ASIS FOUNDATION™

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

Sponsored by

ALERT ENTERPRISE

PHYSICAL | LOGICAL SECURITY CONVERGENCE

Principal Researcher and Author:
David Beck, managing director, David Beck Associates

Contributing Researchers and Authors:
Michael Gips, CPP, CAE; Beth McFarland Pierce, CAE

ASIS Foundation Research Committee:
Dana Adams, CPP; Brian Allen, CPP; Lee Cloney, CPP;
Linda Florence, CPP; Martin Gill; Ben Suurd, CPP (chair)

Table of Contents

Introduction . . . 3

Part I: Summary of Key Results . . . 6

Part II: Behind the Decision to Converge . . . 11

Part III: The Impact of Convergence . . . 13

Part IV Adoption of Convergence is Gradual . . . 17

Part V: Nonconverged Organizations . . . 19

Part VI: Staking a Middle Ground . . . 23

Part VII: Who Oversees Security at Converged Organizations? . . . 25

Part VIII: Where Business Continuity Fits . . . 28

Part IX: Costs and Budgets . . . 30

Part X: Outlook: Challenges and Opportunities . . . 33

Conclusion . . . 34

ASIS International
1625 Prince Street
Alexandria, Virginia, USA 22314

Price: $195; complimentary for ASIS members.

Introduction

Traditionally, companies have managed physical and cybersecurity threats separately, primarily because the personnel and equipment necessary for prevention and response require distinct technology, talents, and capabilities. Business continuity functions have either resided separately or have been embedded where it seemed most logical: physical business continuity/disaster management within physical security and cyber business continuity/disaster management within cybersecurity.

Over the past 10 to 20 years, companies have explored—and some have even implemented—a holistic approach to security by blending physical, cyber, and business continuity (and sometimes other functions) together in a manner dubbed convergence. (This blending went beyond shared networks to include management, operations, processes, and other organizational factors. By contrast, many companies have long had "integrated" security—meaning physical and cyber components that share technical systems and/or run over the same network.) Other organizations are contemplating such a change, while many others are resistant. A few once-converged companies have even de-converged as part of organizational structural overhauls.

One chief security officer of an international energy company interviewed for this study said he had converged information and physical security 10 years ago. But that effort was in name only. In reality, cyber and physical security had continued to operate mostly independently until just a few months before the study, when a new CISO joined the company and began to merge the functions to make true convergence a reality.

Convergence has intrigued security professionals and business executives for three main reasons. First, the world of physical security has become very much IP-enabled. The number of devices such as cameras, card readers, smart cards, and sensors that are IP-capable is mushrooming daily. Physical and IT systems are coming together as part of a natural evolution.

Second, the ability to mitigate risks and respond to incidents resides in both the physical and the cyber functions. It makes sense to manage threats via a joint and collaborative response.

Third, senior management closely monitors costs and efficiency. Overlap of functions, to many executives, means duplication, waste, and needless expense. Because many security functions overlap, top management may come around to the view that "security is security," and bringing everything together as part of a formal plan seems logical.

Convergence doesn't encompass only cyber and physical security. Security professionals and business executives increasingly realize that business continuity is a critical part of the equation. Long associated with physical disruptions or natural disasters such as terrorism, sabotage, fires, floods, and storms, business continuity management gained a cyber component with the advent of the digital age. But often these two business continuity components remain separate: physical security, supply chain, and facilities personnel handle physical attacks, while specialized IT teams focus on digital disruptions, such as inoperable systems or malicious hacker attacks.

Convergence doesn't encompass only cyber and physical security. Security professionals and business executives increasingly realize that business continuity is a critical part of the equation.

CONVERGENCE DEFINED

Convergence is defined here as security/risk management functions working together seamlessly to address security holistically and to close the gaps and vulnerabilities that exist in the spaces between functions. Fully converged security programs 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.

For the purposes of this report, a "converged" organization has converged at least two or all three of the following functions: physical security, cybersecurity, and business continuity. A "nonconverged" organization has not combined any of the three functions.

Experts question whether this division of responsibility makes sense in an era where so much business has migrated online, e-commerce has come to the fore, and physical and cyber risks and consequences are so intertwined. There is a growing sense that emergency and crisis management as well as planning and disaster recovery must be integral to a convergence strategy.

Consider the hypothetical case of a mining company that deploys massive self-driving trucks and trains as well as autonomous drilling technology, all part of the Internet of Things. Under a siloed security model, the type of threat or attack would dictate who would respond, even if the consequences were identical. Sabotage to, theft of, or an attack on the equipment would yield a response by the physical security team. An explosion caused by either a natural disaster or a manmade attack would call the disaster management experts into play. A breach resulting in remote takeover of trucks, trains, or drills would invoke the cybersecurity team, and likely the cyber business continuity group as well. Similar consequences, different personnel.

Given this situation, convergence seems to be the logical course for most security departments. But while the industry may be inching in that direction, many organizations are hesitant to take the plunge.

Organizations are often slow to adapt to change unless forced to do so. Reluctance to converge often centers around people issues. Physical security personnel are fixed in traditional silo structures where their distinctive competencies include people management, investigations, and intelligence. They and their managers are hesitant to relinquish these roles.

Cybersecurity personnel have their own distinct culture built around the latest technology, cyberthreats, and system innovations. They have granular knowledge of cyberattack vectors, hardware and software, technical jargon, and computer tools.

Convergence, some fear, could mean that either cyber or physical is subjugated to the other, with loss of status, authority, and staffing. With the prospect of such an impasse, both functions are satisfied to wait until the command to converge comes from the top—which may never happen.

Security professionals who advocate for convergence have had mixed results in their efforts to communicate to the C-suite why convergence is essential and timely.

At least that is how the security landscape appears at first glance. To learn more about the true state of security convergence, the ASIS Foundation commissioned an in-depth study. This research explores the following questions:

1. To what degree are organizations converging cybersecurity, physical security, and business continuity?
2. What are the (a) drivers leading to convergence and (b) the obstacles hindering convergence?
3. What have been the results of convergence, and how do they compare to organizations that remain siloed?
4. Are there any differences in the extent and results of convergence with respect to:
   a. Geography (United States, Europe, India)?
   b. Size of organization?
   c. Industry vertical?
   d. Role of the survey respondent (physical security, cybersecurity, business continuity—physical, cyber, or both)?

The results represent a snapshot of the state of security convergence in 2019. With little existing research on convergence, there is not much data

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. The survey drew 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, the ASIS Foundation partnered with outside groups to survey additional cybersecurity and business continuity professionals, as well as security professionals in Europe and India. About two dozen in-person and telephone interviews were conducted with respondents from a cross-section of geographical regions, security functions, and industries to provide additional context to the results.

to compare to, so this study does not explore the prevalence of convergence over time. But the information presented here can serve as a benchmark for continuing research to track this issue going forward.

Beyond the hard data, this report provides a narrative to help converged firms maximize the benefits. What's more, it can serve as a roadmap for organizations that have not yet converged. Telephone interviews conducted as part of this research provide anecdotal case studies from a range of business types, sizes, and geographies, everywhere along the spectrum from completely siloed to thoroughly converged.

The combination of hard data and the insightful voices of senior security directors creates a powerful array of best practices that can help guide security decision making.

Part I: Summary of Key Results

Full convergence of cybersecurity, physical security, and business continuity is still rare at just 19% of those surveyed. Yet just more than half of respondents (52%) say they have some sort of convergence. Physical and cyber alone are converged in only 5% of companies, so combined with the organizations that have converged all three functions, a total of 24% of firms have converged physical security and cybersecurity in a single department.

EXTENT OF CONVERGENCE

19% have converged cybersecurity, physical security, and business continuity

5% have converged cybersecurity and physical security only

7% have converged cybersecurity and business continuity only

21% have converged physical security and business continuity only

48% have not converged cybersecurity, physical security, or business continuity

Although the security functions in many organizations are not fully converged, the various functions do find other ways to work together. In fact, more than half (55%) of nonconverged firms report some level of coordination and integration among security operations.

NONCONVERGENCE RELATIONSHIPS

32% Cybersecurity, physical security, and business continuity collaborate or are partially integrated.

23% Two of the three functions (cybersecurity, physical security, and business continuity) collaborate or are partially integrated.

45% Cybersecurity, physical security, and business continuity operate independently.

While the overall rate of full convergence is 19%, and 52% have converged at least two of the three functions, there is some variability by industry. Based on this study, the utilities industry is much more likely to be fully converged, while retail and healthcare organizations are less likely to converge.

CONVERGENCE BY INDUSTRY

Industry	Fully Converged	2 Functions Converged	Not Converged
Utilities	30%	40%	30%
Technology & Software	19%	42%	39%
Hospitality/ Leisure	19%	38%	43%
Financial Services	19%	29%	52%
Industrial & Manufacturing	14%	32%	54%
Retail	11%	43%	46%
Healthcare	11%	23%	66%

Smaller firms tend to converge in greater numbers due to economic necessity and the "everyone is responsible for everything" nature of startups and small companies. A clear trend toward convergence will be evident when more large firms fully converge.

ANNUAL REVENUE (USD)

	Fully Converged	2 Functions Converged	Not Converged
Less than $25 million	31%	30%	39%
$25 million to $100 million	25%	35%	40%
$101 million to $500 million	24%	23%	53%
$501 million to $1 billion	13%	44%	43%
$1 billion to $10 billion	13%	37%	50%
More than $10 billion	16%	29%	55%

In this study, Europe and India show higher rates of convergence than the United States.

FULL CONVERGENCE BY REGION

23%	Europe
23%	India
16%	USA

Substantial percentages of both converged and nonconverged organizations believe convergence strengthens security.

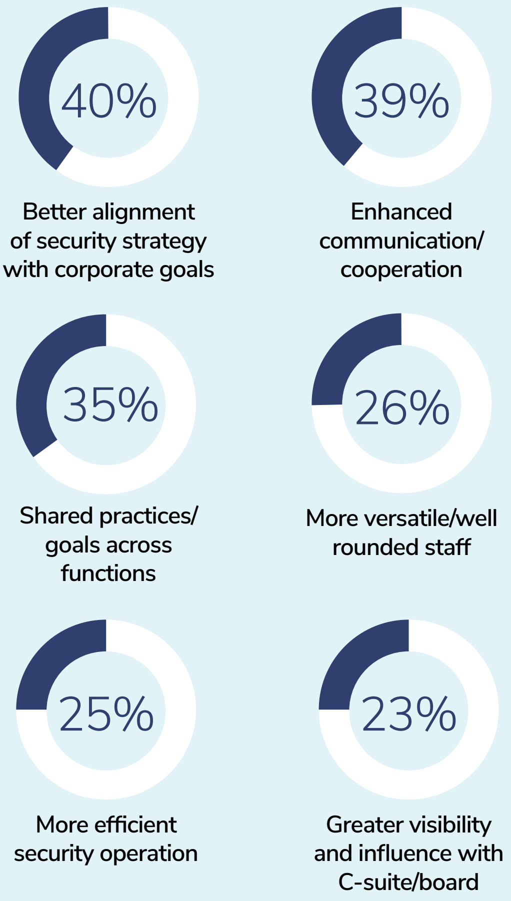
THE EFFECT OF CONVERGENCE ON SECURITY

	Strengthen	Weaken	No Change
Converged	76%	3%	14%
Nonconverged	78%	7%	12%

Respondents in converged organizations report a wide variety of benefits from convergence.

TOP 6 BENEFITS OF CONVERGENCE

As reported by organizations that have converged



*Total does not equal 100% because respondents could select multiple answers.

For converged companies, almost half report no drawbacks.

DRAWBACKS OF CONVERGENCE

44%	No negative results
29%	Confusion over roles and responsibilities
25%	Confusion over lines of reporting/ communication
25%	Conflict, other personnel issues among converged staff

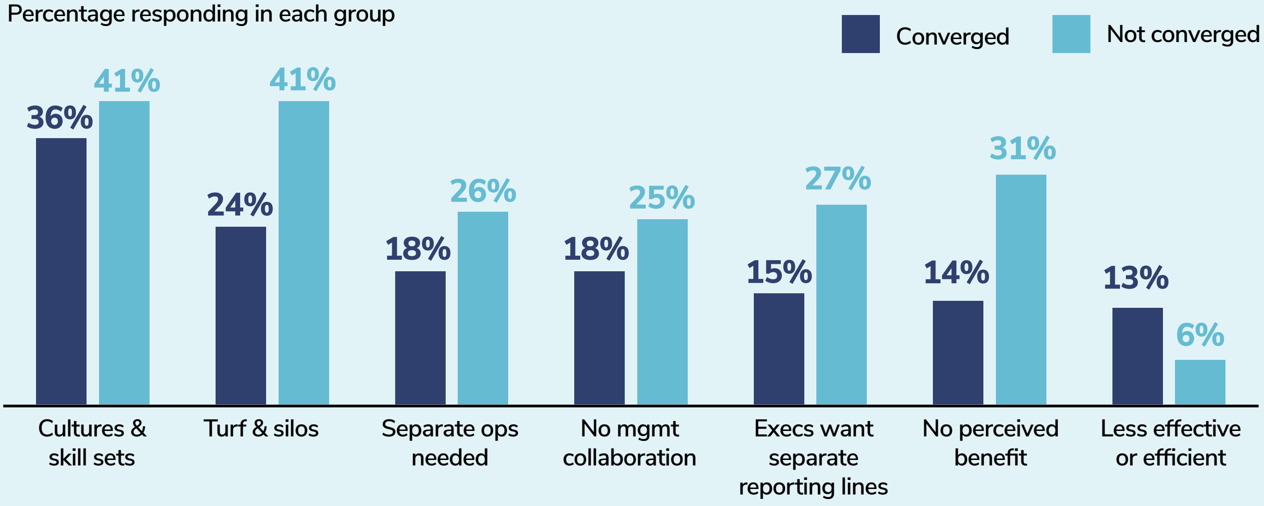
Reasons for converging security functions deal with business and process improvements and cost savings.

FACTORS LEADING TO CONVERGENCE

38%	Better alignment of security/risk management strategy with corporate goals
28%	Advances in technology integration/ security operations centers
27%	Greater efficiency in security and/or business continuity operations
21%	Clear cost savings

Difficulties in merging cyber, physical, and/or business continuity functions often center around personnel issues. The actual challenges experienced by converged organizations are very similar to the challenges anticipated by nonconverged firms.

BOTH CONVERGED AND NONCONVERGED ORGANIZATIONS IDENTIFY MANY OF THE SAME CHALLENGES



*Total does not equal 100% because respondents could select multiple answers

Most nonconverged firms have no plans to converge in the near term despite the benefits cited by many of the respondents from converged organizations.

WHEN NONCONVERGED COMPANIES PLAN TO CONVERGE

5%	Within next 12 months
10%	Within next 24 months
5%	Within next 36 months
10%	Beyond 36 months
69%	No current plans to converge

When asked about the budget status for each security function, respondents in both converged and nonconverged organizations report that cybersecurity budgets are increasing.

SECURITY BUDGETS FOR ALL RESPONDENTS (CONVERGED AND NONCONVERGED)

52%	Physical security budgets are stable
55%	Business continuity budgets are stable
54%	Cybersecurity budgets are increasing

Converged organizations are more likely to have an enterprise-level security leader than those that are not converged.

PREVALENCE OF ENTERPRISE-LEVEL SECURITY LEADER

Converged: 78% have an enterprise-level security leader

Nonconverged: 57% have an enterprise-level security leader

For companies with an enterprise-level security leader, large percentages of both converged and nonconverged organizations are pleased with the results.

EFFECTIVENESS OF ENTERPRISE-LEVEL SECURITY LEADER

Converged: 83% believe leader enhances the effectiveness of corporate security

Nonconverged: 75% believe leader enhances the effectiveness of corporate security

SURVEY PARTICIPANTS

BY ORGANIZATION

Private companies	59%
Public companies	27%
Government	8%
Non-profit	5%
Education	2%

BY GEOGRAPHIC LOCATION

Location	of headquarters	of your department
USA	56%	52%
India	19%	25%
Europe/UK	15%	13%
Other	10%	10%

BY ORGANIZATION'S REVENUE (IN USD)

Less than $25 million	15%
$25-50 million	6%
$51-100 million	7%
$101-500 million	10%
$500 million to $1 billion	9%
$1 billion to $10 billion	26%
More than $10 billion	26%

*Does not total 100% due to rounding.

BY INDUSTRY REPRESENTED

Financial services	17%
Other services	17%
Technology and software	14%
Industrial and manufacturing	8%
Healthcare	5%
Hospitality/leisure	5%
Retail	4%
Education	4%

Remaining 26% includes: public sector, utilities (e.g. electric, gas, Internet), engineering/construction/diversified services, oil and gas/extractive services, pharmaceuticals, transportation, consumer products, communications, chemicals, entertainment/media, and e-commerce.

BY REPORTING STRUCTURE

Who respondent reports to	All	Converged	Nonconverged
CSO/head of security	15%	14%	15%
CEO/chief executive	13%	11%	15%
Vice president of security	11%	13%	9%
COO/head of operations	9%	11%	8%
CIO or CTO	7%	7%	6%
General counsel/chief legal officer	5%	3%	6%

Part II: Behind the Decision to Converge

How do organizations arrive at the decision to converge?

Is it a fiat handed down by top management or does the impetus start from security and rise to the C-suite? In general, it's a combination of both.

Almost 30% of respondents say the primary catalyst to converge was "executive management's perception that 'security is security' and multiple aspects should be converged."

Whether the idea originates with top management or percolates up from security, interviewees uniformly stated that convergence won't succeed without management firmly behind it.

"The companies that do it successfully are those where there is management support and board support," according to the vice president, group security, of a European telecommunications firm.

Occasionally the case for convergence is so overwhelming that company leadership will mandate it despite cultural factors, organizational roadblocks, or staff resistance. As the CSO of the European telecommunications firm describes the move to convergence: "The order to converge was made by the CEO and board management. There was no transition period or planning. There was collaboration prior. But everyone still had their own agendas, goals, and ideas. We didn't do it step by step but in one big step, and it was successful. One senior level person was in charge overall. A board member. At the highest possible level."

Technology also helps make the case for convergence. Long gone are the days when IT required the security department to run video, alarm, access control, and other data on its own network due to bandwidth issues. Not only do cyber and physical share a network, but almost every physical security tool has a cyber component, and many cyber defenses protect against physical consequences. What's more, physical security is critical to protecting physical aspects of virtual environments, including data centers and network hubs.

Many companies have thus integrated their physical and cyber components, which is a big step toward—but far short of—full convergence. Twenty-eight percent of nonconverged respondents said that technological advances could persuade them to converge in the future.

"More and more physical security is moving toward IT security," says an assistant director of business continuity, physical security, and crisis management. As head of the Indian division of a large multinational financial services firm, he serves as global vice chair for risk management overseeing all global security. In his world, global security is converged under the risk management and business continuity umbrella, but individual units in various global locations manage their own needs in line with local requirements.

Convergence at his firm was triggered by corporate business continuity concerns and the desire to create a shared set of business practices and goals across all security functions.

PROMOTING CORPORATE GOALS, EFFICIENCY, AND COMMUNICATION

> The main catalyst for convergence, reported by 40% of survey respondents, is the "desire to better align security strategy with corporate goals."

Although corporate goals vary by company, it is reasonable to assume that major corporate goals include growing business, gaining efficiencies, enlarging markets, enhancing shareholder value, and increasing productivity. And indeed, some 16% of respondents indicate that the "need to increase efficiency" is a major reason to converge.

Organizations across industries and regions understand that having multiple security departments that don't talk to each other or meet sparingly is unacceptable in an age of threats that defy traditional boundaries. Though many nonconverged organizations insist that their security departments meet frequently and work jointly on projects, the survey responses show that collaboration is closer at converged organizations. Some 30% of respondents indicate that a major catalyst for converging was "need for enhanced communication/cooperation among security and/or business continuity functions."

For one international energy company, the path to convergence was charted when a new CISO was hired and immediately instituted a convergence plan. "He wanted a much closer connection between cyber and physical security," says the firm's head of physical security. "The main reason to converge is sharing of information in a combined area. Security is now so complex—physical information and cyber—that combining all the knowledge is essential."

Who ends up leading the converged effort may be based on culture, personality, relationships, or even happenstance. A minority of organizations report to a chief risk officer or another executive who owns the entire organizational risk palette.

"We have a senior leadership integrated risk committee that I lead and administer that is accountable for security," says the vice president of enterprise risk management and global security for a technology company. "We are working collaboratively together to direct and manage the strategic risk that is presented to our company. There are daily conference calls with IT and physical providing some level of support."

His team lists and reviews the top risks, and the business continuity group develops plans. ''Our business continuity team has a plan B to respond and mitigate the risks."

Part III: The Impact of Convergence

Typically, the decision to reorganize the security function—in many cases entailing reorganization of departments such as IT and risk management—is not easily made. Cost, in terms of training, new personnel, and new systems, is one factor. Another is disruption to existing operations and the potential for heightened vulnerabilities during the transition. And there are questions of the impact on culture and morale.

But the overriding concern is, of course, will a converged department result in a stronger security operation and a unified strategy that enables the organization to meet new threats and challenges? Or, is security more effective when divided into separate teams, communicating and collaborating as events dictate?

SECURITY IS BETTER OFF WITH CONVERGENCE

The survey results paint an overwhelmingly positive portrait of convergence.

Nearly half of survey respondents say that convergence has at least "somewhat strengthened" their overall security function, and another 30% note that it has "greatly strengthened security." Only 4% indicate that convergence has led to a weakened operation, and just 14% indicate there is "no change."

These numbers are consistent across all three security disciplines. More than 60% of respondents say physical security is either somewhat or greatly strengthened. The numbers for cyber and business continuity are 55% and 70%, respectively, indicating that business continuity gains the most from convergence.

> The bottom line is that the great majority of organizations that have converged are satisfied with the results and feel the effort was worthwhile.

Convergence can lead to benefits that security and strategy planners may not have envisioned. For example:

- One-quarter of security professionals say that convergence has helped them gain a more efficient security operation. No doubt this was a primary goal.
- An almost identical number indicate that a holistic approach has enabled the security staff to become more versatile and well-rounded.
- Forty percent say that convergence has led to better alignment of security strategy with corporate goals.
- Some 35% say that convergence has smoothed the way to create a shared set of practices and goals across physical security, cybersecurity, and business continuity teams.
- In 39 percent of cases, convergence has clearly enhanced communication and cooperation.
- About 23% say that convergence has resulted in more visibility and influence with the C-suite and board.

These percentages in reality could be higher since respondents were limited to choosing just the top three benefits they had experienced.

Consider some of these illustrative responses from the interviews:

"We collaborate on risks and how to manage them at the most senior level. And we partner." (U.S. technology company)

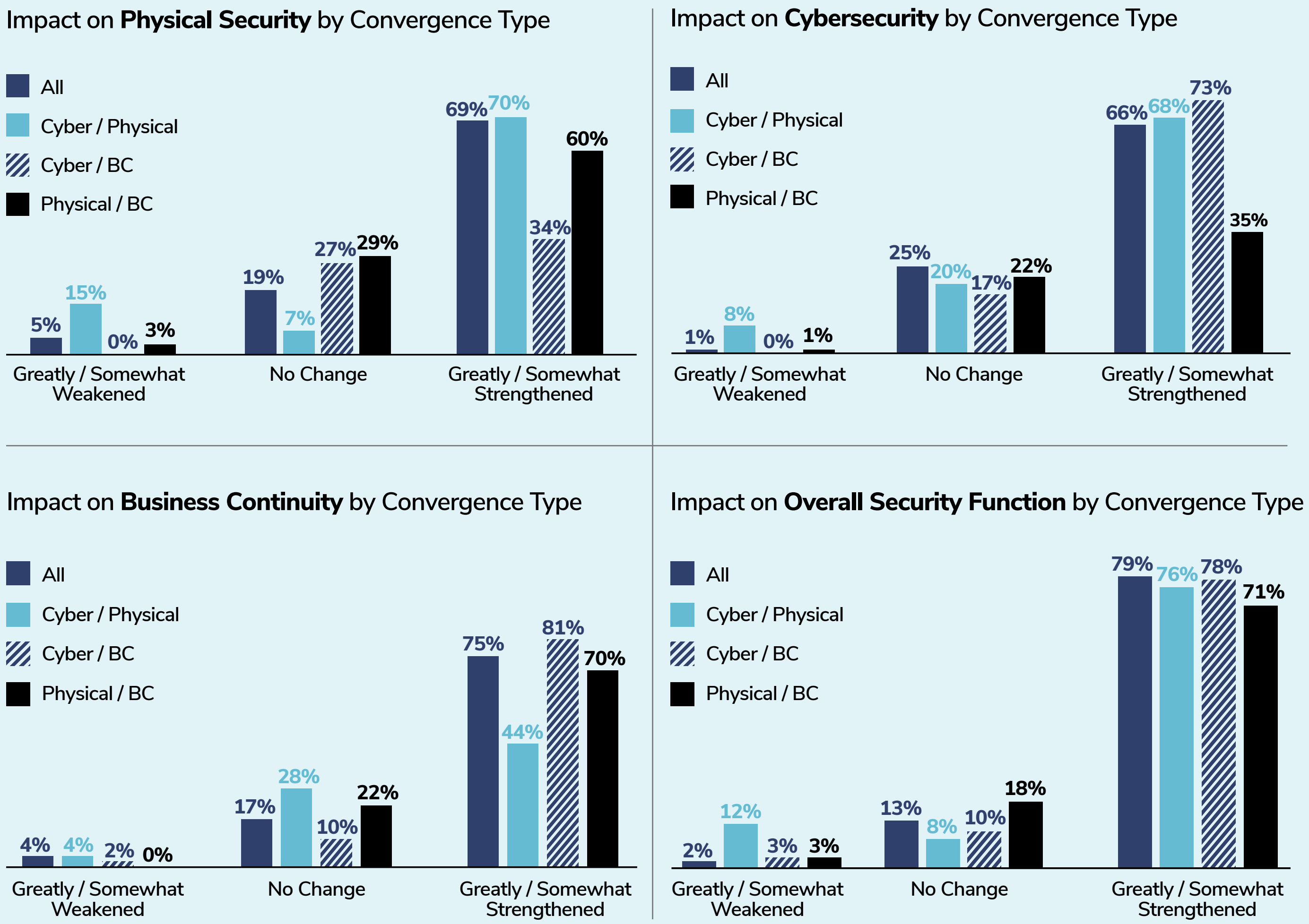
"There's been a great improvement in security training and awareness across business units." (International energy company)

"The main benefit is increased information sharing. The key element is that cyber and information security cannot be separated from physical security since there is always a physical manifestation somewhere." (European interior ministry)

"It makes all security teams stronger. Second is the cost savings aspect. Third is the smooth functioning of the group." (India-based division of international finance company)

We achieved our two main objectives—cost savings and better alignment between security functions." (International telecommunications company)

HOW CONVERGED ORGANIZATIONS VIEW IMPACT OF CONVERGENCE



Impact on **Physical Security** by Convergence Type

Impact on **Cybersecurity** by Convergence Type

Impact on **Business Continuity** by Convergence Type

Impact on **Overall Security Function** by Convergence Type

CHALLENGES IN CONVERGING

The path to convergence is not always smooth. What are the main drawbacks?

The good news is that 44% of organizations that have converged two or more functions report "no negative results" when prompted with a list of potential negative consequences. However, challenges remain.

Role confusion, communication issues, and turf battles. For the 56% that have experienced some problems, the main issues relate to staff. Almost 30% of converged security leaders report confusion over roles and responsibilities, and another quarter indicate they are unsure about lines of communication and reporting. Heads of security can't assume that because their departments are converged, communication will take care of itself. Other common problems include cultural conflict and turf/silo operating traditions.

The CSO has a key role to play here. It's up to him or her to provide leadership. "That's how I see my role, communicating between the different specialties, "observes the security chief at a European energy agency.

"The cyber and physical jobs can overlap. If the access controls to servers are limited or have a flaw in data management, my physical guy needs to know that," he continues. "They have different skills and need to inform each other. Access controls have a physical part, a cyber part, and a management part. So one must inform the other if there is a problem. While our staff is versatile and well-rounded now, we experienced conflict among staff and confusion over responsibilities."

A New Delhi security department for a large multinational finance firm has a similar issue. Convergence is on a global basis, but vertical geographic teams operate independently. The global project leader assists the local teams to implement project requirements. This India-based assistant director reports confusion over lines of reporting and over roles and responsibilities.

In organizations where cyber and physical security are converged but business continuity is on the outside, confusion abounds. That's the case for the European energy agency. "Business continuity is not converged," says the security chief. We have different business continuity plans if you are looking at cyber risk, safety, or physical security issues. That's something we need to address. We are starting to have a more collaborative response plan."

A European telecommunications company has faced challenges with battles for primacy. "The main barriers to convergence were turf and silo issues," says the vice president of group security. "Everyone wanted to safeguard his responsibilities, his people, his budget, his prestige and his importance to the company."

This telecom security executive has been able to overcome "siloed thinking" two ways. First, he has demonstrated to his department the added value of convergence. Second, he has received support from the CEO and the board in making clear that convergence is a top management priority.

According to the CSO of an international energy firm, the main cultural problem has been with the cyber group. "People need to understand what each must do. Six weeks into the new organization, there were growing pains and ambiguities. [Cybersecurity staff members] were concerned about how changes would impact job security. The cyber side was much larger than the physical side, which didn't have this problem because it was leaner. There may have been concern that we would move people out."

Lack of skill sets. Indeed, creating a converged department requires talented people with the skills to make it happen. And, for many organizations, budgets and costs remain an issue.

"When you look for someone with the cyber talent, there is the financial part to consider," says the CSO of a European energy firm. "I need to pay a lot more to have a cybersecurity guy than a physical security guy. Here everyone earns about the same, so I have to hire a junior cyber person and train him."

Finding the various skill sets in a single person is rare. According to the vice president of enterprise risk management and global security for an international tech company, "We have not found a skill set or competency in one individual that addresses the three buckets—cyber, physical and BC. The downside is that this talent costs money, so we tackle these risks as a team. The upside is you have more eyes on it."

Confusion over roles and responsibilities. Another key impediment is organizational. Many professionals believe that security operations run better within a stovepiped department, especially in the cyber area. Some 21% of security directors say that cybersecurity requires its own operation. Cyberthreats are often perceived as higher priority because of the proliferation of attacks, the anonymity of adversaries, and the high-profile consequences of a data compromise or privacy breach. The growing threats of hacking and data compromise are constantly in the news.

CASE STUDY: AN EFFECTIVE CONVERGENCE TRANSFORMATION

An integral piece of the convergence puzzle is the ability of senior security staff to articulate their vision of a converged department to senior management.

In one case, the CEO of a $300 million finance company was seeking a CISO to head the cybersecurity department. In the recruiting process he interviewed a former CSO of several major companies that had converged departments.

Says the candidate: "I told him (the CEO) that forward-looking organizations are bringing all security together under one roof. It turned out that they hired me and gave me all of security to converge. I have a military background. I knew physical and cybersecurity. And I had worked closely with the chief security officers at two previous jobs who had converged their security departments."

Over a six-month period, this CSO was able to converge physical security, privacy, business continuity, enterprise risk, cyber, and credit. What led to the successful convergence project? A number of factors.

First, it had the support of the CEO. The CSO continues: "The CEO is visionary. I described to him the status of his security operation and explained that we are starting to see convergence across many industries. The vision for him was how to take all these functions and bring them together. You become a much more proactive organization. You didn't have the silos that you had previously."

"We have been fortunate. We are a relatively small organization growing rapidly. We didn't have a strong function in any of these areas. It's come together well. We didn't have the cultural issues that I had to deal with in other places."

But this CSO concedes that there were some political issues, although they were relatively minor.

He wanted to show success early as a strategy to minimize resistance. "Who cares who reports to whom, let's start working together and getting some quick wins, then highlight what happened," he recalls. "We were able to show loss avoidance. We showed how with the old way of doing things we were losing X dollars in fraud. With this new way, we are preventing it. So we built a business case and demonstrated it can be successful."

The CSO makes it clear that an organization cannot achieve every goal at once. He notes that business continuity is still maturing. "There is a tech piece and a physical piece [to business continuity]. No one really brings them together. My goal is no matter what happens, any incident or crisis, the same organization is handling it the same way every time. That way the executive team is confident and comfortable with our response."

A major benefit of convergence has been awareness. "Culturally it has people thinking differently about security. Everyone knows where to go. People pay attention to security. There is no confusion. When it comes to investigations, we are already making headway. We are preventing things. The fact that we have all these folks working together—fraud, privacy, cyber, physical, BC—makes investigation and response much smoother."

Part IV: Adoption of Convergence Is Gradual

Convergence has dominated conversations at security conferences and appeared regularly in the trade press. The consensus appears to be, "yes, the benefits far outweigh the drawbacks so it's inevitable that lots of organizations will embrace convergence and sooner rather than later."

But that's more speculation and theory than fact.

Since this is one of the first studies to put solid data behind speculation, this research initiative cannot analyze the uptake of convergence over time. However, at least two studies have measured the extent of convergence at least obliquely.

Tackling Cyber Crime: The Role of Private Security (M. Gill and C. Howell, Perpetuity Research Group, June 2016) surveyed 289 security professionals. Discussing convergence, the report states: "over a quarter of respondents (27%) said in the companies they discussed there was one overall strategy that included both physical security and cybersecurity and a half (50%) said they had separate strategies for each. When asked whether there was a senior person responsible for both cyber and physical security, less than a third of cases (31%) said [there] was."

While convergence as defined in that report does not necessarily track perfectly with the definition used in this ASIS Foundation research, it's notable that in both cases convergence is about 25 percent.

Recent research on security at healthcare organizations also touches on convergence. In *Critical Issues in Healthcare Security* (G. Seivold, Tarsus Direct, October 2018), security professionals at hospitals and healthcare institutions were asked about the relationship between physical security and cybersecurity. Twenty-eight percent said there is "linkage" between the executive in charge of physical security and the one responsible for cybersecurity, and that they report to the same person. The survey didn't inquire about convergence per se, however.

The report also found that there is "moderate" strategic alignment between the two functions. "Linkage" has a broader connotation than "convergence," which might explain the 28% of linkage found in the healthcare study and the 11% of convergence in the healthcare cohort in this ASIS Foundation research.

As is frequently the case in the business world, planning and execution do not necessarily flow in a smooth sequence. That appears to be equally true with convergence. There is no groundswell movement toward convergence. Nor are companies abandoning it en masse. Neither again does it appear to be a fad.

To gain a clear understanding of where convergence stands in 2019, one must examine the various levels of convergence. At one extreme is complete convergence, the holistic blending of all major areas of security into a single unit. That would include cybersecurity, physical security, and business continuity, and perhaps other disciplines such as white-collar crime, brand protection, and safety. There are, of course, different interpretations of complete convergence based on industry practices. So, for example, convergence in financial companies would likely have to include other white-collar crime, while in chemical companies it would embrace safety. In others, it might include personal or executive protection.

In common parlance, convergence is predominantly between physical and cybersecurity. A look at this breakdown shows that 24% (the 19% that converged physical, cyber, and business continuity plus another 5% that converge cyber and physical but not business continuity) of responding security professionals indicate that they have achieved this form of convergence.

An additional 21% of respondents say their physical security and business continuity functions are converged in a single department and 7% have converged cyber and business continuity.

But CSOs of nonconverged firms do not believe this situation will inevitably lead to total departmental convergence.

> This research suggests that companies take small steps toward convergence, encouraged by the prospect of increased efficiency, cost savings, and more effective incident response. The integration of new IP-enabled physical equipment and systems—cameras, access controls, etc.—onto corporate IT systems also favors a converged approach.

Yet objections persist. Many were articulated in interviews for this study, such as the following:

"Our system of security works fine the way it is, why change it?"

"It will take extra physical and monetary resources to achieve this goal, we may be vulnerable in the process."

"Our culture indicates departments operate by themselves, silo considerations could create morale problems."

And the list goes on.

Thirty percent of respondents report that "cybersecurity and physical security routinely work collaboratively," and another 10% say that "cybersecurity and physical security have formal connections and shared objectives; they meet weekly or more often." Another 11% point out that these two departments are "heavily integrated with a single set of shared practices and goals." So more than 50% of respondents have some serious integration policies that border on complete convergence.

Yet some 49% concede, "cybersecurity and physical security are two separate departments and only interact when circumstances require it."

WHO IS CONVERGED?

Size matters. Smaller organizations are the most likely to have converged all three functions: 31% of organizations with less than $25 million in annual sales report being converged. Incidence of convergence falls by almost half for the largest companies: 16% for businesses with more than $10 billion in sales, and 13% for companies with sales between $500 million and $10 billion.

It stands to reason that small firms, with lean staffs and modest physical and cybersecurity requirements, are converged out of economic necessity. In startups, one person will often take on all security-related tasks.

What's holding the large companies back? Interviews indicate that many companies want to ensure that convergence aligns with organizational goals and that silo issues can be minimized before they move ahead.

But duplication of effort and overlap are driving more larger firms to consider convergence.

THE INDUSTRY PROFILE

The rate of full convergence (all three functions) across industries in our study is 19%. Full convergence is more common in the utilities industry (30%), and about average in financial services (19%), and technology/software (19%). It is least common in healthcare (11%), retail (11%), and engineering/construction/diversified services (11%).

REGIONAL COMPARISONS

Is location a primary factor in an organization's determination of whether to converge or not to converge?

U.S. organizations are yet to move decisively to full convergence; just 16% have achieved full convergence. By contrast, 23% of Indian and European organizations have converged.

Part V: Nonconverged Organizations

Convergence is not a new concept. Security executives report having considered the idea as far back as 10 to 12 years ago. A few began the effort two decades ago.

Yet 44% of firms currently have no form of convergence, and many more are only partially converged. This is the case although (1) convergence seems to yield more benefits than drawbacks, and (2) advances in technology have permeated even the physical security space and seem to be naturally drawing the different security functions closer together.

So why aren't more firms converged? The data and in-depth interviews with security leaders identify many hurdles. But the major reason is clear: most organizations are content with the status quo until a triggering event or a C-suite mandate requires change.

A major delta exists between a good idea and a corporate imperative.

> Many security directors say convergence is a great idea and plan to converge. But not yet.

LEVELS OF INTERACTION

This research sheds light on the organizational structures in which nonconverged firms currently operate and the extent to which cybersecurity, physical security, and business continuity interact.

Given today's increasingly sophisticated threats, one might expect routine, robust collaboration between the various security functions. But 45% of nonconverged organizations report that "cybersecurity, physical security, and business continuity have operated independently and continue to be separate departments."

In nonconverged organizations, interaction between cyber and physical is less likely. In fact, their departments are so isolated that 63% report that they interact "only when circumstances require it."

Of the 45% of firms that are completely nonconverged, less than one-third say their three key functions—cyber, physical, and business continuity—are "continually collaborating or are partially integrated."

Some interviewees see convergence as a false panacea, promising much more that it can deliver. In fact, they see it exacerbating tensions between the functions, at least in the short term. One former CSO of two multinational corporations based in Europe says that convergence turns into a competition to determine who is able to impose their particular view of security: "The convergence discussion has been driven more by a classic turf fight between physical security, IT security, and compliance," he contends. "Each function is very much convinced that they understand all risks and that they shall lead the 'converged' effort to protect the company. In reality, risks are diverse and the strategies to fight risk are diverse as well."

He argues that the converged security leader can't help but take a parochial view. "Converging all these risk-fighting functions may lead to a preference of one of these risk factors, likely the one the functional leader feels most comfortable with. There is no win from just merging functions and people for the sake of convergence."

ORGANIZATIONAL BARRIERS

Organizational barriers are among the top obstacles to convergence. That's the case at a transportation company that runs three airports. Security is not converged. The CISO runs an IT security function on a group level; he is responsible for cybersecurity at the three airports. However, physical security is divided by profit and loss centers or by airport location.

"I am responsible for cybersecurity across a whole group for all the different entities. I take a group view of all the solutions," says this CISO. "That doesn't happen in physical security. They are run by policy security managers. They are low down the chain. Physical security is decentralized; cyber is centralized."

There is minimal collaboration. Adds the CISO: "We could get a lot of synergy and cost savings. We could do more if we centralized everything in the same way we centralized cybersecurity."

A similar impediment exists for the head of physical security and support operations at a New England health system. Cybersecurity is run as a shared service across all four hospitals in the system. Physical security, by contrast, is independent at each hospital.

This head of physical security describes a collaborative but not close working relationship with cybersecurity. "We formed mini work groups and teams to be engaged and figure out what's going on. When anything comes up, like cyberattacks, we absolutely work together with cybersecurity."

Some companies eschew large departments and prefer small working groups, which they believe promote flexibility. Such is the situation with one international software company based in India that prefers smaller, distinct operations. Its director of safety and security reports that there is much overlap among the functions and that he would prefer being converged. "It would be more efficient if there was one team, converged with business continuity. We would also save money for the organization."

Some large international companies say they are too geographically dispersed to operate effectively in a converged environment. One European-based beverage firm with a popular global product is most concerned with protecting its brand and securing events that it sponsors, such as professional sports matches. The director of global security is responsible for personal security of top staff, event security, and travel security.

"We are partially involved with cybersecurity, which includes criminal threats and incidents that fall within our mission," he says. "But the main responsibility is with our global IT team. Business continuity reports into the supply chain."

Some of the most significant organizational resistance to convergence lies within the physical security team itself, which sees the threats as too diverse and particular for convergence to work. "We work with local division companies and they are responsible for their own physical security. They also have to be worried about global events in different regions, like Africa," says the beverage company's director of global security. "Many companies that converge are not dealing with wars or civil unrest like we do."

REPORTING RELATIONSHIPS

The incidence and extent of convergence depends in part on reporting relationships and structures. These are difficult to modify, both from a top management perspective and from the view of employees and their managers.

Physical security reports to a myriad of different roles. They include: CEO, CFO, COO, head of administration, head of HR, general counsel, head of real estate/facilities, chief risk officer, and many more.

The same holds true for the business continuity function, which reports mainly to the COO, chief risk officer, and CEO, but to many other roles as well.

By contrast, cybersecurity reports almost exclusively to either a tech or IT executive. Almost two-thirds of respondents in the cybersecurity function report either to the chief information security officer (CISO), the chief information officer (CIO), or the chief technology officer (CTO).

BARRIERS TO CONVERGENCE

The leading roadblock to convergence among nonconverged organizations is turf and silo traditions, cited by some 41% percent of organizations. Here are some key points to consider:

First, top security managers do not necessarily perceive silo and turf as being political in nature, but rather a justified tradition and perhaps a business necessity considering the specific risks to their operations. Divisions might even be necessary for compliance reasons. The vice president of security at a major European chemical firm cites silo and turf objections to convergence. But he is quick to add that safety is a major concern in the chemical industry and that it is much more aligned with physical security than it is with cyber. Traditionally, safety has been in the domain of the physical group and needs to stay there.

"I see a lot of converged activities between physical security and safety in the chemical sector," he says. "It would be more complicated to converge in chemicals because if you wanted to converge cyber and physical, how would you deal with the safety aspect?" He cites as a complication that at several sites there are joint physical security and fire brigades. "Would we have cyber and fire brigades converged in one team? I am not sure that makes any sense."

> In fact, many of the security executives interviewed acknowledge that they are happy with the status quo and think that each function should operate in its own department.

"The timing is not right," according to the director of security at an automotive services firm. "We have a turf and silo operating tradition with the belief that physical security owns its operation and cyber owns its operation."

His firm is concerned that changes would only add to the confusion. "Right now, everyone is operating in their own silos and knows where to go. If somehow, we try to merge those units it's going to take from our daily jobs. It will cause disruption because no one will know where to go."

Different cultures and skills were also cited by 40% of survey respondents as a major barrier to convergence. The head of group security at an international insurance firm who opposes convergence is one example. "Skills are very different, and the view is there is no benefit of having one department and head," he says. "Why should we put things together when they are not broken. There is no reason."

One head of physical security mentions that at his firm, and others, physical security is a mature operation with its own culture. The cyber group is fairly new. Still, he would like to overcome these roadblocks and plan for convergence. "I am quite convinced it is an advantage if you can get there because of more balance between cyber and physical budget-wise. It would operate more efficiently and productively."

In some cases, cybersecurity is considered so important that leaders believe convergence would actually dilute its effectiveness. As mentioned earlier, that can sometimes be true. One example among nonconverged companies is a major global retailer. Physical security and business continuity are converged and report to the general counsel, but cyber is a separate stovepipe; the chief information security officer reports to the chief technology officer.

"We are coming off a major data breach and poured millions into information security. It derailed many internal partnerships because they (cyber) built out so far and so fast. It went from dozens of people to hundreds," says the head of physical security for the retailer.

This head of physical security says resistance to convergence goes beyond the data breach. "Our brand is very well known. And people have an emotional connection with us. It wasn't only about the size of the breach. It was about the trusted relationship people had with us." Top management set a priority of safeguarding customer trust through stringent data protection measures. It felt this key goal was best accomplished by maintaining a distinct cybersecurity function.

Cultural differences, skill sets, and silo operating conditions all stand in the way of total convergence at this organization. "The systems we have in place now tell us we are best prepared in case we have another breach tomorrow. But that also slows us down toward migration to the convergence model."

This head of physical security would like to see some form of convergence between physical and cyber systems but not to create a single operating unit. "Two separate functions within a broader function is the best way to describe what I would like to see happen." Perhaps, he added, both groups would report into a chief risk officer.

Senior executives contemplating convergence have successfully identified what the problems might be if they embark on the path to convergence; many of the feared negative results are cited by security experts at companies that had converged.

> Nonconverged security executives identified silo and cultural issues as top barriers to convergence and executives with converged departments indicate that these silo and cultural concerns did indeed pose challenges to them as they embarked on convergence. Several say that these issues remain challenges, even years after convergence.

Similarly, 25% of security executives fear that managerial collaboration (or lack thereof) could be a barrier to convergence. Eighteen percent of converged company executives say that this indeed has proved to be a hurdle.

Organizational structure also emerges as a justified concern. One-quarter of nonconverged firms resist convergence out of concern that security necessitates separate operations. Among converged companies, 18% confirm that this is a major hurdle.

PLANS TO CONVERGE

Even among security directors whose departments have not converged and who cite significant barriers to convergence, almost half believe convergence would greatly strengthen their security function, and another one-third note it would at least "somewhat strengthen overall security."

Although 78% of security directors in nonconverged organizations have a positive view of convergence, that does not augur an imminent move in that direction.

Nearly 70% of security executives say their companies have no plans to converge. Another 10% say they don't plan to converge for at least three years—about the average time a strategic plan extends into the future.

Why is there a gap between perceived benefits of convergence and actual plans to converge? Several data points provide clues to why the timing may not be right. One relates to overall strategy and corporate goals, which, as indicated previously, are key factors in momentum for convergence.

Senior management does not change organizational structure easily or frequently. Managers require evidence of a benefit that will coincide with corporate objectives.

When asked what factors would compel them to converge, almost 40% cite "better alignment of security risk management strategy with corporate goals." For many organizations, that alignment is still down the road. As the CISO of a U.S. financial firm puts it, "We are not there yet. There would have to be some business justification. There are no current plans for convergence but there might be in 3 to 5 years."

The director of global security for an international beverage company expresses a similar sentiment. "We are not converging yet. We are a conservative company. Cyber has only been on our agenda a very short time," he points out. "Business continuity is more connected to physical security at the moment. But there is a movement more to the IT side."

Many security executives are satisfied that collaboration among the three functions is adequate and that full integration is unnecessary or even risky. More than half of nonconverged companies report that at least two of the three functions collaborate or are partially integrated.

In fact, nearly a third report that all three functions—cyber, physical security, and business continuity—collaborate or are partially integrated.

CASE STUDY: E-COMMERCE COMPANY

To a large extent, the question of convergence comes down to the way a firm does business as well as its culture and organizational structure. A major U.S. e-commerce company provides a good example where the director of security manages physical security, travel safety, and resiliency. He has more than 25 years of experience and reports to the company's CFO.

He notes that his firm's physical security and business continuity functions are merged but stand apart from cybersecurity. "As an e-commerce company, cyber is very important and so it is kept separate from all other sectors," he says.

At this company, the degree of integration is driven more by people than by formal structures or policies. "I would say we have a close collaboration with cybersecurity, but it is more driven by personalities. When personalities get along, the collaboration works great. If not, it suffers," he says, adding that his security partner, the CISO, reports up to one of three CEOS—the CEO of the Web services group (as mentioned previously, the physical security director reports to the CFO).

The director of security does not support total convergence. "I actually prefer this to a formal structure, after seeing how well it works for us. It's become part of the company culture."

A key part of the collaboration involves protecting facilities such as data centers. "We (cyber and physical) conduct joint audits for which my team is responsible. This is an area in which we have close collaboration. We balance the right level of risk for our internal customers who work in those buildings."

Business continuity has been tethered to physical security for 19 years. "During much of that time, business continuity received little attention and was viewed as a real estate function. We now have the people and expertise to know what it should look like," the security director says. He believes that convergence would weaken security at his firm. "At other companies, it would probably strengthen security overall. I think segmenting the company and having individuals taking responsibility for different segments…works 95–98% of the time. I would argue that each company needs to evaluate independently what they are doing to meet the security needs of their internal customers."

Part VI: Staking A Middle Ground

This research shows that even nonconverged companies believe there are major benefits to convergence.

As mentioned previously, almost 80 percent of nonconverged organizations acknowledge that convergence would strengthen their overall security function.

WHAT IMPACT, IF ANY, DO YOU FEEL CONVERGENCE WOULD HAVE ON YOUR SECURITY FUNCTIONS?

	Somewhat Strengthen	Greatly Strengthen
Physical security function	35%	32%
Cybersecurity function	41%	33%
Business continuity function	37%	38%
Overal security function	32%	38%

The obstacles to convergence are presented in detail on pages 19–21. But is there a middle ground? Is there a path to convergence that will yield many of the benefits while avoiding the drawbacks, at least in the near term?

.

PARTIAL CONVERGENCE

5%	Cybersecurity and physical security are converged in a single department.
7%	Cybersecurity and business continuity are converged in a single department.
21%	Physical security and business continuity are converged in a single department.

Almost one-third of all nonconverged companies claim some convergence even if it's not full convergence. That leaves open the possibility that full convergence may occur down the road. In fact, several security directors say they are increasing collaboration and hope to fully converge in several years.

What becomes clear is that some form of collaboration, if not convergence, between cyber and physical security is essential, even at nonconverged companies.

For example, 32% of nonconverged firms report that cybersecurity, physical security, and business continuity "collaborate and are partially integrated," and another 17% of firms report some degree of integration between physical, cyber, and business continuity.

> The key observation, supported by interviews, is that convergence or integration needs to be customized to fit the needs and demands of individual organizations within specific lines of business. There is no one model that works for everyone.

Take, for example, the operation of a major U.S financial services firm. The CISO heads cybersecurity and reports to the CIO. He has "a limited relationship" with physical security, which is headed by a director of security who reports to human resources. Says the CISO: "We have meetings once a month to discuss everything from access to potential systems integration to overlap in our security centers. We coordinate access to our buildings. We need physical security to understand the controls we have in place for things like data centers. We also collaborate on execution because we need to know if we have people on site."

At this financial services firm, where data security is essential, business continuity planning reports to the CISO. That's where there is currently some convergence but not total convergence. So far, customization works for this firm. "[We have] no current plans for convergence, but I stated it is something I want to do in 3 to 5 years," the CISO says.

A large U.S. technology company manages security through the risk management structure. In fact, the head of security carries the title of vice president, enterprise risk management and global security. He does not see the term convergence in the typical way it is used; rather, he views it as the leveraging of resources. "We have responsibility for enterprise risk," he explains. "That is, risk that impacts the entire organization whether it is business or strategic risk, an IT risk, or a natural disaster risk."

While this security director reports to the general counsel, the head of IT security reports to the

CIO. In a formal sense, enterprise risk management is converged with business continuity. "We have been completely integrated, one budget and one department," the CISO says. "Even though IT is formally managed separately from physical security, the customers get the benefit and they don't know the difference between physical and IT security."

The head of security at another firm, a United Kingdom-based company in the energy space, emphasizes the benefits of his company's customized approach to security. His title is vice president of global security, and he reports to the CFO. He has responsibility for physical security and business continuity. The CISO, who reports to the senior vice president in the cloud business, has responsibility for all cybersecurity. "I am not a proponent of the word 'convergence,'" he says. "The operational environment has always been converged. We try not to belabor the organizational issues, but we operate around one security strategy.

Managing risk is the corporate objective: "We (cyber and physical) are two independent organizations but we are completely aligned on strategy and implementation because we need to maximize our effectiveness and mitigate risk together."

Part VII: Who Oversees Security at Converged Organizations?

At converged organizations, who gets the top job? Finding the right talent to lead a converged department can be challenging. For those making the transition to convergence, talent, skills, and knowledge at the senior level are key. The chief security officer who heads convergence at the interior ministry of a European government went back to university to study information security.

What is the best combination of skills and experience to head a converged department? Some interviewees indicate that someone from a military security background would be a strong candidate. Others who have broad experience in both cyber and physical security would also be considered.

WHO OVERSEES CONVERGED ORGANIZATIONS?

28%	Chief Security Officer
14%	Security Director
11%	Chief Information Security Officer
10%	Vice President of Security
4%	Chief Risk Officer
23%	Other

These responses are likely disproportionately weighted toward physical security professionals, who provided most of the responses. The results change dramatically when broken down by function—physical, cyber, or business continuity.

According to physical security respondents, a CSO (36%) is most likely to lead a converged function, followed by a security director (19%), VP of security (14%), and CISO (6%).

But cyber respondents see one of their own—a CISO—at the top in 54% of cases, with only 13% reporting to a CSO.

And business continuity respondents also see the situation through their unique lens. Where heads of business continuity are barely cited by physical and cybersecurity professionals, they are said to preside over the converged function in 11% of cases. Business continuity respondents say that CSOs (27%), CISOs (16%), and VPs of security (14%) are most likely to lead a converged function.

The study also asked:

1. Do you have an enterprise-level security leader?
2. If not, in your opinion, would the appointment of an enterprise-level security leader enhance the effectiveness of all corporate security?
3. If so, do you feel your enterprise-level security leader enhances the effectiveness of all your corporate security?

More than three-quarters of organizations with some type of convergence report having an enterprise-level security leader. In nonconverged organizations, just 57% have an enterprise-level leader.

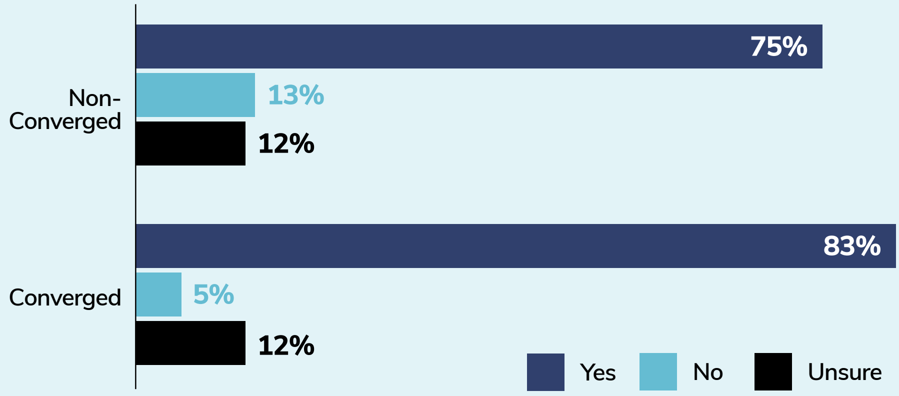
In both converged and nonconverged operations, more than three-quarters of those who have an enterprise-level leader believe it enhances corporate security. In converged firms 83% respond yes, 5% say no, and 12% are unsure. Nonconverged firms respond 75% yes and 13% no, while 12% are unsure.

ENTERPRISE-LEVEL SECURITY CHIEF

78%	of converged organizations have an enterprise-level security leader, 22% do not.
57%	of nonconverged organizations have an enterprise leader, 43% do not
83%	of converged organizations are pleased with the impact of enterprise security leader
75%	of nonconverged organizations are pleased with the impact of enterprise security leader

Large organizations are more likely to have an enterprise-level security leader: 79% of respondents with revenue exceeding $10 billion and 64% of those with revenue of $1 billion to $10 billion. In the mid-cap category, 62% of those with revenue of $100 million to $500 million and 54% of those

DOES YOUR ENTERPRISE-LEVEL SECURITY LEADER ENHANCE CORPORATE SECURITY?



with revenues of $500 million to $1 billion have an enterprise-level security leader.

Larger companies have better results than their smaller counterparts. About 80% of billion-dollar-plus firms say that a single leader has enhanced security. But organizations in the $100 million to $500 million range are less convinced: only 66% give a vote of confidence.

WHAT DO SECURITY PROFESSIONALS SAY ABOUT ENTERPRISE-LEVEL LEADERS?

The security executives interviewed for this study are evenly divided between those who favor an enterprise-level leader and those who oppose that approach.

Several in the "pro" category contend that a security "champion" would have an enterprise-level view of security and the organization; most lower-level security managers operate within their own domains. "Yes, it is better to have an enterprise-level person. He can see all the problems," says the security director at a European food company. "He has a better view of the risks to the company and how to prepare for a crisis. When you can manage everything from prevention to reaction and risk management, of course it will reinforce the ability of the company to survive a crisis." His firm is currently not converged but is considering that move down the road.

The vice president of group security for a European telecommunications firm that is converged also strongly favors an enterprise-level leader. In fact, the firm currently has such a leader. "We have one person responsible for all security—a board member," says this VP. "My recommendation would be to follow our example because we have been very successful. One senior-level person overall in charge—at the highest possible management [level]." He adds that support from top management including the CEO and the board was instrumental in forcing closer collaboration between all facets of security.

The question of who should have the role of enterprise-level leader elicited multiple responses. Some argue that the CISO should have that role, largely because information security has become a board-level concern in many organizations. Physical security executives lack that status.

"We could get access to the C-suite through the CIO," notes the head of physical security at an international energy company. "It causes less confusion for the lines of business and minimizes overlap." This security executive's firm is not converged but he strongly favors convergence.

The senior director for corporate security at a major U.S. retailer, by contrast, believes that the enterprise-level person should reside in risk management. "I think a chief risk officer is appropriate for our organization. We had that person a few years ago and politics got in the way. When you have information that needs to flow, you need to have a leader to make it happen, an enabler." His firm is not converged, and he doesn't see that happening anytime soon.

Those arguing against an enterprise-level security leader pointed to the vast ability and scope of knowledge necessary for that role.

"I don't see one individual able to oversee business continuity, IT security, and physical security," says the director of support operations and security for a New England healthcare system.

The head of group security for an international finance company agrees. "It would be difficult to put one enterprise-level individual in charge. It is a question of one person overseeing everything. He would have to have lots of knowledge, unless he defers to managers below him. He would have to have very broad knowledge of security. It is a tricky thing to find these people."

A similar view is articulated by the vice president of enterprise risk management and global security for a U.S. technology company. "An enterprise-level person? There is not a person out there to really head that in our organization. That's because 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."

The vice president for global security at an international energy firm brings up another factor to consider in convergence leadership. He says it depends on company size:

> "If you are a small or mid-cap firm, then I think it is a good idea to merge everything under one person. But when you get a very large multinational organization that has extremely complex business lines, I think companies and people kid themselves that one person can be effective in that role."

His firm has "a very senior level council of risk owners who have accountability on specific sectors of risk." They merge combinations of two to four people together and that becomes the chief risk group for that area. But he says it comes down to authority and commitment at the highest levels: "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."

Part VIII: Where Business Continuity Fits

While security managers have long defined convergence as the integration of cybersecurity and physical security, many now believe that business continuity must also be part of any convergence to truly be effective.

Forty-eight percent indicate that cyber, physical, and business continuity are not converged at their organizations, while only 19% said these functions are converged in a single department. However, some business continuity functions are converged individually: 7% with cybersecurity and 21% with physical security.

RELATIONSHIPS AMONG SECURITY DEPARTMENTS

Which of the following best describes the relationship between cybersecurity, physical security, and business continuity in your organization (not counting integration of systems)?

Cybersecurity, physical security, and business continuity are converged in a single department.	19%
Cybersecurity and physical security are converged in a single department.	5%
Cybersecurity and business continuity are converged in a single department.	7%
Physical security and business continuity are converged in a single department.	21%
Cybersecurity, physical security, and business continuity are NOT converged in a single department.	48%

Of course, many firms have different approaches to how business continuity fits in. At one major retailer, physical security and business continuity are converged, but not cyber. "Business continuity management (BCM) is a critical process," says the senior director of corporate security. Both report to the firm's chief legal officer. "I think about the bad things that can happen to the organization, and business continuity is on that spectrum very close to emergency management and crisis management. It's a natural fit with physical security."

However, this retailer has a similar component for IT security. "They are focused on continuity of business systems. We call it ITDR, information technology disaster recovery. Many large companies have ITDR teams in place." In this case, as in many other organizations, business continuity itself is not converged. It is split between physical and cyber components.

Many other models exist. For example, the head of security of a European nuclear agency reports that his security function has converged cyber and physical but not business continuity. "We have different business continuity plans for cyber risk, safety, or physical security issues," he says. But he is not satisfied. "We have a business continuity manager. If you have a safety plan and it is isolated from the physical security plan, you know you have a problem. It is not logical that these two are separate."

The same structure exists at a large international energy firm: cyber and physical security are converged, but not business continuity. Again, it is a matter of customization to suit the firm's needs and structure. "Business continuity and resilience in the United States sits with emergency planning," according to the head of physical security. "In the utility industry, emergency planning is a big piece of what we do because you have to worry about storms, hurricanes, etc. We have awareness of what we each do and have monthly meetings but no convergence. You always know what's going on in the resilience world and share information and knowledge with them."

In fact, almost 40% of business continuity manager respondents cite "the need for enhanced communication/cooperation among security and/or business continuity functions as a catalyst for convergence." Another 24% of business continuity managers indicate a "desire to create a shared set of practices/goals across security and/or business continuity functions." This figure matches how the cyber and physical cohort responded.

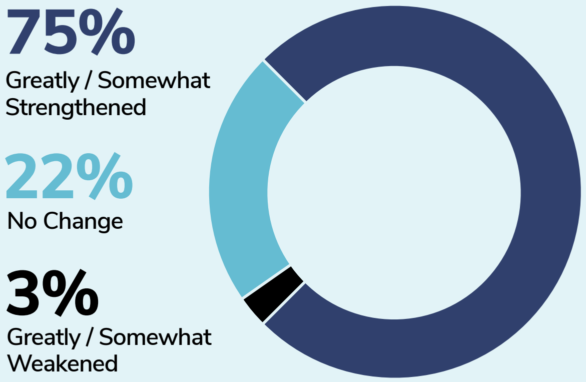
Heads of security at nonconverged organizations might be convinced to bring business continuity into the convergence equation if a number of business continuity issues can be enhanced. For example, 27% of heads of security would be interested in "greater efficiency in security and/or business continuity operations," while 19% want the ability to create a shared set of practices and goals across security and/or business continuity, and another 18% would like to see better communication and cooperation with security and business continuity.

The data show that most business continuity managers endorse convergence. Only 16% believe it would somewhat or greatly weaken the business continuity function, while a resounding 69% believe that convergence would somewhat or greatly strengthen business continuity management.

At some firms, the physical threats have largely been subdued or are not perceived as existential to the business. But not all. For example, at many health systems, physical violence among patients and staff is a more prevalent concern than even a data breach. At many financial service firms, physical security has given way to cyber as the all-encompassing threat. At many firms, the overall risks to the enterprise are what keep the senior staff up at night. It could well be that business continuity emerges as the linchpin of security in the future.

HOW BUSINESS CONTINUITY VIEWS CONVERGENCE IMPACT

Impact on Overall Security Function



Part IX: Costs and Budgets

Costs weigh heavily in the convergence equation—but the confidence that convergence will save money may not be justified. Only 7% of security executives from converged organizations cite cost savings as a primary benefit of convergence. In fact, 6% say that convergence actually increased costs.

That doesn't mean cost savings is a nonstarter. Other responses suggest that cost considerations are relevant. For example, some 40% of security executives indicate that the major benefit of convergence is the alignment of security with corporate goals. Presumably, for many organizations, cost and expense management is a major goal. In addition, 25% indicate that a major positive benefit of convergence is more-efficient security operations.

In some situations, cost savings have materialized, including at one European telecommunications firm. "Why did we converge?" the vice president of group security asks rhetorically. "To achieve cost savings—better alignment between cyber and physical security." From a cost perspective, we had two data centers doing similar work, so we combined them and realized better savings."

In another situation, cost savings are anticipated in the future. The head of physical security at an International energy firm notes that the company has just hired a new CISO who has moved to converge operations. "The budgets have stayed the same. But there will come a time when we don't need 10 people to do a security project, we can do it with four," he predicts. "Budgets will change in the future because we will get more efficiency as we bring the two security operations together."

Closely related to the cost issue is staffing levels. Part of the narrative in why convergence isn't more prevalent is that security professionals will lose their jobs. But staffing doesn't appear to have been significantly affected by convergence. Some 60% of physical functions stayed at the same staffing level as a result of convergence, while 47% in cybersecurity and 56% percent of converged security operations in business continuity retained the same staffing. And most of the staffing changes that did occur were increases. A quarter of firms report an increase in cyber staffing, with 21% citing increased business continuity staffing and 13% higher physical staffing. Only 15% reported cuts in the physical security staffing, 12% in business continuity, and just 8% in cybersecurity.

By and large, convergence benefits the budgets of all three disciplines: converged organizations report an increase in the physical security budget in 24% of cases, of the business continuity budget in 26% of cases, and the cybersecurity budget in 49% of cases. While it's twice as likely that the physical security budget will decrease compared to the cyber budget, that is happening in just 16% of converged organizations. Fifty percent of respondents report that their physical security and business continuity budgets are stable, and 28% report no change in the cyber budgets.

CONVERGENCE IMPACT ON STAFFING

	Increased Staff	No Change in Staffing	Decreased Staff	N/A
Physical security	13%	60%	15%	12%
Cybersecurity	24%	47%	8%	21%
Business continuity	21%	56%	12%	11%

BUDGET STATUS IN CONVERGED AND NONCONVERGED ORGANIZATIONS

CONVERGED ORGANIZATIONS

	Budget Increasing	Budget Staying the Same	Budget Decreasing	N/A
Physical security	24%	49%	16%	11%
Cybersecurity	49%	28%	7%	16%
Business continuity	26%	53%	10%	11%

NONCONVERGED ORGANIZATIONS

	Budget Increasing	Budget Staying the Same	Budget Decreasing	N/A
Physical security	28%	55%	13%	4%
Cybersecurity	58%	30%	4%	8%
Business continuity	19%	57%	10%	14%

WHAT WILL IT TAKE TO CONVERGE?

Survey findings indicate that cost, in and of itself, is not the primary concern for organizations considering convergence. Only 21% of nonconverged respondents say that potential cost savings is a factor that might convince them to converge physical security, cybersecurity, and business continuity.

Alignment of security with corporate goals and enhanced efficiency in security operations are top objectives when organizations consider convergence. Multiple interviews with security heads at nonconverged organizations confirm this result.

"Some areas of physical security are not seeing greater efficiencies so I think it would be better if they (cyber and physical) were merged from a budget perspective," says the CISO of a U.S. financial services firm. "There is a physical operational center and a virtual operational center. Why am I paying for two operational centers?"

But the vice president for global security of a major U.S. e-commerce firm disavows convergence as the best option for his firm. Still, he sees the necessity for aligning goals to achieve efficiency even if security functions are distinct. "We have two independent organizations, but we are completely aligned on strategy and implementation. At any organization, you have limited resources to be able to accomplish something. If you do not have aligned strategies and goals, you are not effectively utilizing resources and probably have a lot of redundancies."

Some security professionals view convergence as a form of centralization. A major European transportation firm has centralized cybersecurity across its three major airport locations but physical security operates separately at each airport. The CISO is in favor of convergence. "We would get a lot of synergy and cost savings. We could do more if we centralized everything in the same way we centralized cyber. There is an economic benefit because you wouldn't have duplication of effort and you could become more efficient."

But some organizations that are pouring resources into cyber have resisted convergence and are willing to absorb extra costs to make sure cybersecurity is strengthened.

This is the case with the U.S.-based retailer that suffered a significant data compromise. "Coming off a major data breach, we spent millions on cybersecurity. A breach is a very emotional thing. People think we can have another one of those tomorrow. We have spent a lot of money being prepared."

Executives at a U.S technology firm that is not converged feel that for the present, the best way to minimize risk is to spend on internal talent even it means incurring extra costs. According to the firm's vice president of risk management and global security, "Our strength is we are leveraging a number of people in teamwork to look at risk and be innovative in how they attack risk. The upside is we have more eyes on it. It gives us a greater level of confidence. And you can be innovative. The downside is it costs more money. You now have salaries in three department budgets to cover."

It is telling that security budgets for nonconverged organizations closely resemble their converged counterparts. It may not be surprising considering that security emphasis has turned to cyber, whether one operates in a converged or nonconverged environment.

For example, physical security budgets have increased at 24% of converged firms and at 28% of nonconverged firms. They are stable at about half of firms in both environments and decreasing at 13% of nonconverged firms and 16% of converged organizations.

Business continuity fares a little better than physical security from convergence. Business continuity budgets are rising at around 19% of nonconverged firms, but at 26% of converged firms. They remain stable at just over 50% of firms in both categories.

Cyber budgets, while still increasing, fare worse with convergence. At converged security operations, cyber budgets are up at 49% of organizations. But the number is even higher at nonconverged companies, with 58% of cybersecurity budgets on the rise. This may reflect the decision to remain nonconverged in order to devote more resources to data and cyber protection as well as risk management.

Part X: Outlook: Challenges and Opportunities

The data suggest that convergence isn't an inexorable trend or foregone conclusion.

Instead, it's clear there are many paths to a successful corporate security risk management function. The "right" solution for any given company takes into account its industry, operating tradition, organizational hierarchy, corporate priorities, and many other factors.

Whatever road is taken, strong leadership is key. Leaders must be able to communicate clear business objectives and overcome turf battles and siloed functions to make needed changes.

The chief of security at a mid-cap financial services firm has dealt with this challenge by getting cyber and physical security staffers to work together successfully on several projects.

But the vice president of group security at a European telecommunications company had to force collaboration. "Everyone has their own agenda, goals, and ideas." He has exercised leadership by articulating the problem to senior management and getting their support and the intervention of a key board member. "Convergence was expected and ordered by the CEO and board management."

As security attempts to remove organizational barriers to change, successful leaders should enlist the support of top management. Who wants to alter current structures or reporting lines? This is a case of turf and silo issues, not only at the staff level, but often among the senior managers. Some 26% of firms report that a major barrier to convergence is that "organization structure necessitates separate operations." Another 27% note the barrier is that "senior executives prefer separate lines of reporting."

Based on this study, it appears that the most successful security operations—regardless of their organizational structure—share the following characteristics:

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

There is a growing need for greater communication and collaboration among security functions. 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 indicate and follow-up interviews confirm, that companies are organizing their security and BC functions in a variety of different ways depending upon business needs. Our survey and interview results show that multiple models—complete convergence among them—can be effective. The chief objective is to create an effective operation to thwart any threats or risks to the organization, whether they be human, technological, or natural.

"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

Conclusion

This first major study of security convergence in the United States, Europe, and India shows that the rewards for convergence are there, but doubts persist, and organizational obstacles remain. While companies are eager for the efficiencies of a converged organization, most of them haven't achieved that ideal. That's due to a combination of factors including culture, operating traditions, industry norms, threatscape, and appetite for change. Though not pursuing standard convergence, many businesses have built processes, relationships, and reporting structures to foster more communication and collaboration between physical security, cybersecurity, and business continuity. Like security generally, these companies are finding that there is no perfect template for convergence.

The ASIS Foundation hopes to continue this research both longitudinally—to track convergence over time—and latitudinally, to more deeply delve into the wealth of information provided by more than 1,000 professionals from three related disciplines over multiple continents. Reader feedback will be key in identifying and targeting future research on this important subject. Please send your feedback on this report to *foundation@asisonline.org*.

Thank you

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 CISOs.

ASIS FOUNDATION™

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.

Support future security research with a gift to the ASIS Foundation. Online at *www.asisfoundation.org*.

ALERT ENTERPRISE
PHYSICAL | LOGICAL SECURITY CONVERGENCE

From our Sponsor

The digital transformation is upon us, as millions of devices become connected via the internet of Things (IoT) and network-connected systems proliferate enterprise landscapes. Inevitably, the threat landscape has evolved as well. Cyber and physical threats are now blended, and the traditional approach of operating with siloed physical security, IT and cyber systems puts the enterprise at greater risk. Today's complex threats require a converged approach that fully integrates and automates security with critical operations and compliance across the entire company landscape. At AlertEnterprise we develop forward-thinking solutions that connect identity governance, access management, security intelligence and compliance validation across IT, HR, cyber and physical security environments—futureproofing security and making it a true business enabler.

Extending converged digital capabilities across logical and physical environments is what we do best. AlertEnterprise brings 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 security convergence 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*