
2025
WISPAMERICA™
BROADBAND WITHOUT BOUNDARIES

# Cybersecurity And Compliance: Safeguarding Your Business And Building Trust

Bis Room 203
9:45 AM - 10:45 AM

## Henry Ortiz, Esq.

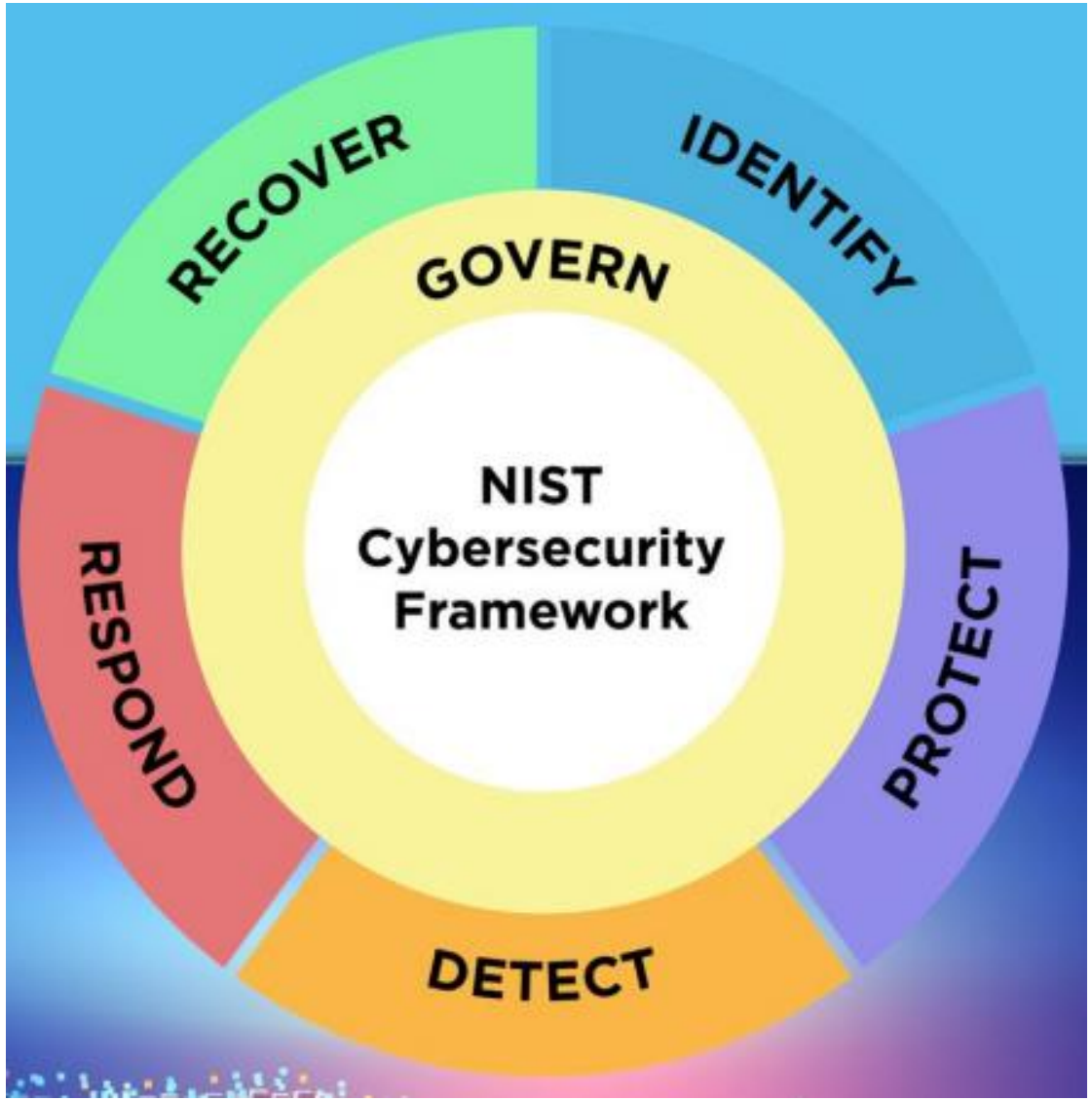
- Licensed Attorney, Database & Network Administrator / HFC
- Cybersecurity & Privacy Compliance Advisor
- Framework based Cybersecurity compliance programs
  - HIPPA - Healthcare
  - CMMC – Dept. of Defense Contractors
  - NIST CSF  - Telecommunications
- Henry.Ortiz@BorderHawk.com
- https://www.linkedin.com/in/hjortiz/

# Cybersecurity:

- **Regulatory point of view**
  - **Thursday March 27th Room 203 / 830 am**
    - Important FCC And Other Federal Agency Cybersecurity Proceedings
      - Louis Peraertz, Esq. WISPA
      - Jeff Carlisle, Esq. Lerman Senter PLLC
      - Henry Ortiz, Esq. BorderHawk
      - Anand Chari Kognitive Networks Inc.

- **Cyber risk Management**
  - Implementation
    - Challenges
      - Frameworks

# NIST CSF 2.0



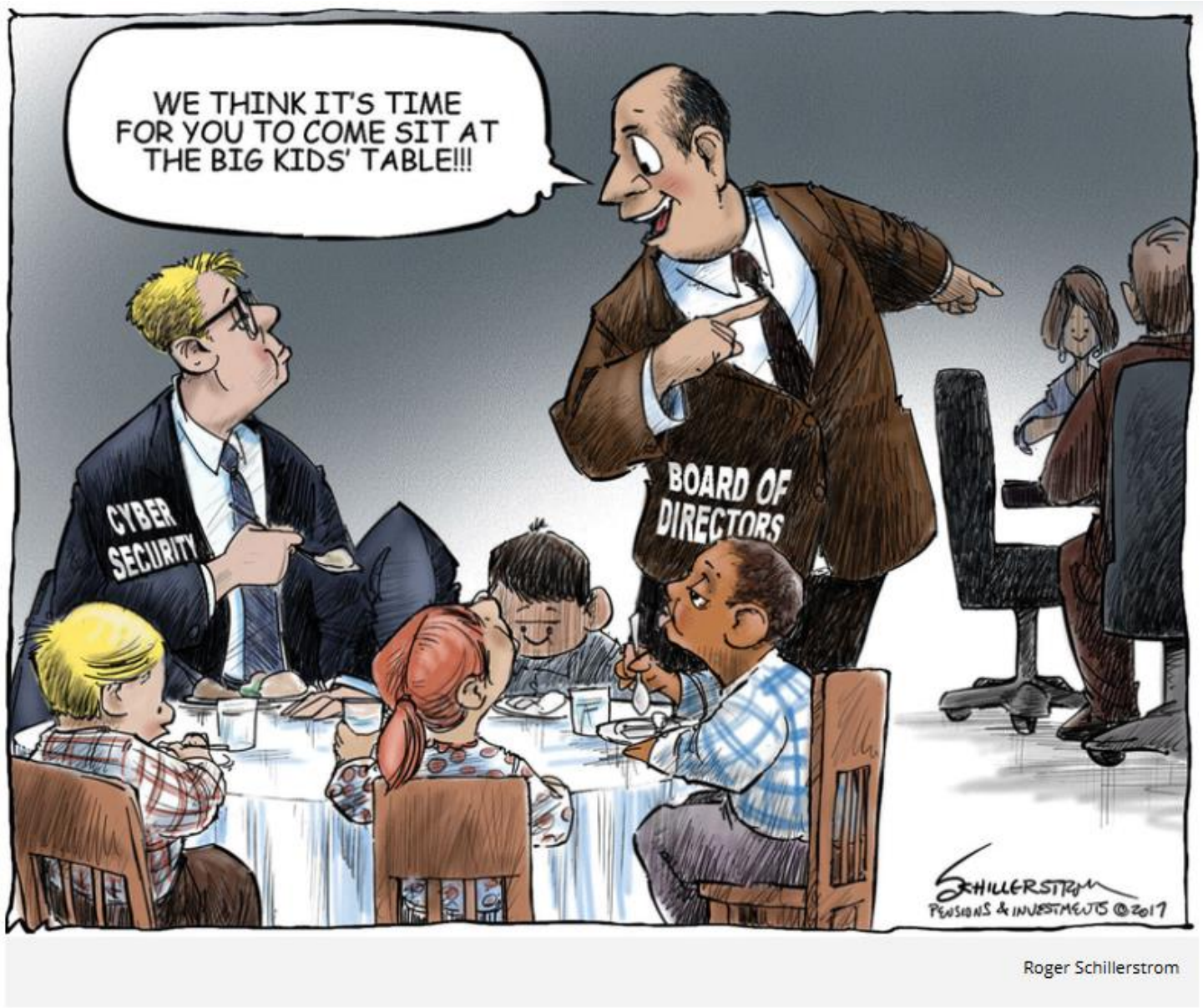
# NIST 2.0 -- How to get there?

- Risk Assessment (Do not confuse with vulnerability scan)
  - **Asset Based Assessment**
    - Identify Mission critical assets (80/20)
      - Identify Critical assets in various business units
        - IT
        - OT (Revenue Generating)
        - MSP or Data Centers (Implied Obligations ➔ HIPAA, CMMC) Critical Vendor

- POAM (Plan of Action and Milestones)
  - Policies (Formalized vs Ad-hoc)
    - Team meetings to ensure organizations stay on plan to maintain alignment with your organization's risk appetite / tolerance.
      - Leadership updates of plan progress
        - Executive team and board level updates

# Missing tools / Processes in Telecom

- Alert Management
  - Event, Incident, Alert, Breach
  - A gap in telecommunications
  - Without it, it is unlikely for telcos to be ahead of threats
- Subscribe / Daily report
  - CALIX, ADTRAN, CISCO, Various government sites such as DHS & CISA
- Indicators of compromise:
  - Applicable to you?
  - Reporting Obligations?
    - CPNI: Private information that telecommunications service providers acquire about their subscribers (type, quantity, destination, technical configuration, location, and amount of use of telecommunications services, as well as information about voice calls)
      - Voice compromised: 2 hours
      - CPNI Breach: 72 hours (and update every 72 hours until closed)
- Evidence Management
  - Search events in the past – 7 years
  - Log your activities - Save information as evidence
    - What did your team do to analyze, mitigate, and report --- When? How? Who?




# Cybersecurity as a corporate strategy.

**Executive team, Board of Directors, Owners.**

Cyber =! Not only delegated to IT

Imagine if the financial strategies for your entire business were developed, implemented, and managed by your billing department?


**Cyber Risk Management**

- Governance & Compliance
- Identify Critical Assets
- Protect Critical Assets
- Detect Anomalies
- Respond (incident response plans & Notification Requirements)
- Recover. BCDR Plans

**GAP we frequently see**

- Technical Teams implementing risk management controls for the business, but unsure if such controls are sufficient to meet corporate compliance obligations.
- Senior leadership unsure if controls implemented by I.T (In-house or outsourced) are sufficient to meet corporate compliance obligations.
- Plans of action or milestones do not exist, or lack structure, ownership, and accountability
- Critical assets that are part of the OT revenue generating network, or other business units (MSP) are often not included in the overall corporate cyber risk management strategy.

# C-Level Team, Board of Directors, Owners.

- Attestations (Signed by C-Level)
  - False Claims Act
  - DOJ. Millions of Dollars in penalties each year.
  - Increases annually
- Risk Management Plans
  - Independent 3rd party Audits
- FTC investigations (Unfair & Deceptive Practices)
  - Former UBER executive – Criminal charges
- FCC investigations (Consent Decrees)
  - ATT & T-Mobile exposed CPNI ($13 and $16 million dollars penalties in 2024)
  - Commitment to implement NIST Risk Management Plans
- CALEA
  - NPRM: NIST Risk Management Plans annually + Audits + Signed by C-level executives
- Incident response
  - 7 days after a reasonable determination of a breach. Secret service, FBI, FCC portal, notify customers.


THANK YOU