ASIS FOUNDATION

Sponsored by ALERT ENTERPRISE
PHYSICAL | LOGICAL SECURITY CONVERGENCE

# The State of SECURITY CONVERGENCE in the United States, Europe, and India

## Executive Summary

***In early 2019,*** the ASIS Foundation launched a study to investigate the extent to which organizations in the United States, Europe, and India have converged any two or all three of the following security functions: physical security, cybersecurity, and business continuity management (BCM). More than 1,000 professionals with senior roles in physical security, cybersecurity, disaster management, business continuity, and related fields responded to the survey.

The results? Despite years of predictions about the inevitability of security convergence, just 24 percent of respondents have converged their physical and cybersecurity functions. When business continuity is included, a total of 52 percent have converged two or all of the three functions. Of the 48 percent who have not converged at all, 70 percent have no current plans to converge.

However, there seems to be a growing need for greater communication and collaboration. Fully two-thirds of organizations reported that their physical security, cybersecurity, and/or business continuity departments or functions are working closely together either through convergence, partial integration, or collaboration.

Data and follow-up interviews show that companies are organizing their security and BCM functions in a variety of different ways depending upon business needs. Our survey and interview results indicate that multiple models—complete convergence among them—can be effective.

## KEY FINDINGS

**1. Strong leadership and a clear security strategy emerged as important factors for effective security regardless of how the functions are organized.**

Most organizations surveyed (67 percent of converged and 57 percent of non-converged) report having an enterprise-level security leader. Of those, 79 percent agree that having an enterprise security leader "enhances the effectiveness of corporate security." The most successful security operations share the following characteristics:

a. Physical security, cybersecurity, and BCM functions are aligned around one security strategy.
b. The functions maintain open communication and share information with one another.
c. Security has a voice in the C-suite and senior leaders provide strong leadership and engagement for the functions.

*"It doesn't matter what model an organization selects for security. It will not work unless you have strong leadership and engagement at the very senior level."*

**–Vice President for Global Security at an international energy firm**

### 2. Business continuity management is more likely to be converged than physical and cybersecurity.

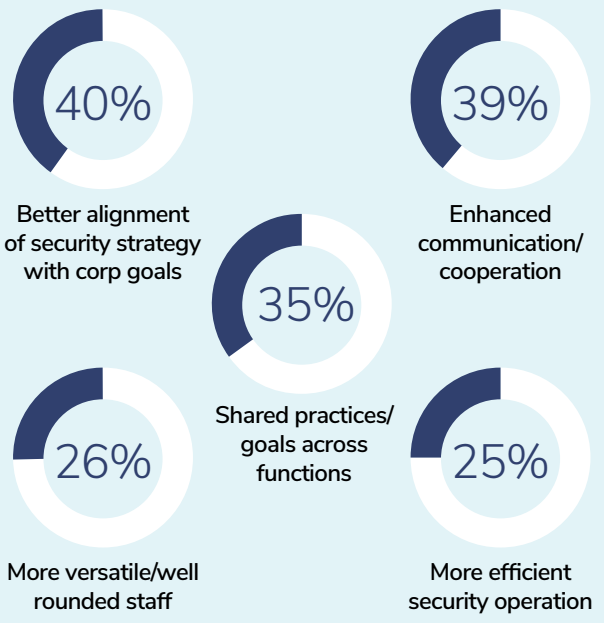
Companies report that BCM is converged with either cyber or physical security in nearly half (47 percent) the organizations surveyed, compared to just 24 percent with converged physical and cybersecurity functions. In addition, 71 percent of BC managers surveyed felt that converging functions would somewhat or greatly strengthen BCM. Only 16 percent felt convergence might weaken the function.

### 3. Security convergence produces tangible positive benefits.

96 percent of organizations that converged two or more functions (physical, cyber, and/or BCM) report positive results from the combination, and 72 percent believe that convergence strengthens overall security. In addition, 44 percent of converged organizations report no negative results from converging. Even in companies that have not converged, 78 percent believe that convergence would strengthen their overall security function.

## TOP 5 BENEFITS OF CONVERGENCE

As reported by organizations that have converged




## DEFINITION OF CONVERGENCE

For survey participants, convergence was defined as getting security/risk management functions to work together seamlessly, closing the gaps and vulnerabilities that exist in the space between functions. Fully converged functions are generally unified and interconnected, reporting to one security leader. They often have shared practices and processes, as well as shared responsibility for security strategy. Converged functions work together to provide an integrated enterprise defense.

### 4. Saving money is not the primary motivation for convergence.

Just 7 percent of those who had converged cited "reduction in security costs" as a primary benefit of convergence. Notably, 20 percent of those not converged cited "potential cost savings" as a factor that might convince them to converge their security functions. For individual functions, 58 percent of non-converged organizations report that cybersecurity budgets are increasing versus just 49 percent for converged organizations. Physical security budgets are also more likely to be increasing in non-converged organizations (28 percent) compared to 24 percent in converged organizations. On the other hand, BCM is seeing a budget increase in 26 percent of converged organizations compared to just 19 percent of non-converged organizations.

### 5. A key driver and benefit of convergence is the desire to better align security strategy with corporate goals.

When asked "which of the following factors might convince you to converge?", the number one answer cited by 38 percent of those who had not yet converged was "better alignment of security/risk management strategy with corporate goals." This was also considered the most positive benefit by 40 percent of the respondents that already converged two or more functions.

**6. The differences in culture and skillset between physical and cybersecurity present the greatest hurdle to convergence.**

The most frequent challenges cited in companies that converged were "different cultures and skillsets" (36 percent), "turf and silo operating tradition" (24 percent), and the "belief that cyber security requires its own operation" (21 percent). Notably, more than one-fifth of all respondents (22 percent) reported no challenges in converging departments.

**7. Finding the right talent to lead a converged security department can be challenging. Physical and cybersecurity require different education and experience.**

According to a vice president at a U.S. technology company, "there is no single skill set for all. The industry has not evolved where we can now have a single security practitioner who can do physical security, digital transformation, and product management. Until the industry evolves towards that, we will operate with three independent roles." Some organizations report success finding individuals from a military security background who have experience and knowledge in both physical and cybersecurity.

*"The main barriers to convergence were turf and silo issues. Everyone wanted to safeguard his responsibilities, his people, his budget, his prestige, and his importance to the company."*

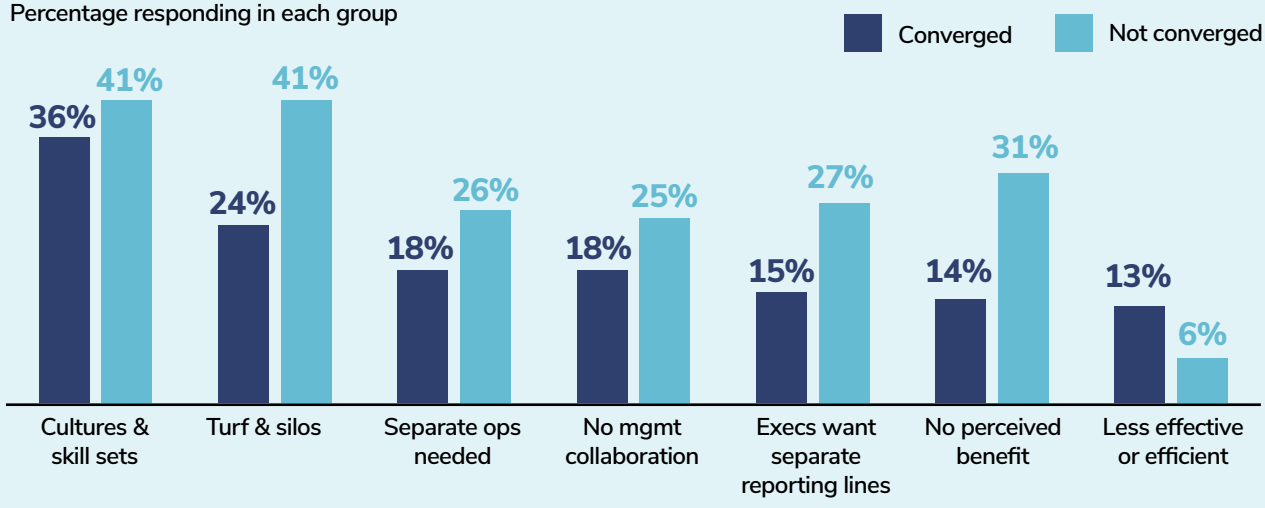
**–Vice President of Group Security for a European telecommunications company**

**8. Convergence or integration needs to be customized to fit the needs of the business and its culture.**

For example, safety is a major concern in the chemicals industry. One chemical industry security leader explained that physical security and fire safety are often converged, but it did not make sense to converge them with cybersecurity. A major U.S. e-commerce company executive explained that "cyber is very important and so it is kept separate from all other sectors." In the case of many airports and hospitals, cybersecurity is run as a shared service across the enterprise while physical security is run by staff at each location. For those industries, cybersecurity is centralized while physical security is decentralized.

## BOTH CONVERGED AND NONCONVERGED ORGANIZATIONS IDENTIFY MANY OF THE SAME CHALLENGES

Percentage responding in each group



## SURVEY METHODOLOGY

The ASIS Foundation surveyed approximately 8,000 senior-level professionals from the United States, Europe, and India in physical security, cybersecurity, business continuity, and related fields. The survey was fielded online in April and May 2019. We received 1,018 full and partial responses and of those, 555 completed the entire survey. Samples were drawn from the ASIS member database, including almost all members of the CSO Center for Leadership and Development. In addition, to obtain a broader sample, we partnered with outside groups to survey additional cybersecurity and business continuity professionals, as well as security professionals in Europe and India. To add context, 21 telephone interviews were conducted with respondents from a cross-section of geographical regions, security functions, and industries.

**The full research report is available online at *www.asisfoundation.org*.**

## ASIS FOUNDATION RESEARCH PROJECT TEAM

This project was led by ASIS Foundation Research Committee members Dana Adams, CPP; Brian Allen, CPP; Lee Cloney, CPP; Linda Florence, CPP; Martin Gill, Ph.D.; and Committee Chair Ben Suurd, CPP. Survey and analysis were conducted by researcher David Beck; ASIS Chief Global Knowledge Officer Michael Gips, CPP; and ASIS Foundation Director Beth McFarland Pierce.

We wish to acknowledge and thank the following individuals and organizations for their help in raising awareness of this survey among their members and contacts. This led to broader survey participation and more robust data collection.

- Manish Datta and Garry Singh for assistance in India.
- Chloe Demrovsky and Buffy Rojas of DRI International for outreach to their members.
- Marc Thompson of ISSA and Jeff Snyder for promoting the survey to Chief Information Security Officers.

## ABOUT THE ASIS FOUNDATION

The ASIS Foundation, a 501(c)(3) nonprofit affiliate of ASIS International, supports global security professionals worldwide through research and education. The Foundation commissions actionable research to advance the security profession and awards scholarships to help chapters and individuals--including those transitioning to careers in security management--achieve their professional and academic goals. Governed by a Board of Trustees, the Foundation is supported by generous donations from individuals, organizations, and ASIS chapters and councils worldwide. To learn more, visit *www.asisfoundation.org*.

## FROM OUR SPONSOR

In today's threat landscape, operating with siloed physical security, IT and cyber systems puts your enterprise at greater risk. Cyber and physical threats are now blended, requiring a converged approach that fully integrates and automates security with operations and compliance. At AlertEnterprise we bring people, processes, data and technology together in a way which increases daily intelligence and reduces risk. That's what we call security convergence and it's our daily mission. With our trusted identity and access management platform, enterprises can do more with less, create engaging workforce experiences, increase compliance and mitigate threats and risk. For more information, visit *www.alertenterprise.com*.