Redefining Cybersecurity Engineering - A Manifesto for Clarity, Structure, and Discipline

Introduction: The Call for an Engineering Discipline

As outlined in our post, "Bringing Clarity and Conformity to Cybersecurity Standards," a structured approach to cybersecurity engineering is more urgent than ever. Securing our digital infrastructure becomes a moral imperative as cybersecurity threats grow more complex. The current state of cybersecurity engineering lacks the foundational rigor found in traditional engineering disciplines, leaving organizations vulnerable to evolving threats. ISAUnited is committed to addressing this gap by establishing cybersecurity engineering as a robust discipline rooted in systems engineering principles.

The Problem: A Field Without Structure

Cybersecurity engineering today is fragmented. It is overly reliant on vendor-driven tooling and certifications, focusing on tactical responses rather than strategic, long-term solutions. The proliferation of thin and shallow certifications has further diluted the industry's depth. While these fast-track certifications promise quick credentials, they often lack the depth to develop true engineering expertise. Many cybersecurity practitioners earn various certifications but often find it challenging to prevent data leaks and workplace compromises effectively.

This overemphasis on certifications undermines the industry’s credibility and shifts focus away from the proper engineering principles needed to build resilient systems. Even organizations with large budgets for tooling continue to suffer from security failures, proving that the sole answer lies in fostering a culture of robust cybersecurity engineering through formal education. The absence of university and college degrees tailored to cybersecurity engineering has left a void that only proper academic programs can fill. Unlike traditional engineering disciplines—built on a foundation of structured methodologies, lifecycle management, and traceability, cybersecurity lacks a unified framework to guide professionals in designing and securing complex systems.

This absence of structure has led to inconsistent standards, limited accountability, and a workforce that is ill-equipped to address the systemic nature of modern threats. The

result is a reactive, patchwork approach prioritizing immediate fixes over sustainable solutions.

The Vision: Engineering for the Future

At ISAUnited, cybersecurity must evolve into a true engineering discipline that integrates traditional engineering fields' clarity, discipline, and structure. Guided by our manifesto statement, we propose a vision for cybersecurity engineering that is:

- **Clarity**: Developing standards and practices that are transparent, understandable, and actionable.
- **Discipline**: Embedding rigor and traceability into every phase of the cybersecurity lifecycle.
- **Structure**: Establishing a robust foundation of methodologies and frameworks to ensure consistency, coherence, and resilience in cybersecurity engineering practices

This vision is not only aspirational but actionable. By leveraging systems engineering principles, we can create a foundation for cybersecurity engineering that addresses the unique challenges of the digital age.

The Path Forward: Building an Engineering Discipline

1. **Adopting Systems Engineering Principles**:
    - Integrate lifecycle processes, including concept development, design, implementation, and retirement.
    - Emphasize traceability and interdependence, ensuring that every system component contributes to its security.
2. **Developing Unified Standards**:
    - Collaborate with industry leaders, academic institutions, and professional organizations to create technically rigorous and universally applicable standards.
    - Focus on actionable guidelines that bridge the gap between compliance and engineering excellence.
3. **Empowering the Workforce**:

- Advocate for establishing cybersecurity engineering degree programs in universities and colleges to replace the reliance on fast-track certifications.
- Design educational programs and professional certifications emphasizing engineering fundamentals over tool-specific expertise.
- Foster a culture of innovation, encouraging cybersecurity engineers to think strategically and creatively.

4. **Promoting Inclusivity and Collaboration**:
   - Unite diverse perspectives by engaging stakeholders across industries and academic institutions.
   - Ensure that standards and practices are inclusive, addressing the needs of organizations of all sizes and sectors.

ISAUnited: A Beacon for Structured Cybersecurity

ISAUnited is a beacon for advancing cybersecurity into a more structured, mature, and disciplined field. As the industry faces increasingly complex threats, ISAUnited serves as the platform to unite professionals, institutions, and organizations in a shared mission to redefine cybersecurity engineering. By providing the tools, standards, and collaborative opportunities necessary for clarity and consistency, ISAUnited empowers security practitioners to build robust, resilient systems.

Conclusion: A Call to Action

The time has come to redefine cybersecurity engineering. By embracing systems engineering principles and building a disciplined, structured approach, we can empower professionals to design resilient systems that protect what matters most. At ISAUnited, we invite you to join us in this mission, uniting clarity, discipline, and practicality to create a future where robust security is not just a goal but a reality.

Together, we can transform cybersecurity engineering from a fragmented field into a respected and practical discipline, ensuring confidence and consistency in the face of evolving threats.

With respect and commitment to our shared mission,

Arthur Chavez
President and Chief Security Architect of ISAUnited.org