Yin and Yang of Cybersecurity and Governance and AI

MassCyber – Monthly Health Care Provider Call
December 10, 2025
Anne L Coulombe, Bleuet LLC

Bleuet
LLC

ABOUT ANNE

vCISO, CISO – contracts and advisory, e.g. CohnReznick (Tax, Audit, Assurance), Investics Analytics (FinTech start-up in big data)

CISO, Werfen -- Medical Devices, InVitro Diagnostics

Principal Security Lead, ProServe Healthcare & Life Sciences, AWS

Head of Data Protection, BISO, ISO EMEA & APAC, DPO

Active certs -- CISSP, CISM, CDPSE, PMP, FAIR, MBA

Yin and Yang

Ever felt pulled in many directions?

- Internal governance
- External governance
- Cybersecurity “the basics”
- Cybersecurity “at the speed of business” in “the age of AI”
- Frameworks and regulations, privacy
- Now we add AI to the mix (the seen and unseen AI)

How do you define governance?

What: act or process of governing / overseeing the control and direction of something

Core Definition: the framework of rules, relationships, systems, and processes within and by which authority is exercised and decisions are made and implemented (thanks Copilot…)

Rules of the Road: who, how, what, when, accountability mechanisms

How do you define cybersecurity governance?

Key Elements: Zero trust architecture, incident response, regulatory compliance (NIST CSF, ISO/IEC 27001, etc.)

Goal: Safeguard data, ensure resilience, and align security with business strategy [thanks Copilot …]

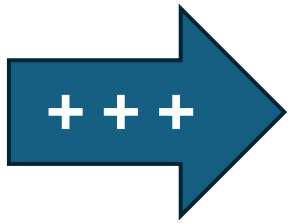
ISC2: strategic framework that guides how an organization manages and oversees its cybersecurity initiatives. Technical controls, aligning security with business goals, regulatory requirements, and risk management priorities

ISACA: "ensuring that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved"— includes cybersecurity

EC-Council: structured framework that enables key decision-makers—especially CISOs—to effectively manage an organization's IT security program. Policies, leadership, accountability, and strategic alignment

Governance Frameworks

Popular Frameworks	Focus Area
NIST CSF	Risk-based approach to identify, protect, detect, respond, recover
ISO/IEC 27001	Information security management system (ISMS)
CIS Controls	Prioritized actions to defend against threats
SOC 2	Data security and privacy for service providers
PCI-DSS	Payment card data protection



HIPAA

HITECH

HITRUST CSF

NIST SP 800-53

COBIT 2019

CMMC

NIS2

Many privacy regulations

CSA CSM

MITRE ATT&CK®

GDPR

ITIL

FDA Premarket Cyber Guidance

NIST HPH

ISO 14971

ISO 42001 (AI Governance)

Yin and Yang

- Not opposing forces
- Complementary disciplines that must co-exist in harmony
- Governance sets strategic direction, defines accountability, and aligns with business goals
- Cybersecurity protects direction, ensuring resilience, trust, and operational integrity
- Forms a dynamic system where leadership and defense reinforce one another
- Sometimes you must agree to disagree

Health Care: balancing protection and care

Governance Pillars in Health Care

Oversight, compliance and leadership

- **Regulatory Alignment:** HIPAA, HITECH, FDA, ISO 14971
- **Board-Level Oversight:** Cyber risk, AI risk as part of enterprise risk
- **Policy & Accountability:** Clear roles across clinical, IT, and executive teams
- **Vendor & Third-Party Governance:** Risk management for EHRs, cloud, and devices

Cybersecurity Execution

Technical controls, threat response, resilience

- **Medical Device Security:** Embedded governance in procurement and lifecycle
- **Incident Response & Continuity:** Plans that prioritize patient safety
- **Data Protection:** Encryption, access controls, and audit trails for PHI
- **Threat Intelligence:** Governance-driven monitoring and proactive defense

In health care, cybersecurity governance is not just about protecting data—it's about safeguarding patient trust, clinical integrity, and life-critical systems

Health Care: Scenario

Health Care: Reality

Governance Intentions

Oversight, compliance and leadership

- Regulatory Alignment: HIPAA, HITECH, FDA, ISO 14971, NIST HPH, NIS2
- Board-Level Oversight: Cyber risk integrated into enterprise risk management
- Policy Frameworks: HITRUST, ISO/IEC 27001, NIST CSF
- Clinical Integration: Security embedded in patient care workflows and device lifecycle
- Manufacturing, third-parties and product lifecycles affect entire PDLC/SDLC

Cybersecurity Execution Reality

Technical controls, threat response and resilience

- Siloed Teams: Security, compliance, and clinical operations rarely collaborate effectively
- Reactive Posture: Breach response dominates over proactive risk management
- Legacy Systems: Outdated infrastructure with limited patching and visibility
- Medical Device Blind Spots: Limited governance over connected devices and IoT
- Vendor Risk Exposure: Third-party EHRs and cloud platforms lack consistent oversight
- Budget Constraints: Cybersecurity underfunded relative to clinical priorities

Healthcare cybersecurity governance must evolve from compliance-driven checklists to risk-informed, patient-centric strategy. The stakes aren’t just financial—they’re clinical.

What You Can Do

Match intent and execution

- Your priorities

- Must have … regulatory, clinical integration, patient data protection, patient safety, EHR integration, third party risk, AI policy

- Should have … security embedded in patient care workflows and device lifecycle, cybersecurity embedded in all of your product lifecycles (and don’t forget the physical buildings!), continuous situational training

- Nice to have … embedding cybersecurity in everything you do, reducing technical debt, patients actively participating

- Words matter: what is risk, what words are used, how it is measured

What About AI?

Where is it used today, and how to plan for the future

- Your priorities
- It is embedded in more places than you may think!
- Within medical applications, within your IT infrastructure, in every day usage, how patients interact with AI
- AI policy, controls + verification, understand your data flows and where AI fits in, education
- Determine which group owns AI policy, who owns AI controls, who owns data privacy, how do all groups work together?
- Be prepared for continuous monitoring and constant enhancements to understand / leverage / benefit from AI while keeping your data safe

Take aways

Yin and Yang creates a dynamic environment

Need cooperation and mutual benefit between cybersecurity and governance

Governance cannot be a checkmark

Cybersecurity is about protecting people / data / systems -- but never in a vacuum

Priorities rule: sometimes you must agree to disagree

AI Policy Highlights

- **Purpose and Scope** – include a statement about criteria for risk and safety, protecting patients and employees,
- **Define AI** – include a definition of AI for your environment, and what it means with third and fourth parties.
- **Responsible Use -** list type of AI tools that are allowed / approved, including their specific use cases (not specific tool names), include allowed and disallowed categories for use cases.
- **Data Privacy and Security** - include guidelines on how data should be handled when using AI tools. From types of data that can be input / used in AI systems and/or models, where the data is stored and who has access to it (goes beyond DPA and BAA), what sensitive information must be protected to prevent data breaches.
- **Ethical Use and Bias Prevention** – important for setting expectations for fair and non-discriminatory use of AI. Used in hiring, performance evaluation, medical decision support (must check the model and it's training data).
- **Governance -** for oversight and accountability, this aligns with your governance framework. Define who is responsible for managing AI use within the organization, typically supported by a multi-disciplinary team. Establish a clear reporting process for any concerns, questions or uncertainties regarding AI tools or use of data.
- **Compliance –** a statement about monitoring, auditing, and impact of misuse.
- **Training and Awareness** - continuous training for employees on how to effectively use AI tools and understand their limitations. Consider training / educational material for patients and your third parties to ensure alignment. Objective is confidence in using AI and reduce risks of misuse.
- **Legal Compliance** - AI policy must align with relevant laws and regulations.
- **Regular Review and Updates** – plan for change and assume this policy will require frequent reviews, some areas may need reviews every 3-6 months. The AI policy must adapt to new technologies, innovations, regulations, and organizational changes.

1-5 pages, in clear language, embracing evolution and use of AI while ensuring safe use

Enjoy the ride

THANK YOU

Stay safe out there!

Anne L Coulombe

linkedin.com/in/annecoulombe

(if connecting: please add a note about where we met)