



SECURITY CONVERGENCE: COMBINING FORCES

BRIDGING THE DIGITAL AND THE PHYSICAL

CYBERHAGEN CYBERCRIME CONFERENCE, COPENHAGEN, DENMARK – 13 SEPTEMBER, 2023



- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP
- Former Principal Investigator, US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Former CEO, Director, Instructor, and President Emeritus
- SANS ISC456 Instructor: Essentials for NERC Critical Infrastructure Protection
- US Coordinator, Centro de Ciberseguridad Industrial (CCI)
- Instructor, Cyber Information Security Leader (CISL), CSA CPH
- Former utility staff (telecommunications, water & electric)
- One of the original architects of NERC CIP standards for North America
- First NERC CIP auditor in the US
- NERC SCWG, SITES, and SPIDERWG contributor
- Speaker/contributor to multiple FERC Technical Committees, NOPRs and Orders
- Contributing author for DHS CISA Cross-Sector Cyber Performance Goals (CPGs)
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- National Telecommunications and Information Administration (NTIA) and Idaho National Lab (INL) Software Bill of Materials (SBOM) Energy POC Stakeholders
- DOE Solar Energy Technology Office (SETO) and National Renewable Energy Lab (NREL) Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- Advisor to multiple industrial hardware and software vendors

AMPERE INDUSTRIAL SECURITY



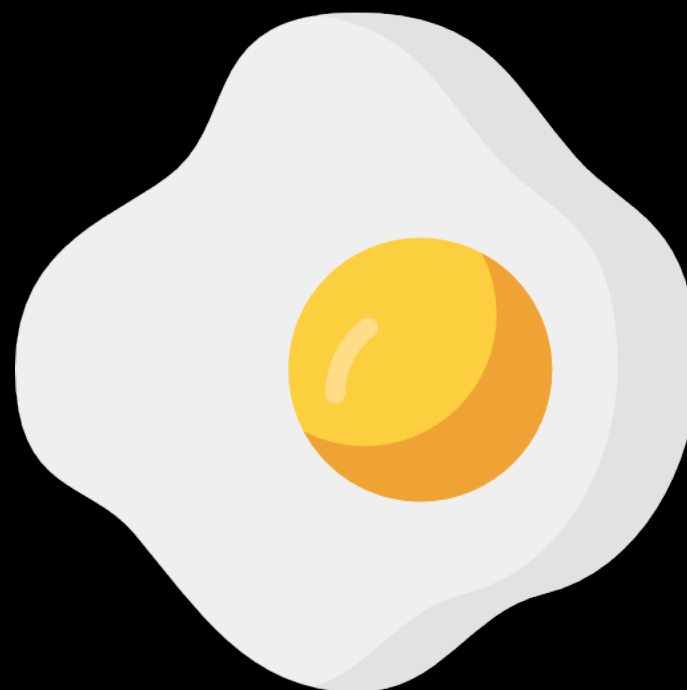
- Pure services, specialized consulting firm
- Industrial (OT/ICS) cybersecurity
- Industrial physical security
- Regulations, standards, and frameworks
- Operations in USA, Canada, Europe

We keep you ahead of your adversaries – and your auditors

CHICKEN OR EGG?



- You don't get cybersecurity without physical security.
- You don't get physical security without cybersecurity.
- These two functions were different in the past. This is no longer the case.
- Go watch any heist movie.





PHYSICAL THREATS TODAY

- Very few organizations are truly local (think supply chain)
- Geopolitical tensions
- Active warzones
- Politics
- Disinformation and misinformation
- Terrorism, supremacy
- Religious/belief
- Domestic/relationship
- By the time it is physical, it is serious





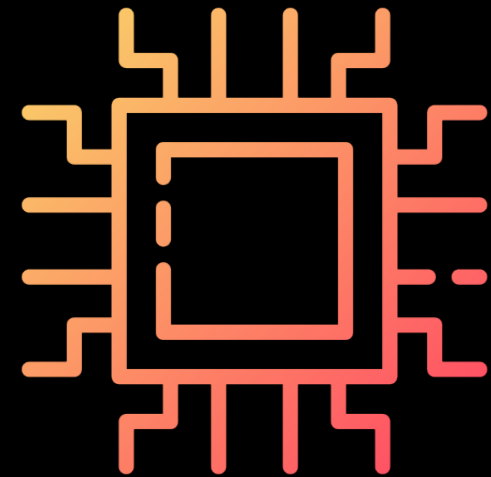
EVERYTHING IS DIGITAL

- Vendors are only creating new digital components
- Analog equipment is going away
- Biometrics
 - Face, palm, fingerprint, gait, blood vessels, handwriting
- Cameras – so many cameras
- Readers
 - Anti-spam, keyed read,
- Sensors
 - REX, temperature, light, motion, weight/force
- Locks, hasps, jams, guards, gates, guns...



PHYSICAL IS CYBER

- PACS Servers
- PACS Workstations
- Badge printers
- Badge readers
- Digital keys
- Gates
- Locks
- Facial recognition/biometrics
- Camera and data analytics





INNOVATION ALWAYS WINS

- Innovation, disruption and human nature
- Mobile everything
 - Instant access to anything from any device from anywhere
- Cloud
 - If everything is digital, everything creates a data stream
 - Someone else will always be better at analytics
- Vanishing technology
 - Embedded cyber/physical security technology
 - Size will continue to get smaller
 - May eventually become invisible to the eye



1985 CALLED

- Who you hire matters most
 - Think forward not backward
- CISO, CPSO, CSO
- CFO, COO, CRO, OGC
- Facilities
- Property management
- "Other duties as assigned"
- Budget benefits
 - Technology integration
 - SOC training/staffing
 - Network connectivity





DATA IS EVERYWHERE

- Converging physical and cyber security data is powerful
- Add in other operational data for more context
- Break down organizational silos to share
- Synthesize key data for full picture
- Do not forget to balance privacy
 - Not everyone is a threat
 - Insider threat programs can go too far
 - Be clear on all international regulations
 - Focus on the critical functions/personnel





INCIDENT RESPONSE BENEFITS

- Goal: enhanced incident response coordination
- Combined in a SOC or with clear communications paths
- Diversions, two-front, cross-domain intent
- Physical access vs. cyber access indicators
 - A situation in one should alert the other
- Dual-approach expertise with external law enforcement
- Respective "coverage" during active incidents



EXAMPLES OF CONVERGENCE

- Badge read compared with system login
- Critical location and critical commands
- License plate compared with badge read and login
- Badge read and geographic distance between two points
- ITSMF for PACS; manage it like technology
- Cross-discipline threat sharing
- Holistic security approach for entire organization
- Enhanced safety in OT/ICS environments

SUMMARY



- Physical and cyber security threats, technologies and practices are converging – more each day
- Physical security practices (and mindsets) need to change to keep pace with innovation and convergence
- Infosec, OT-sec, and IT can assist with successful approaches
- Organizations should consider how to maximize the benefit of holistic convergence
 - Data analysis
 - Threat management
 - Incident response

CONTACT ME



Patrick C. Miller – CEO, Ampere Industrial Security

- pmiller@amperesec.com
- <https://www.linkedin.com/in/millerpatrickc/>
- [@patrickcmiller@infosec.exchange](https://infosec.exchange)
- [@patrickcmiller.bsky.social](https://bsky.social)
- [@patrickcmiller](https://twitter.com/patrickcmiller)
- +15032721414

