MSU DENVER The Cybersecurity Center
Cybersecurity Multi-Use Training Environment

WAVE TOPS

White Paper Series
April 10th, 2026

Converged Security:
The Imperative to Break Down Silos in a Borderless Threat Landscape

Author:
Richard C. Mac Namee MCGI, FInstLM, CPP, CISSP

The Cybersecurity Center
1250 7th St, Suite 118, Denver, CO 80204
thecybersecuritycenter@msudenver.edu

Executive Summary

The modern threat environment has fundamentally evolved. No longer confined to discrete domains, threats now traverse seamlessly across Personnel Security, Physical Security, Information Security, and Emergency and Crisis Management response. This convergence has rendered traditional siloed approaches obsolete and increasingly dangerous.

Organizations that continue to treat these disciplines as independent functions are exposed to systemic vulnerabilities, delayed response times, and fragmented decision-making. In contrast, those adopting a Converged Security model gain a unified operational picture, enhanced resilience, and the ability to respond to complex, multi-domain threats in real time.

This paper argues that converged security is not a theoretical evolution but an operational necessity. It outlines the drivers behind convergence, illustrates real-world implications, and provides a strategic framework for implementation.

The Collapse of Traditional Security Boundaries

Historically, organizations have structured their security functions along distinct lines:

- Personnel Security – vetting, insider threat, workforce trust
- Physical Security – facilities, access control, surveillance
- Information Security – networks, systems, data protection
- Emergency and Crisis Management Response – incident response, continuity, recovery

This separation was logical in an era where threats were largely domain-specific. However, the digital transformation of society, combined with geopolitical instability, hybrid warfare, and advanced persistent threats has essentially dissolved these boundaries.

The New Reality

Modern threats are that we are increasingly encountering today are appearing in blended form as follows:

- Hybrid – blending cyber intrusion with physical access
- Human-enabled – exploiting insider vulnerabilities
- Rapidly cascading – a single breach triggering multi-domain consequences
- Ambiguous in origin – blurring criminal, state-sponsored, and insider actions

Example: A compromised employee credential (Personnel Security) enables unauthorized building access (Physical Security), which facilitates the installation of a rogue device on the network

(Information Security), resulting in a ransomware attack that halts operations and triggers crisis response protocols (Emergency Management).

In this new environment, no security domain operates in isolation and the imperative to adjust our postures is immediate.

The Risks of Siloed Security models

Despite the changing threat landscape, many organizations continue to operate within legacy structures. Doing so creates critical vulnerabilities:

Fragmented Intelligence

Each function collects valuable data, but without integration:

- Warning signs remain isolated
- Patterns go undetected
- Threats escalate unnoticed

Delayed Response

Siloed teams often:

- Escalate issues sequentially rather than collaboratively
- Operate under differing priorities and protocols
- Lack shared situational awareness

Time lost in coordination is often the difference between containment and catastrophe.

Conflicting Objectives

- IT prioritizes uptime
- Physical security prioritizes access control
- HR prioritizes employee relations
- Crisis teams prioritize rapid action

Without convergence, these priorities will conflict, creating paralysis at the exact moment decisive leadership and management is required.

Converged Security Defined

Converged Security is the strategic integration of security disciplines into a unified framework, enabling organizations to prevent, detect, and respond to threats holistically. It is not merely organizational restructuring—it is a transformation across:

- Governance
- Technology
- Operations
- Culture

Core Principles of Converged Security

- **Unified Risk View** - A single, enterprise-wide understanding of threats and vulnerabilities
- **Integrated Operations** - Cross-functional teams operating within shared processes and systems in the form of a Global Security Operations Center (GSOC)
- **Shared Intelligence** - Data from all domains aggregated, analyzed, and actioned collectively
- **Coordinated Response** - Emergency and Crisis Management Response executed as a single, synchronized effort
- **Leadership Alignment** - Executive ownership of security as a strategic business function.

Drivers of Convergence

- **Digital Transformation** - Cloud computing, IoT, and remote work have blurred the line between physical and digital environments
- **Insider Threat Evolution** - Employees, contractors, and partners now represent one of the most significant risk vectors.
- **Hybrid Threat Actors** - Nation-states and sophisticated criminal groups deliberately exploit cross-domain vulnerabilities
- **Regulatory and Compliance Pressure** - Frameworks increasingly require integrated risk management approaches rather than isolated controls
- **Speed of Crisis Escalation** - Incidents now escalate in minutes, not days—demanding synchronized response capabilities

Real-World Convergence Scenarios

Scenario 1: Credential Compromise → Physical Breach → Data Exfiltration

- Phishing attack compromises employee credentials
- Attacker gains badge access to facility
- Rogue device installed on internal network
- Sensitive data exfiltrated

Failure Point:
Lack of integration between IT alerts and physical access anomalies.

Scenario 2: Disgruntled Insider → Operational Disruption

- Behavioral red flags identified by HR
- Elevated system access remains unchanged

- Individual sabotages systems before termination

Failure Point:
Personnel risk not integrated into access control decisions.

Scenario 3: Cyberattack Triggering Physical Crisis

- Ransomware disables building management systems
- HVAC, access control, and safety systems impacted
- Evacuation required under uncertain conditions

Failure Point:
Cyber incident not integrated into crisis management planning.

The Role of Leadership in Convergence

Converged security requires executive-level sponsorship and cannot be delegated or implemented solely at the operational level.

Key Leadership Responsibilities

- Establish enterprise-wide security governance
- Break down organizational silos and establish or out-source a GSOC
- Align security with business continuity and resilience
- Invest in integrated technologies and platforms
- Foster a culture of shared accountability

Organizations who are leading in this space appoint roles such as:

- Chief Security Officer (CSO)
- Chief Risk Officer (CRO)

Establishing these roles unifies monitoring and oversight across all security domains and enables more effective and timely decision-making.

Technology as an Enabler Not the Solution

It cannot be disputed that technology plays a critical role in all security functions however, but, it must serve to inform and support, not replace strategy.

Key Capabilities

- Integrated (Global) Security Operations Centers (GSOCs)
- Unified data platforms (SIEM/SOAR)
- Identity and access management across physical and digital systems
- AI-enhanced analytics for cross-domain threat detection

Building a Converged Security Model

Phase 1: Assessment

- Map existing security functions
- Identify gaps and overlaps
- Evaluate cross-domain dependencies

Phase 2: Governance Alignment

- Establish unified leadership structure
- Define roles, responsibilities, and decision authority

Phase 3: Operational Integration

- Develop shared workflows
- Implement joint incident response protocols
- Conduct cross-functional training

Phase 4: Technology Integration

- Consolidate data streams
- Deploy unified monitoring and response platforms

Phase 5: Cultural Transformation

- Promote collaboration across disciplines
- Embed security into organizational DNA
- Shift mindset (greatest challenge) from “ownership” to “shared mission”

The Role of Training and Professional Development

A critical barrier to convergence is the lack of cross-domain expertise. Traditional training produces:

- Cyber specialists with limited physical security understanding
- Physical security professionals with limited cyber awareness
- Crisis managers disconnected from technical threat vectors

The workforce, both current and future requires practitioners to be well-versed in the following:

- Multi-domain awareness
- Leadership capability in complex incidents
- Decision-making under uncertainty
- Integration of cyber and physical response strategies

This is where specialized professional development programs in Converged Security become essential as they serve to bridge the gap between theory and operational reality.

Conclusion

The threat landscape has outpaced traditional security models. The artificial boundaries between Personnel, Physical, Information Security, and Emergency and Crisis Management response no longer exist in practice and only in outdated organizational charts.

Organizations that fail to adapt will face:

- Increased risk exposure
- Slower response times
- Greater operational and reputational damage

Those that embrace convergence will achieve:

- Enhanced resilience
- Faster, coordinated response
- Strategic advantage in an increasingly uncertain world

Converged Security is not the future but the present requirement for any organization serious about protecting its people, assets, and mission.

Author's Note

This white paper reflects the perspective of a practitioner operating at the intersection of cybersecurity, physical security, and emergency and crisis leadership, with experience spanning high-risk operational environments and enterprise security strategy. The concept of converged security is grounded not only in theory, but in the realities of modern threat environments where failure to integrate disciplines has real-world consequences.