of Technology Services	No industry standards
Primary Regulator responsible for cybersecurity risk oversight	Comptroller of the Currency and State Treasury Departments	Differs per System, e.g. for power: North American Electric Reliability Corporation Federal Energy Regulatory Commission	Federal Trade Commission, which regulates all businesses by default	None so far

- Effective regulation aims to align private behavior with the public interest.
- The common purpose of all regulation is performance.
- Regulation defines standards for performance, then assigns consequences, positive and negative, for that performance.

Source: https://www.americanbar.org/content/dam/aba-cms-dotorg/products/inv/book/413436990/chap1-5350267.pdf

Chapter 4 : Communication

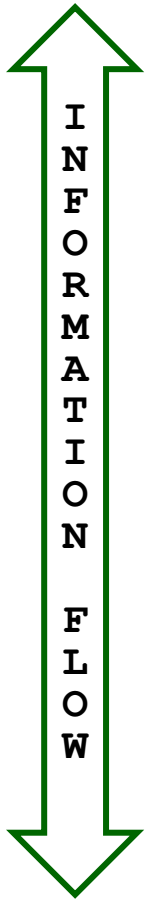


The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Exemplar Frameworks

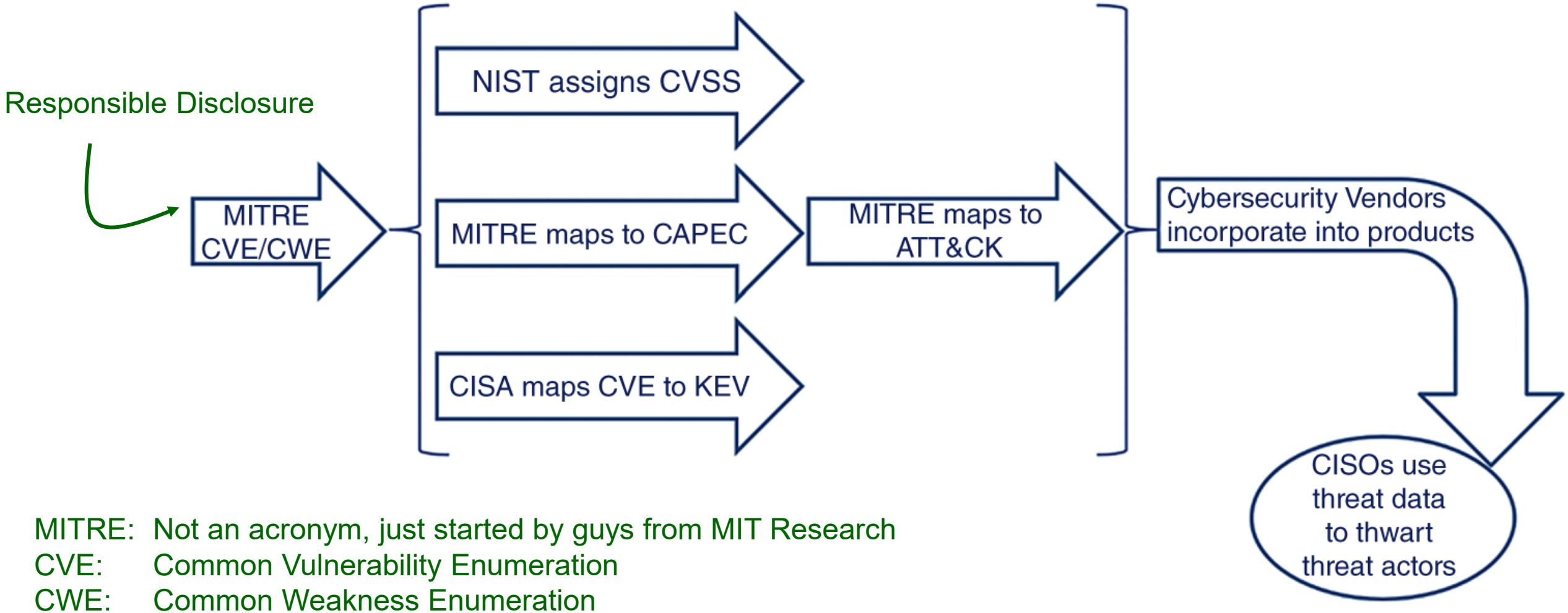
Layer	Framework	Publisher
Governance	Risk Management Guidelines. (31000)	Joint effort by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 2018)
	Enterprise Risk Management – Integrating with Strategy and Performance (ERM)	Committee of Sponsoring Organizations of the Treadway Commission (COSO 2017)
	Control Objectives for Information Technology (COBIT)	Information Systems Audit and Control Association (ISACA 2019)
	Managing Information Security Risk (SP 800-39)	National Institute of Standards and Technology (NIST 2011)
Cybersecurity Program	Cybersecurity Framework (CSF)	National Institute of Standards and Technology (NIST 2024)
	Information Security Management Systems Requirements (27001)	International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 2022a)
	Cloud Controls Matrix (CCM)	Cloud Security Alliance (CSA 2021)
Dependency	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161)	National Institute of Standards and Technology (NIST 2022)
	Information Security for Supplier Relationships (27036)	International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 2021)
	PCI Data Security Standard (PCI DSS)	Payment Card Industry Security Standards Council (PCISSC DSS 2024)
	Statement on Standards for Attestation Engagements No. 18, System and Organization Controls 2, Type II report (SSAE 18 SOC2)	American Institute of Certified Public Accountants (AICPA 2017).
Assessment & Benchmarking	Guidance on Information Security Risk Management (27005)	International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 2022b)
	Cross-Sector Cybersecurity Performance Goals (CISA CPG)	Cybersecurity and Infrastructure Security Agency (CISA 2025a)
	Center for Internet Security (CIS)	CIS Critical Security Controls Implementation Groups (CIS n.d.)

Public Private Partnership Information Sharing Examples



International	**Forum of Incident Response and Security Teams**	*https://www.first.org/*
National	**National Council of ISACS**	*https://www.nationalisacs.org/*
	National Vulnerability Database	*https://nvd.nist.gov*
Industry	**Vocabulary for Event Recording and Incident Sharing Community Database**	*https://verisframework.org/vcdb.html*
State	**New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)**	*https://www.cyber.nj.gov/*
Local	**Chicago First**	*https://www.chicagofirst.org/members-and-partners/*

Communication about Vulnerabilities

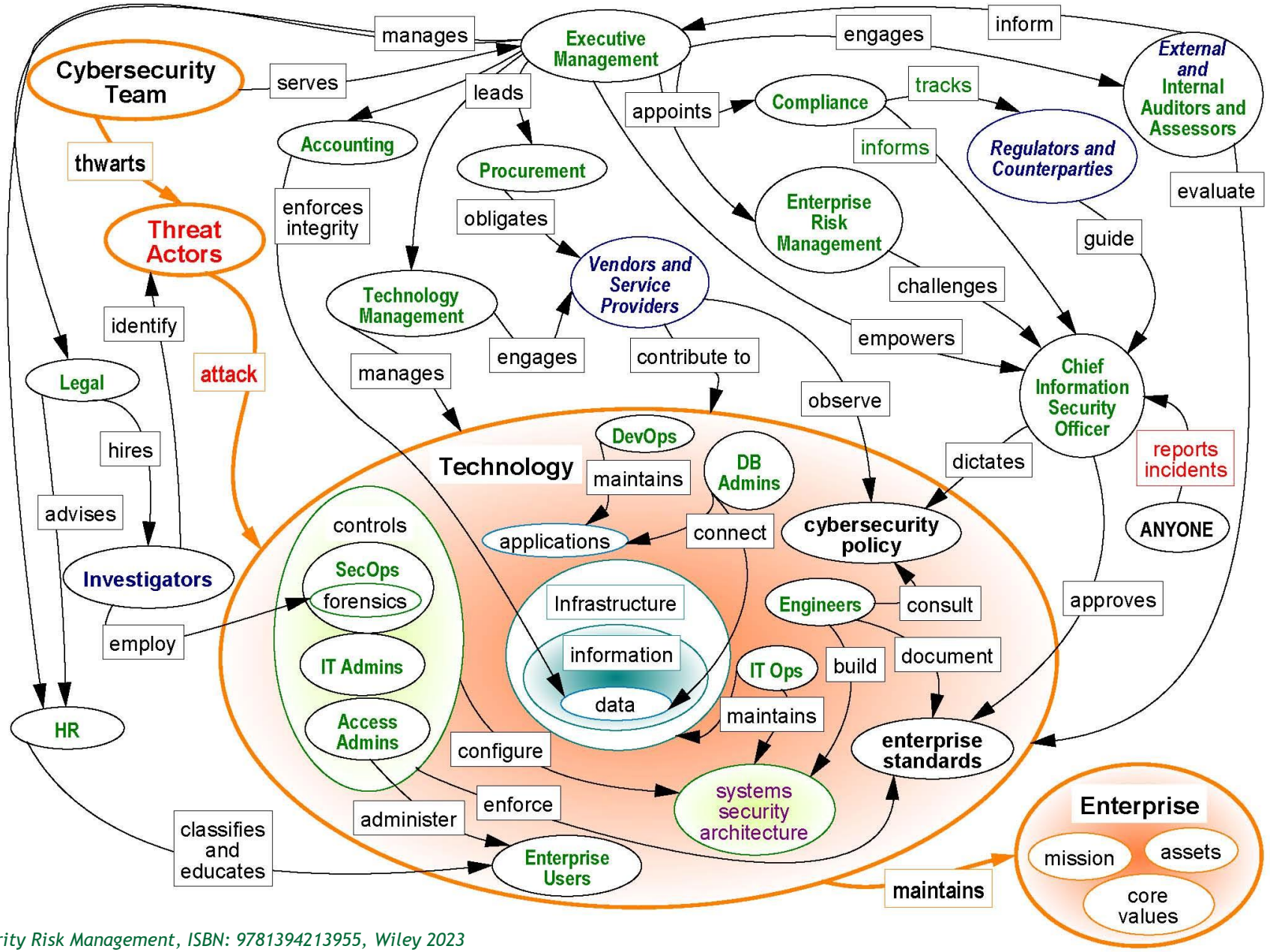


MITRE: Not an acronym, just started by guys from MIT Research
CVE: Common Vulnerability Enumeration
CWE: Common Weakness Enumeration
CVSS: Common Vulnerability Scoring System
CAPEC: Common Attack Pattern Enumeration and Classification
KEV: Known Exploited Vulnerability
EPSS: Exploit Prediction Scoring System

**FIRST maintains CVSS and EPSS and publishes an EPSS Score*

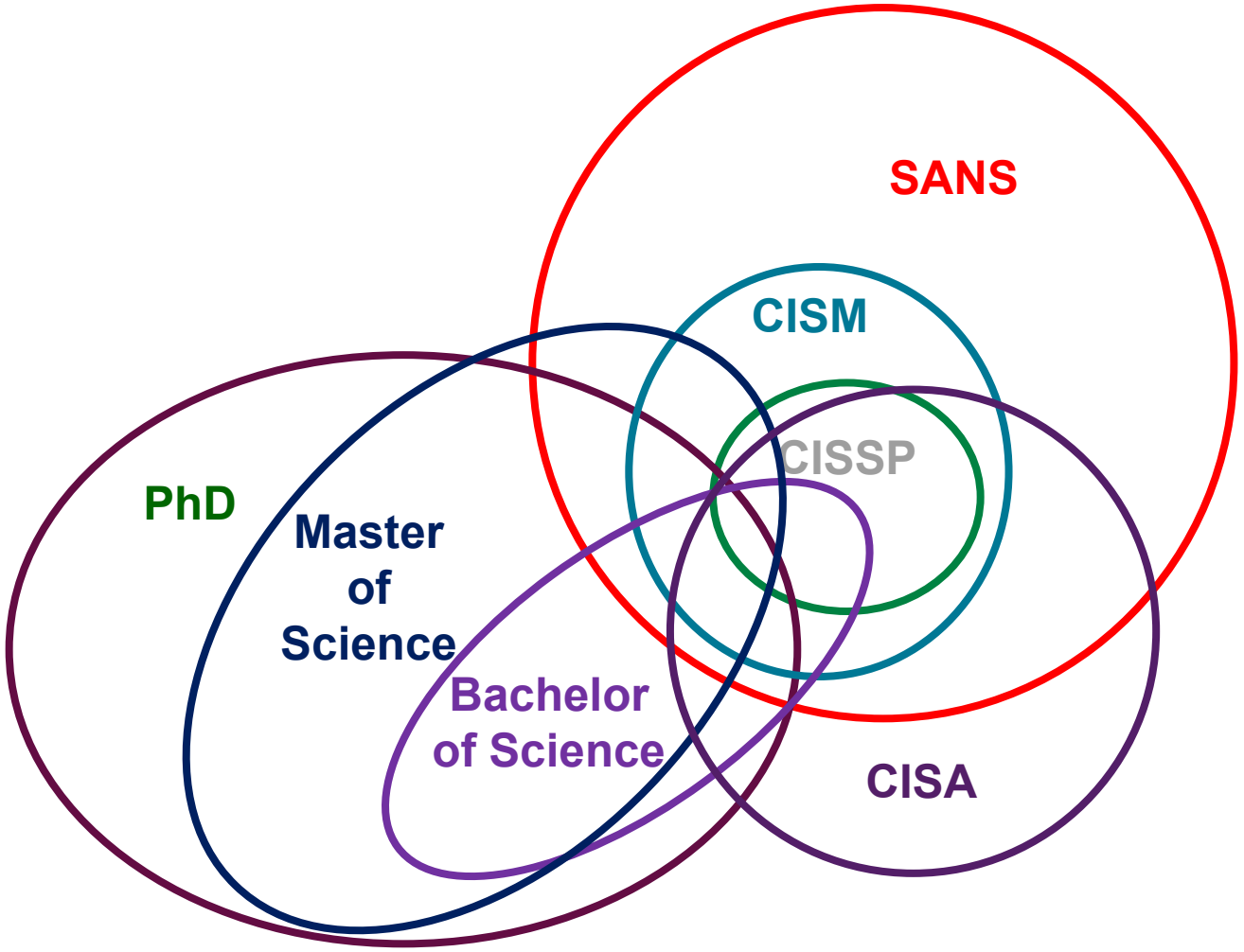
Chapter 5: Cybersecurity Workforce

Cybersecurity Roles and Responsibilities

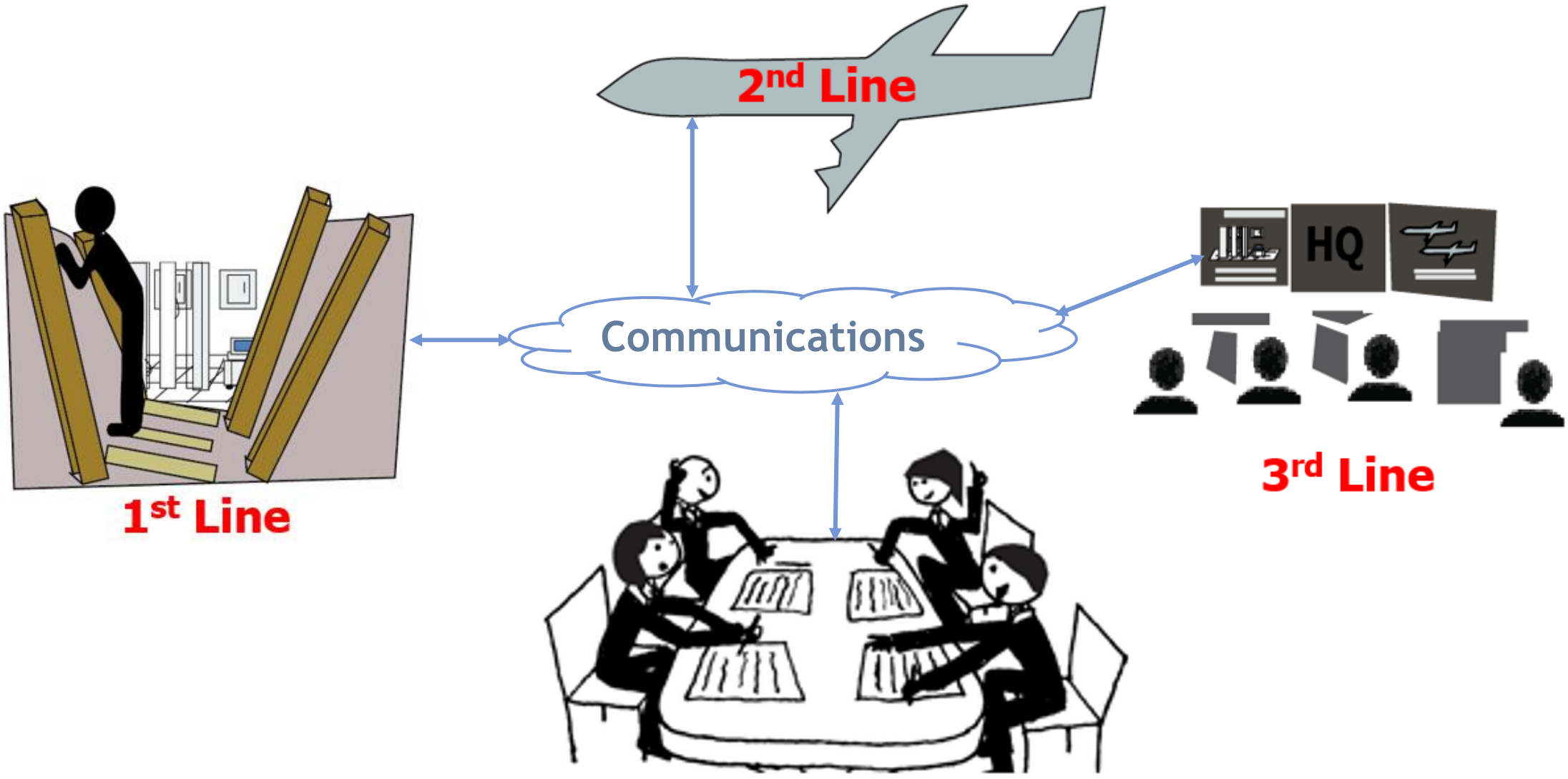


Source: Bayuk, Stepping Through Cybersecurity Risk Management, ISBN: 9781394213955, Wiley 2023

The Cybersecurity Workforce: Career Training Paths



Chapter 6: Three Lines of Defense



Source: Decision Framework Systems, 2021.

Guidance For Decision-Makers

1. Informed – thoroughly researched and tested
2. Clear – presented in layman's terms
3. Adaptive – anticipate technology evolution
4. Comprehensive – minimize overlap with sufficiently large scope
5. Cohesive – enacted within a framework with no conflicting regulations
6. Global – ubiquitously applicable
7. Collaborative – anticipate need for cooperative enforcement

Source: Kosseff, J. (2023). Cybersecurity Law. New York: Wiley

Questions/Discussion?

jennifer@bayuk.com

www.bayuk.com