POSITION STATEMENT

Siemens' Operationalizing Cybersecurity

Putting ideas into action
usa.siemens.com/ruggedcom-cybersecurity

In the face of advanced, persistent, and evolving cybersecurity threats to private enterprise and critical infrastructure, decisionmakers must put strategies and technologies into action in their day-to-day operations.

Operationalizing cybersecurity plays a critical role in protecting operational and business continuity and avoiding potential costs and impacts to public safety.

SIEMENS

Coining a term

"Operationalizing cybersecurity" refers to the ongoing implementation of cybersecurity frameworks, policies, processes, and technologies to secure Operational Technology (OT) networks and the Industrial Control Systems (ICS) that run them. It is a proven approach to establishing and maintaining a comprehensive cybersecurity program. Operationalizing cybersecurity means putting ideas into action.1 [See "Operationalizing Cybersecurity: Evolution, Seamlessness and Holistic Thinking as Key Drivers," Forbes.com, 9 May 2019]

Operationalizing cybersecurity assures business continuity and thus avoids the prospect of interruptions in production and the damage to operational networks that can ensue. This outcome can only be achieved when frameworks, policies, processes, and technologies are successfully integrated into actual physical and digital operations on a continuous, ongoing basis.

The drivers for operationalizing cybersecurity include advanced, persistent and constantly evolving cyber threats, some of which make headlines, many of which do not surface in the news.

This approach sounds simple – the best ideas are simple – but implementing operationalizing cybersecurity requires expert, experienced management of many disparate elements and functions.

These elements and functions include:

- Developing a comprehensive cybersecurity strategy or strategies that addresses both operational and enterprise networks,
- Identifying and selecting a relevant cybersecurity framework,
- Creating pertinent policies and procedures for personnel,
- Instituting "cybersecure by design" networks and technologies, and
- Coordinating and implementing these elements under the guidance of an experienced, trusted advisor.

Drivers

Comprehensive, effective cybersecurity for OT networks and the ICSs that run them has rapidly become a prerequisite for the continuity of critical infrastructure operations in the face of advanced, persistent, evolving threats.

Frequent headlines attest that ensuring operational and business continuity for critical infrastructure should make this topic top-of-mind for C-suite decisionmakers as well as the gamut of stakeholders, including customers and regulators. Because regulatory reporting requirements for various infrastructure sectors vary, it is widely understood that cybersecurity breaches reported in the news represent only the tip of an iceberg of unknown but pervasive proportions.

Today, profit-seeking criminal organizations seek to disable critical infrastructure and, using ransomware-as-a-service, demand huge payments to release their grip on operational networks. Potential outcomes include the disruption of operations that could result in the destruction of facilities and impact public safety. This trend applies to power plants, water and wastewater treatment facilities, oil and gas installations, automated industrial facilities, food and beverage manufacturing – in short, private and public enterprises that support civil society and help drive our economy.

Simply put, the leadership of these facilities is responsible for addressing tangible if unpredictable threats to the continuity of their operations. Failure in this regard can lead not only to loss of operational and business continuity, but to associated costs, injury to reputation, loss of market and brand value and the confidence of the public, regulators, investors, and other stakeholders. Ultimately, in the worse-case scenario, human lives are at stake.

Yet, as headlines attest, a significant proportion of legacy and even new operations in these infrastructure sectors remain vulnerable. Decisionmakers may hesitate to act on the cybersecurity threat for a variety of reasons. They may not have experienced a significant cybersecurity breach. They may view the expense as a cost rather than as an investment. They may not possess the in-house expertise to navigate the abundant uncertainties and choices inherent in the process. They may be overwhelmed by the myriad challenges posed by the creation of a comprehensive cybersecurity program.

One of the fundamental challenges is how to operationalize cybersecurity; in other words, how to put strategies, solutions, and technologies into meaningful, ongoing action to maintain operational and enterprise continuity.

Putting ideas into action

Large organizations, such as those running critical infrastructure, will always face a challenge in creating and maintaining a culture that embraces a new prime directive such as cybersecurity. Thus, consistent, dedicated C-suite leadership and support is required for a pan-organizational, holistic approach to cybersecurity that echoes the traditional industrial commitment to safety. Think of cybersecurity in the 21st century as Safety 2.0, a comprehensive approach that addresses the gamut of physical, OT, and Information Technology (IT) cybersecurity. Just as industrial safety programs have evolved as ongoing data establish evolving dangers, so a cybersecurity program must adapt to evolving threats. A cybersecurity culture internalizes the fact that threats to operational networks are persistent and ongoing.

The actual how-to aspect of operationalizing cybersecurity begins with selecting from among a diversity of existing, well-established risk-management frameworks that apply to the specific industry and types of operational networks in question. Selecting from among these risk-management frameworks will help an organization define an acceptable level of risk, giving scope and scale to proactive cybersecurity strategies and investments. To select an applicable framework, an organization must determine its own business goals and processes and how to take practical, affordable steps to achieve cybersecurity to its own specific case.

Over the past two decades, as the cyber threat to OT networks became real and deterrence became urgent, globally recognized authorities developed a variety of risk management frameworks. These frameworks were specifically developed for OT environments and spell out the process of identifying risks, assessing the potential impact of those risks, and planning how to respond if the risks lead to impactful cyber-attacks.

A brief review of these risk management frameworks should suffice to illustrate their purpose.

Risk Management Frameworks

International Electrical Commission (IEC) 62443 provides a series of standards that specify security capabilities for industrial automation and control system components, using a flexible framework to address and mitigate current and future security vulnerabilities.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk, prioritize investments and maximize the impact of cybersecurity budgets.

NIST Special Publication (SP) 800-82 Rev. 3: ***Guide to Industrial Control Systems (ICS) Security***, is being updated to align with relevant NIST guidance and other relevant control system cybersecurity standards and best practices, and to address changes in the threat landscape.

ISO/IEC 27001 provides requirements for an information security management system.

The European Union Agency for Cybersecurity (ENISA) seeks to enhance the trustworthiness of information and communication technology (ICT) products, services, and processes with cybersecurity certification schemes and keep society and citizens digitally secure.

The U.S. Federal Communication Commission (FCC) is tasked with protecting Customer Proprietary Network Information (CPNI), which requires consumer communication carriers to file annual reports certifying their compliance with CPNI rules.

The U.S. Department of Energy's voluntary Cybersecurity Capability Maturity Model (C2M2) has been adapted for both IT and OT networks for building, maintaining, and maturing a cybersecurity program.

Risk assessment tools

In addition to these well-known, vetted risk-management frameworks, methodologies are available for Quantitative Risk Assessment (QRA), which is a systematic, analytical approach to quantifying risks arising from the operation of an engineering process, such as an operational network. We mention just four well-regarded QRAs here:

- OCTAVE® – Operationally Critical Threat, Asset, and Vulnerability Evaluation, is a self-directed approach that puts responsibility on leadership for setting an organization's cybersecurity strategy.
- FAIR™ – Factor Analysis of Information Risk has emerged as a valuable framework for determining cybersecurity and operational risk.
- NIST 800-30, Guide for Conducting Risk Assessments helps organizations identify and manage privacy risks to enable innovation, while protecting individuals' privacy.

- NIST Framework for Improving Critical Infrastructure Cybersecurity defines the core activities and outcomes of a successful cybersecurity program, including five key functions – identify, protect, detect, respond, recover – which can be applied to manage cybersecurity at an acceptable level of risk and investment defined by the organization itself.

Based on the selected framework, an organization must develop strategies and policies that map to business goals and processes. Those strategies and policies must address how people, processes, and technology adopt and support cybersecurity within practical, affordable limits.

These risk-assessment frameworks apply to both legacy systems and new, "greenfield" networks. A review of legacy systems in the United States, for example, should comply with the Federal Energy Regulatory Commission's (FERC) Critical Infrastructure Protection standards v.5, adopted in 2013, which require utilities to adopt well-defined cybersecurity measures for networks not originally designed with cybersecurity in mind.

Mandates under CIP v.5 standards require a defense-in-depth approach that include well-recognized measures such as zero trust policies, virtual private networks, encryption, multi-factor authentication, network segmentation, next-gen firewalls, deep packet inspection, intrusion detection systems, intrusion prevention systems – measures that do not compromise network efficiency.

In contrast, new, "greenfield" networks and systems must adhere to Cybersecurity by Design concepts, to avoid introducing new, avoidable vulnerabilities.2 [See "Siemens' Cybersecurity by Design: Global leadership advances a cybersecure world."]

Cybersecurity by Design's purpose is to prevent intrusions. Yet the cat-and-mouse game of protection against evolving, advanced persistent threats recognizes that breaches are inevitable. Thus, Operationalizing Cybersecurity must include strategies and capabilities for operational recovery known as resilience.

One major goal in Operationalizing Cybersecurity is to achieve actual cybersecurity protections while also meeting any mandated or anticipated compliance requirements. The latter must be anticipated for any industry or operational network as headlines about cybersecurity incidents continue to drive new reporting and compliance requirements.

Siemens' own cybersecurity culture

A significant aspect of coordinating and applying these various steps in Operationalizing Cybersecurity is acquiring the guidance of a trusted advisor with a deep heritage in designing, manufacturing, installing, maintaining, and protecting operational networks.

Siemens' embrace of cybersecurity began more than 35 years ago. The company recognized that this approach – crucial to industrial network integrity, infrastructure safety, and business continuity – would become fundamental to its own enterprise. Therefore, its advances in this area would be critical to its customers as well. It's widely recognized that industrial automation offers competitive efficiencies, productivity, and profits. Siemens has pioneered a corollary: that competitive efficiencies, productivity, and profits are only assured when operational and business continuity are supported through a holistic approach to OT and IT cybersecurity.

As Siemens pursued industrial network cybersecurity over decades, it developed a sense that a holistic approach required more than smart, technical solutions and stringent policies. To truly embrace cybersecurity as a linchpin of its own operations and those of its customers, Siemens

developed an organizational culture that explicitly recognized the intrinsic value of cybersecurity as a guarantor of network integrity and infrastructure safety, as well as business continuity.

This organizational culture was codified in 2018 when Siemens reorganized all of its cybersecurity resources, operations, and personnel into a single, global network dubbed "Product and Solution Security." This unified team of more than 1,300 people provides even greater speed and flexibility in dealing with the rapidly evolving threat landscape.

Today, Siemens' global enterprise lives and breathes cybersecurity as it continues to focus its own organizational culture on this critical element of reliability and trust in a networked, digital world.

Thus, Siemens is well-positioned by experience and expertise to recommend a culture of cybersecurity. Just as people are an organization's greatest asset, so they can become a weak link as well. Simple mistakes can lead to unintended consequences, creating vulnerabilities to external actors or incidents in themselves. On a positive note, this weakness can be an opportunity for the most improvement. Adopting a cybersecurity culture is a 21st century challenge, just as a safety culture was developed in the 20th century in response to the dangers of industrial processes.

Siemens' resources

Siemens can perform the role of trusted advisor and ongoing cybersecurity partner based on our own heritage, culture, and development of best practices as applied to our own operations and enterprise.

Our Information Security (InfoSec) protocols rely on Secure File Exchange (SecuFEx) to protect our own – and, by extension, our customers' – confidential data. Our Product Certification (ProductCERT) teams support Siemens' own personnel as well as our partners and customers by rapidly responding to security threats, incidents, and newly discovered vulnerabilities. Our SiemensCert team secures our own infrastructure and assesses potential impacts to enterprise continuity while serving as a trusted research partner to industry and academia. Siemens has developed a formal process for handling reported security vulnerabilities in our own products, processes, and infrastructure that encompasses not just vulnerabilities but incidents and recovery planning as well – a process that we apply to our customers.

Siemens was the first company, globally, to gain TÜV SÜD certification for an effective, interdisciplinary process of developing our automation and drive products. This includes industrial software based on the International Electrotechnical Commission (IEC) 62443-4-1 global standard, including third-party components that covers open-source software quality assurance, architecture and design, and issue handling, as well as security updates, patches, and change management.

In a North American context, Siemens complies with the North American Electric Reliability Corporation Critical Infrastructure (NERC CIP) 13 standard for supply chain management relevant to critical infrastructure.

Internally, all Siemens software and firmware releases undergo Threat & Risk Analysis (TRA), vulnerability scanning, robustness and penetration testing.

These resources, certifications, and standards compliances – just a few pieces of a diverse tool kit – are governed by Siemens' own, comprehensive Cybersecurity Policy Framework that defines roles and responsibilities so nothing "falls between the cracks." Our own, internal processes extend to ongoing, mandatory personnel training to grow, maintain, and hone a cybersecurity-centric organizational culture.

By keeping its own house in order, Siemens is able to extend its hard-earned expertise to its customers, partners, and industry stakeholders.

How customers benefit

Siemens' end-to-end solutions involve Industrial Network Services, secure software, and secure hardware made for harsh industrial environments. Siemens' solutions meet the strictest cybersecurity requirements for communication, data integrity, access control, and continuous monitoring for industrial automation. Optimized integration ensures that all products, processes, and solutions we offer form a secure, end-to-end system. Our solution partners and supply chain providers all are required to meet strict security standards that match our own. In fact, third-party suppliers' compliance with these security standards is articulated in a binding clause in all new contracts for critical components such as software, processors, and electronics for ICSs.

Siemens' Industrial Network Services can play a leading role in assessing a client's operational requirements and designing a network from its underlying architecture to the "edge." Our teams conduct network assessments, asset inventories, and vulnerability assessments. They perform integrations and deployments and provide on-site services and support, always with the customer's explicit authorization and in line with the customer's own security policies. They also provide training for clients' ongoing OT network management and updates on the threat landscape.

Charter of Trust

As a trusted advisor and cybersecurity partner in the OT network domain, Siemens also has led a global effort to support cybersecurity beyond its own designs, products, and services. Our overarching goal is to make a digital world more secure. To that end, Siemens initiated the widely supported Charter of Trust, which urges the adoption of the highest appropriate level of security and data protection for all networks and network assets.

Directly addressing Cybersecurity by Design principles, the Charter emphasizes the need to ensure that cybersecurity is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

Since its founding in 2018 at the annual Munich Security Conference, the Charter's membership has grown to become a global consortium of leading stakeholders dedicated to a secure, safe, productive, digital future.

The Charter's three founding principles are to protect the data of individuals and companies, prevent damage to people, companies, and infrastructure, and create a foundation of reliability and confidence in a networked, digitized world and its future.

Let's talk

To have a conversation on how Siemens can advise your organization on Cybersecurity by Design, please give me a call.

Jeff Foley
Chief Technology Evangelist for Cybersecurity
Senior Business Development Manager
Siemens Digital Industry – Digital Connectivity and Power
Mobile +1 954.296.5648
Email jeff.foley@siemens.com

Published by
Siemens Industry Inc.

Siemens Industry, Inc.
100 Technology Drive
Alpharetta, GA 30005
United States of America

www.usa.siemens.com/ruggedcom-cybersecurity

Order No. RCPS-OPCYB-1121

SIEMENS