AUBREY IAN PERIN, CISSP | MBA
Hudson, NH | linkedin.com/in/aiperin/
Enterprise Cyber Risk & Security Governance Executive | Published Author

EXECUTIVE PROFILE

Enterprise Cyber Risk and Governance Executive with nearly 20 years of experience leading risk intelligence, vulnerability strategy, and security modernization. MBA-trained and pursuing legal education (JD), bringing financial fluency, fiduciary literacy, and structured risk quantification to C-suite and board-level discussions. Published author of *Ethical Business* (2025), architecting proprietary frameworks (CWE, ALE Standard) to align corporate accountability with capital allocation insight.

CORE LEADERSHIP CAPABILITIES

- **Enterprise Cyber Risk Strategy**: Translating complex technical exposure into board-level risk posture.
- **Proprietary Risk Modeling**: Developer of the ALE (Expanded Balance Sheet) and CWE frameworks.
- **Vulnerability & Exposure Management**: Leading enterprise-scale remediation in regulated environments.
- **Strategic Security Investment**: Optimizing multi-million dollar tech stacks (e.g., Microsoft E5) for maximum ROI.
- **Regulatory & Compliance Alignment**: Expert in NIST 800-53, CMMC, and emerging fiduciary disclosure requirements.

PROPRIETARY FRAMEWORKS & INTELLECTUAL PROPERTY

Author, *Ethical Business: Restoring Philosophical Integrity* (2025)

- **The ALE Standard**: Developed an "Expanded Balance Sheet" formula for systemic risk and corporate accountability.
- **Corporate Welfare Equation (CWE)**: Created a quantitative metric to evaluate company integrity and economic impact.
- **Marketing Integrity Test (MIT)**: A formula-based approach to assessing organizational transparency.

PROFESSIONAL EXPERIENCE

MassMutual, Hybrid – September 2024 – Present – Vulnerability Manager
Lead vulnerability risk evaluation within a regulated financial services environment, translating technical exposure data into executive-ready risk assessments.

- Lead enterprise vulnerability risk evaluation within a regulated financial institution, translating technical data into executive-ready prioritization frameworks.
- Advise senior leadership on remediation sequencing aligned to regulatory expectations, operational resilience, and enterprise risk tolerance.
- Integrate CVE intelligence and exploitability trends into structured governance reporting for high-stakes financial scrutiny.

Qualys Inc, Remote – January 2021– June 2024 - Lead Threat Intelligence Analyst
Directed strategic threat intelligence operations within a global cybersecurity platform organization.

- Directed a 6-person Threat Research Unit within a global cybersecurity platform serving enterprise customers worldwide.
- Led the development and publication of the **Qualys TruRisk** and **TotalCloud Security Insights** reports, defining industry standards for risk analytics.
- Aligned adversary intelligence strategy with product direction, influencing executive-level product and operational decision-making.

FLIR Systems, North Billerica, MA – December 2018 – January 2021 - Vulnerability Manager
Led vulnerability and endpoint security modernization within a complex enterprise environment.

- Directed the modernization of enterprise EDR solutions, aligning technical tooling with global risk exposure and operational requirements.
- Designed and maintained security control frameworks aligned with NIST 800-53 and CMMC for federal defense compliance.
- Coordinated cross-functional remediation efforts across IT and engineering, applying "Lean" principles to eliminate process waste.

Microsoft Corporation, Redmond, WA – April 2015 – March 2018 - Security Program Manager/Threat Analyst
Operated within Microsoft Threat Intelligence Center, supporting defense against advanced persistent threats and cross-organizational security strategy.

- Operated within the Microsoft Threat Intelligence Center (MSTIC), defending against advanced persistent threats (APTs).
- Served as a primary liaison with the FBI for APT-related investigations and cross-organizational security strategy.
- Managed 180+ active vulnerability coordination cases simultaneously, ensuring SLA compliance for enterprise products like O365.

US Air Force – January 2007 – March 2012 - Cyber Intelligence Analyst
Operated within mission-critical cyber defense environments.

- Developed advanced intrusion detection and anomaly detection methods, reducing false positives and improving detection precision.
- Led analytic missions and training initiatives.
- Conducted malware research and mitigation strategy development.
- Contributed to automation initiatives within network defense operations.

EDUCATION & CERTIFICATIONS

- Juris Doctor (JD) | New England Law Boston, In Progress
- Master of Business Administration (MBA) | University of New Hampshire, 2025
- Certified Information Systems Security Professional (CISSP) | License #503648
- Bachelor of Arts | Southern New Hampshire University, 2021

THOUGHT LEADERSHIP

Strategic Publications: Author of papers on Risk Quantification, Security Investment Optimization, and the Business Logic of Remote Work.

Portfolio: aubreyperin.com/publications-scholarly-writing.html