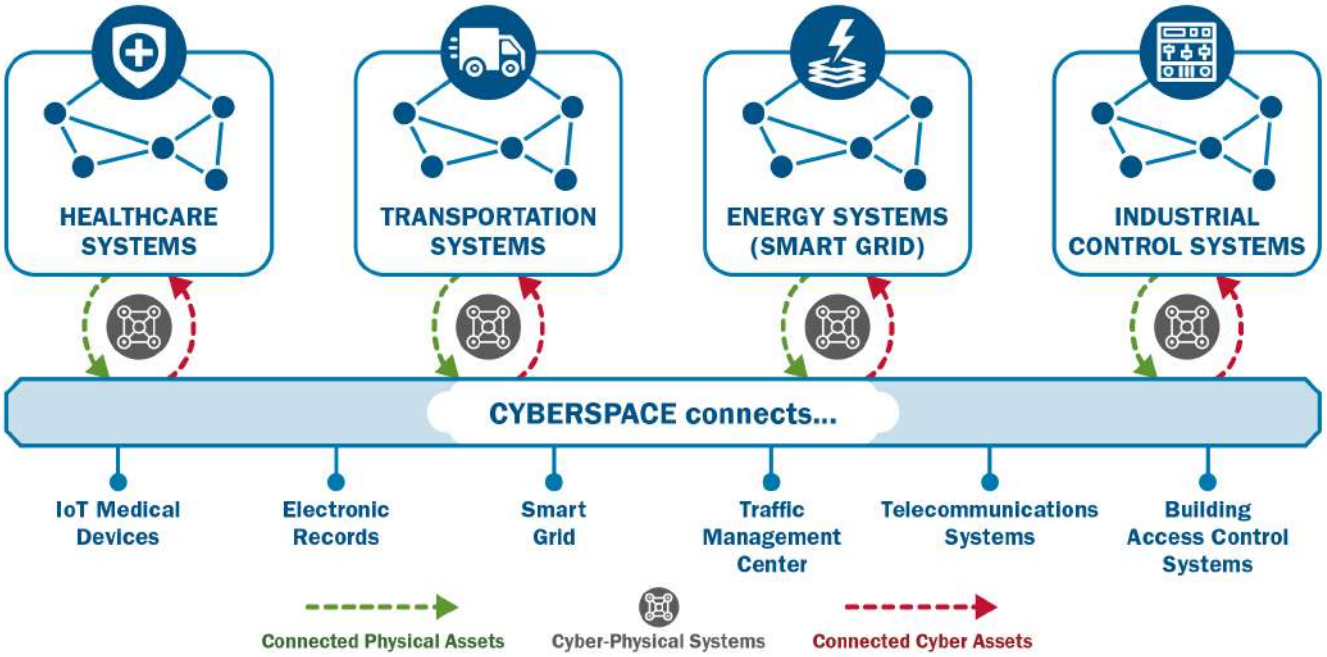
CYBERSECURITY AND PHYSICAL SECURITY CONVERGENCE

A CONNECTED OPERATING ENVIRONMENT

Today's threats are a result of hybrid attacks targeting both physical and cyber assets. The adoption and integration of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices have led to an increasingly interconnected mesh of cyber-physical systems (CPS), which expands the attack surface and blurs the once clear functions of cybersecurity and physical security. Meanwhile, efforts to build cyber resilience and accelerate the adoption of advanced technologies can also introduce or exacerbate security risks in this evolving threat landscape.

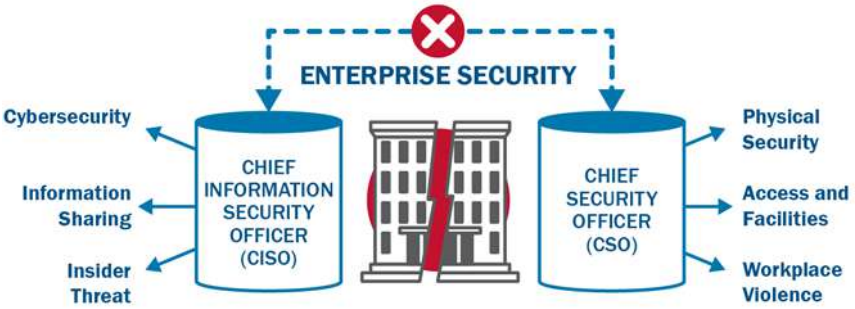


A successful cyber or physical attack on connected industrial control systems (ICS) and networks can disrupt operations or even deny critical services to society. For example:

- A security gap in access controls, such as unauthorized access to facilities or system permissions, can allow an individual to use a universal serial bus (USB) device or other removable hardware to introduce a virus or malware into a network.
- Heating, ventilation, and air conditioning (HVAC) systems can be virtually overridden, causing a rise in temperature that renders network servers inoperable.
- A cyber-attack on telecommunications can impair communication with law enforcement and emergency services, resulting in delayed response times.
- An unmanned aircraft system (UAS) can compromise sensitive information by gaining access to an unsecured network using wireless hacking technology.
- A cyber-attack exploiting healthcare vulnerabilities can compromise sensitive data or cause a connected medical device to malfunction, resulting in injury or loss of life.

ORGANIZATIONAL CHALLENGE: SILOED SECURITY FUNCTIONS

Together, cyber and physical assets represent a significant amount of risk to physical security and cybersecurity—each can be targeted, separately or simultaneously, to result in compromised systems and/or infrastructure. Yet physical security and cybersecurity divisions are often still treated as separate entities. When security leaders operate in these siloes, they lack a holistic view of security threats targeting their enterprise. As a result, attacks are more likely to occur and can lead to impacts such as exposure of sensitive or proprietary information, economic damage, loss of life, and disruption of National Critical Functions (NCFs).[1]



- Security functions operate independently with limited collaboration on enterprise-wide risks.
- Senior leaders and teams lack visibility of interconnected physical and cyber assets.
- Lines of communication are unclear and impede coordination and collaboration.
- Organization is unable to quickly identify, prevent, and respond to complex threats.

ORGANIZATIONAL SOLUTION: CONVERGED SECURITY FUNCTIONS

Convergence is formal collaboration between previously disjointed security functions. Organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified security policies across security divisions.

- Integrated security functions address cyber-physical infrastructure security.
- Holistic threat management ensures physical and cyber assets are secure.
- Senior leaders and teams communicate, coordinate, and collaborate.
- Organization is prepared to prevent, mitigate, and respond to threats.

BENEFITS OF CONVERGENCE

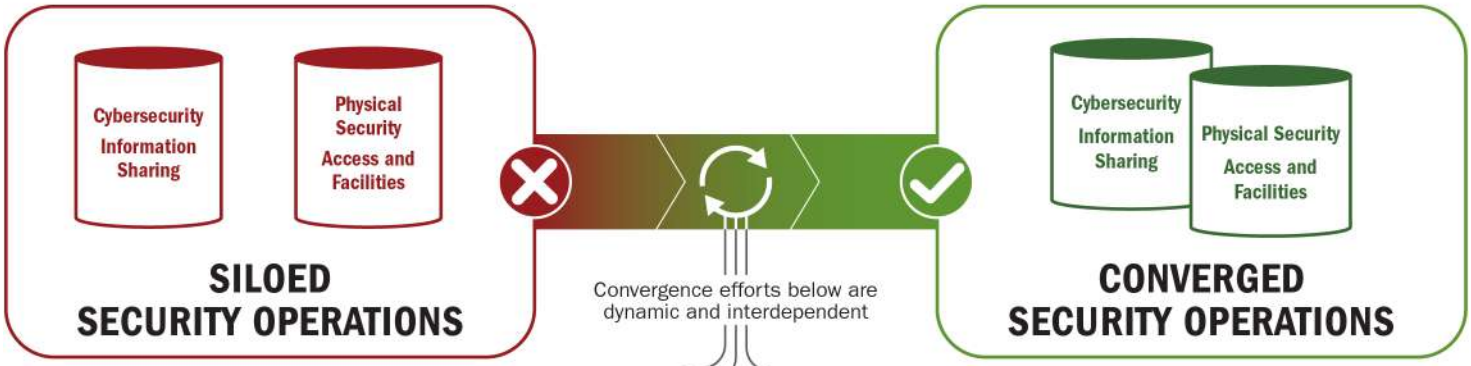
An integrated threat management strategy reflects in-depth understanding of the cascading impacts to interconnected cyber-physical infrastructure. As rapidly evolving technology increasingly links physical and cyber assets—spanning sectors from energy and transportation to agriculture and healthcare—the benefits of converged security functions outweigh the challenges of organizational change efforts and enable a flexible, sustainable strategy anchored by shared security practices and goals:

[1] For further information and resources on National Critical Functions: cisa.gov/national-critical-functions

GETTING STARTED

A culture of inclusivity is vital to successfully converging security functions and fostering communication, coordination, and collaboration. Organizations of all sizes can pursue convergence by developing an approach that is tailored to the organization's unique structure, priorities, and capability level. The guide below provides a flexible framework for developing a holistic security strategy that aligns security functions with organizational priorities and business objectives.

A FRAMEWORK FOR ALIGNING SECURITY FUNCTIONS



COMMUNICATION

Initiate a Dialogue
Enable communication with security leaders. Engage with upper management to discuss what convergence might look like within your organization—successful convergence relies on support from senior leaders.

Review Leadership Roles
Discuss whether your current leadership structure can be realigned.

Establish a Convergence Team
Identify key players, such as CSO, CISO, physical security, IT, cybersecurity, and facility managers.

Enable Information Sharing
Engage with team members across all security functions to identify points of convergence.

COORDINATION

Formalize Convergence Team Roles and Responsibilities
Establish a cadence and structure for team coordination and integration.

Identify Linked Assets
Coordinate with team members across security functions to assess cyber and physical assets and identify those that are linked. Assess the risk level of each asset based on linkages.

Conduct a Vulnerability Assessment
Identify gaps in security and risk mitigation and determine where gaps can be closed through convergence.

Determine the Baseline
Leverage initial assessments and gap analyses to determine the baseline for security operations and incident management.

COLLABORATION

Run the Numbers
Determine if convergence on any scale is financially feasible from a short-term and long-term perspective.

Prioritize Improvements
Identify and prioritize improvements, including patches, software updates, virus protection, and opportunities for automation.

Craft Risk-Driven Policies
Develop and implement risk-driven policies with broad applicability and that reflect converged security functions. Identify best practices.

Strategic Alignment
Align strategy to shared practices and goals. Focus on improving efficiency and increased information sharing.

Not ready to converge? Consider performing a security assessment. If you are unable to perform the assessment internally, seeking out a third-party assessment to identify security vulnerabilities may help identify your ideal path to converged security operations. For information on how CISA can help you, please see below for additional resources.

CONVERGENCE CASE STUDIES

Large Foreign Shipping Company, June 2017 – An indiscriminate state-sponsored cyber-attack unleashed a virus or "worm" that halted operations across hospitals, power companies, airports, banks, and government agencies and crippled the global shipping industry for more than a week. The virus was able to penetrate the network of the world's largest container shipping company through a single computer operating outdated accounting software. Although not the primary target, the company's global systems were quickly paralyzed, corrupting proprietary data and hampering communications. Maritime shipping ground to a halt as the outage isolated 76 ports and 800 vessels carrying millions of tons of cargo. The company's own financial losses exceeded $300 million and the ripple effects on global supply chains included impacts to the U.S. national security supply of vaccines. With total estimated costs in damages exceeding $10 billion, this incident is regarded as one of the most devastating cyber-attacks in recent history.

Large U.S. Energy Company, January 2019 – The company observed an evolving threat landscape and a lack of formal collaboration between physical security and cybersecurity functions, hindering the development of a comprehensive threat management strategy. These siloed operations led to significant financial consequences when an internal probe revealed 127 security violations that ultimately cost the company millions, all stemming from non-compliant security practices and lack of collaboration across organizational units. In response, the company increased oversight; restructured roles; hosted discussion panels on best practices for security and compliance; added resources to manage and implement compliance and security efforts; and updated/enhanced systems to track access and vulnerabilities. As a result, the company saw an improvement in information sharing and collaboration, as well as rapid identification and mitigation of threats.

U.S. Power Grid Operator, March 2019 – One of the first attacks on the U.S. power system occurred when hackers exploited a firmware vulnerability and caused a grid operator's firewalls to continuously reboot, leading to a brief communications outage. The attack led the North American Electric Reliability Corporation (NERC) to issue a series of recommendations, including: applying best practices for vulnerability and patch management; minimizing Internet-facing devices; using virtual private networks (VPNs) and access control lists (ACLs); layering defenses; segmenting and monitoring networks; identifying exploitable vulnerabilities; and employing redundant solutions.

IoT Devices Impacted by Ripple20 Vulnerabilities, June 2020 – A group of 19 vulnerabilities known as Ripple20 impacted millions of connected devices, including smart home devices, power grid equipment, healthcare systems, industrial gear, transportation systems, mobile/satellite communications equipment, and commercial aircraft devices. These high-risk vulnerabilities in critical IoT devices across numerous sectors could lead to compromised data and device malfunctions. In response, some vendors released their own recommendations to mitigate potential risks. The Cybersecurity and Infrastructure Security Agency (CISA) issued an alert on potential weaknesses that malicious actors could exploit and provided recommended mitigation approaches, including performing an impact analysis and risk assessment; minimizing network exposure for control system devices and systems; and ensuring access points are updated to the latest software version. Security researchers have identified additional impacted vendors and devices since Ripple20 was initially discovered.

ADDITIONAL RESOURCES

Connect with CISA: cisa.gov/publication/cisa-services-catalog

Connect with a Protective Security Advisor: cisa.gov/protective-security-advisors

Conduct a Cybersecurity Assessment: cisa.gov/cybersecurity-assessments

Infrastructure Vulnerability Assessments: cisa.gov/critical-infrastructure-vulnerability-assessments

Critical Infrastructure Sectors: cisa.gov/critical-infrastructure-sectors

Critical Infrastructure Exercises: cisa.gov/critical-infrastructure-exercises

Recommended Practices: us-cert.gov/ics/recommended-practices

For more information or to seek additional help, contact us at Central@cisa.gov.