2022 CHEMICAL SECURITY SUMMIT

August 23-25, 2022

#ChemicalSecurity

Is There a Need to Blend Cyber and Physical Security Resources? If so, Why and How?

DHS / CISA

CHEMICAL SECURITY SUMMIT

AUGUST 2022

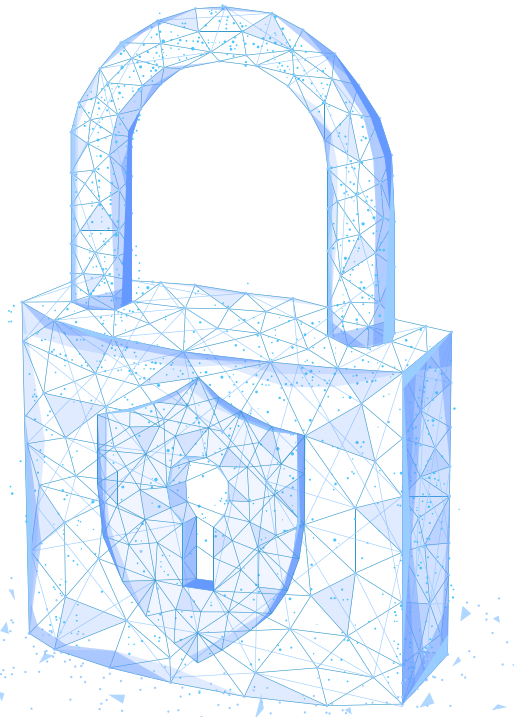
Institute for Homeland Security
SAM HOUSTON STATE UNIVERSITY

Is There a Business Case for Blending The Cyber and Physical Security Functions?

IT DEPENDS…

WHAT'S YOUR ORGANIZATION'S TOLERANCE FOR RISK?

The Problem



- Originally physical and cyber security were separate departments, with different cultures and ways of thinking.
- Physical security had strong forensic investigation, interviewing, behavioral risk analysis, asset protection and risk/threat assessment capabilities.
- Cyber security had cyber intelligence, IT security systems design and engineering skills, hardware & software vulnerability assessment, digital investigations, evidence collection, and analysis capabilities.
- Today, physical security relies upon IT tools for identity management, intrusion detection, data analysis, incident management, etc., and similarly, cyber security is dependent upon the human and physical dimensions of protecting physical data space and hardware systems including IOT and SCADA.
- ***Collaboration and seamless communication is essential for an effective integrated security management function!***

Is there a Solution that Makes both Operational Security & Business Sense?

- As cyber-physical threats become more pervasive, complex and potentially materially impactful, it is essential to have a clear view of the integrated risk environment, combined with a coordinated process for deterring, neutralizing and managing 21st century threats.

- To that end the U.S. Cybersecurity and Infrastructure Security Agency (CISA), recommends critical infrastructure organizations implement a “blended approach to cyber and physical security” to obtain the focused organizational and leadership capabilities required for today’s risks and threats.

The Benefits of Blending Security Functions are Clear!

There are many benefits to having cyber and physical security teams work in close partnership:

- A stronger, more holistic view of security risk, threats and operations
- Better alignment, integration and accountability for achieving corporate objectives
- Faster identification, assessment and response to threats that fall within both the cyber and physical domains
- Better communication with critical infrastructure senior leadership
- Real time sharing of analyzed threat information, technology solutions, and awareness knowledge transfer for avoiding / responding to security risk and threats
- Improved containment of escalating operating costs for security management systems

Blending Cyber and Physical Security Functions Has Been A Discussion Topic for 20 Years!

The debate about whether there's an operational need to blend corporate Cyber and Physical Security has been occurring with greater frequency since the attacks of September 11th.

According to an ASIS survey in 2020, 76% of the >1000 corporate CISO's and CSO's surveyed believe blending the cyber and physical security functions will strengthen and improve the performance of security management, and 83% believe a single security leader will increase the effectiveness and status of the security function.

However, only 24% of the respondents have implemented steps to achieve that outcome, with nearly 2/3 of the 24% being European or Indian multi-national corporations.

WHY No Follow-up Action???

People Issues Drive the Resistance to Change

Confusion about roles, responsibilities and communication

Fear as to loss of prestige and status (including budget loss) as a result of a merger

A belief that cyber security is a higher priority to the company and therefore the physical security personnel will lose the ability to influence senior leadership

Resistance to change - “If it ain’t broke, don’t fix it” syndrome – A strong belief that having a separate structure for each security function that comes together when needed is a more efficient use of resources given that cyber security is focused upon technical risks, whereas physical security is concerned with behavioral risks

Concerns about job security particularly within the cyber-security function as their function generally has a much larger staff than physical security. Who will be the leader of the blended security organization, CISO or CSO?

CEO of a major energy company allegedly noted: “Security Is Security; Why not work together?”

The Colonial Pipeline, Florida Water Authority incident and other high impact events is leading C-Suite Executives and Boards to ask if a single integrated view of security risk would be a more effective means of protecting a company

Having segmented, stove-piped operations is less likely to have an accurate, timely view of all security risk impacting the company, just as the amount of digital access points throughout the company (and within physical security systems) is increasing as noted above

Two separate security functions often results in duplication of resources and personnel, SOC’s for example, which adds unnecessary operating costs

Efficiencies can be improved by replacing the ever-increasing operating costs associated with manned security services using IT based technologies operating in a centralized remote model

Digital Technology is Inserting Itself into Core Security Management

Cyber & Physical Security are becoming more integrated and dependent upon one another, not less!

“Security drones” with on-board data analytics to assess changes in “normal” behaviors are being employed for perimeter surveillance, reconnaissance, incident response, and emergency management support for firefighting, and loss of containment events

Ground based “security robots” also with on-board data analytics are being utilized at perimeter access points to inspect cars, trucks and rail cars for unauthorized materials

“Automated security receptionists” provide access control and security concierge services to visitors, package delivery personnel and employees needing site specific security & safety training for chemical manufacturing, distribution, and headquarters facilities

IT enabled services are expanding as operating costs for manned physical security services escalate

Cyber – Physical Threat Case Study

”Cyberthreats” that infect the IT network through a physical device often sent by mail (known as a physigal threat) pose new risks that require a joint response by cyber and physical security

Phygital threats include “warshipping,” a Trojan horse strategy that involves physical devices that hack into digital infrastructure

Warshipping devices range from USB drives, to WiFi network adapters, to mini-computers (i.e. Rasberry Pi). Once on site, the devices can log into local Wi-Fi networks to install malware or access sensitive data

A 2021 FBI warning noted USB devices with malicious code disguised as important information were being mailed to unsuspecting corporate employees who plugged the devices in, and unwittingly granted unauthorized access to critical information systems

Many packages sit in mailrooms or on desks for weeks—especially in companies with remote work policies – and these phygital devices are within easy reach of servers and other critical digital infrastructure

So, what’s the best way to protect againstphygital threats? Implement integrated responses that combine physical and cyber security

Blending Cyber and Physical Security is a Compelling Value-Added Decision

Physical and cyber security convergence has already started at the operational level

The next step to improving effectiveness and the ability to rapidly respond to the multi-dimensional fast paced risks and threats of the 21st century is to create an integrated organization and leadership structure

The integrated structure needs to create results-oriented dynamic cooperation between the cyber and physical security functions so they can quantifiably improve protective performance and contribute to the critical infrastructure organizations goals and objectives

The blended security function will improve security management capabilities and efficiencies and thereby create a more safe and secure environment for employees, customers, suppliers etc.

Increased investment and commitment to integrated security management will provide HR with a means of **differentiation when recruiting and retaining new members** of the critical infrastructure workforce – **a positive benefit to a security program!**

Optimal Organizational Strategies for Critical Infrastructure Security Function

"Fully Blended Cyber and Physical Security Function"- Both functions contained within one organization led by a single senior security executive who is the principal point of contact for all security issues with the organization

"Partially Blended Cyber and Physical Security Function" – Each function maintains separate functional identity and general area of responsibility which is led by a senior security executive, however the functions report into the same organizational structure (i.e. Legal, CFO, CRO, etc.) with the head of the Cyber and Physical security functions reporting to the same senior leader (GC, CFO, CRO, etc.)

"Formal Functional Collaboration" – Each function maintains a separate functional identity and is led by a senior security executive, but they report into different company functions. To enhance communication and cooperation there is a process wherein cyber and physical security leadership regularly meet to review, discuss and cooperate in achieving company objectives relating to security, emerging physical and cyber risk and threat issues, and the status of joint projects / investigations.

"Separate Independent Operations" – Physical and Cyber Security maintain their separate identity and functional responsibilities; they report into different company functions. They only interact with one another when required to do so due to an incident clearly impacting both functions.

“Fully Blended” Cyber and Physical Security Function

POSITIVES:

- Enhanced impact of functional leader with CEO/LT/Board – Single leadership voice, vision & focus;
- Reduced duplication of effort and lower annual operating costs; increased synergies and capabilities to assume new risk related roles
- Better alignment of security management with corporate goals; Improved communication & engagement throughout the organization
- Improved identification and exploitation of IT Technology for Security Management
- Enhanced career mobility opportunities for staff; Reduce confusion as to roles and responsibilities
- More effective, rapid analysis of converging security threats, plus clear, streamlined communication channels
- Create a competitive advantage by improving security’s ability to exceed customer expectations

NEGATIVES:

- Cultural Differences between functions; Perception that functional responsibilities are too different (i.e. technical vs behavioral)
- Fear of Change; “Turf” battles; Uncertainty as to Who will lead the new organization, CSO or CISO and whether there will be a loss of status
- Perceived lack of support by senior leadership; Budgetary reduction concerns; Dilution of focus during the transition increases risk to Org.

“Partially Blended” Cyber and Physical Security Function

POSITIVES:

- Overall single leadership voice & vision but not from the “top” security professional
- Reduced duplication of effort and lower annual operating costs, better synergies
- Better alignment of security management with corporate goals; Improved communication throughout the organization
- Better exploitation of IT Technology for Security Management; Improved, not enhanced career mobility opportunities
- More effective, rapid analysis of converging security threats, plus clear, streamlined communication channels

NEGATIVES:

- Fear of Change, Turf battles, Cultural differences
- Change in organizational reporting structure will diminish status, access to CEO, and budgets
- Concern roles and responsibilities are too different to work together (technical vs behavioral risks)

Positives & Negatives for Other Strategies!

Formal Functional Collaboration:

A reasonable strategy to address emerging risks and opportunities that are predictable, but don't require in-depth knowledge of how each security function operates when supporting critical infrastructure operations.

The strategy is ***dependent upon personalities and the ability of individuals throughout the organization to develop sustained relationships*** with colleagues that are effective and reliable.

Changes in leadership (retirement, resignations, etc.) means starting anew in creating a process and procedure for effective collaboration.

Separate Independent Operations:

Good strategy for maintaining the ***status quo of security management*** performance, but will not be able to effectively identify and manage the ever-increasing convergence of complex cyber and physical risk / threats to critical infrastructure which will increase risk to critical infrastructure.

Ensures security management opportunities to increase the utilization of security technologies, plus, staff career enhancement and alignment with achieving corporate / organizational objectives are ***limited and inefficient*** in execution.

Operational Efficiency, Cost Avoidance, Improved Communication / Leadership & Employee Development Benefits are Compelling

As CISA noted, the time has arrived for consolidating critical infrastructure security resources to optimize their effectiveness in a world of digital risk

This is particularly true for organizations seeking to protect themselves from physical and cyber threats which have become increasingly intertwined, complex, and rapidly evolving

The question is: which of the 4 strategies for blending cyber and physical security will work best for your company culture and risk environment?

The **Fully Blended** model is the most effective and impactful means to enhance security management within a critical infrastructure organization, and it is the recommended model.

However, the **Partial Blend Model** has most the benefits of the Fully Blended model, but, also has less of the negative obstacles to implementation, and therefore is an attractive alternative that provides critical infrastructure with enhanced security management capabilities and less brand / reputation risk for less negatives.

In the Meantime: One Last Point of Execution: (Human Nature Being What It Is!)

The Fully Blended Option has the largest, most sustainable positive impact upon effective security risk management and **is recommended**

But, it's also the strategy most resisted by employees, particularly those assigned to the Physical Security function

If the Fully Blended Option is chosen, then a change management and communications strategy in partnership with HR will be needed to describe the quantifiable benefits of the Fully Blended Option, particularly those related to upward career opportunities for Physical Security staff who tend to be the most vocal about resisting change.

Communicating a positive, personal career benefit will make it easier to motivate and incentivize employees to embrace the strategy.

Knowledge Test (True or False)

1. There is uniform opposition by executives to blending cyber and physical security functions within critical infrastructure organizations.
2. A significant reason for opposing the blending of cyber and physical security within critical infrastructure is because there is no security management or business operations benefit to doing so.
3. There is no meaningful cyber-security connection or overlap to the responsibilities of physical security.
4. The “Formal Functional Collaboration” strategy for blending cyber and physical security is dependent upon personalities and personal relationships to be an effective contributor to protecting critical infrastructure.
5. The Colonial Pipeline, Florida Water Authority incident, as well as other recent events is causing Executives and Boards to ask if a single view of security risk is a more effective means of protecting a company.
6. Blending the cyber and physical security functions has a career mobility benefit AND is a source of safe space differentiation for HR when recruiting and retaining new members of the critical infrastructure workforce.