SECURITY CONVERGENCE AND BUSINESS CONTINUITY

REFLECTING ON THE PANDEMIC EXPERIENCE

Executive Summary

Just over 20 years ago, terrorists struck the World Trade Center and the Pentagon, and were foiled in their attempt to strike the U.S. Capitol. Nonetheless almost 3,000 people died on September 11, 2001. Since that time, COVID-19, natural disasters, social justice and first amendment demonstrations, and human-made incidents have created disruptions across the world. In addition, data breaches, ransomware, identity theft, malware, and cryptocurrency scams have significantly increased the cost of cybersecurity. But how prepared are businesses to cope with these security issues? What is the level of preparation? Are they converging their physical and cyber security functions with business plans?

It is within this context that Justice & Security Strategies (JSS) and DTE Consulting LLC, with guidance from the ASIS Foundation, conducted research on the value and methods of merging business continuity and security. The primary concern was to assist the security industry in 'moving the needle' to convergence.

JSS built upon a previous ASIS Foundation survey of senior-level security professionals across the globe. Results from that study indicated that in 2019, only 24% of respondents converged their cyber and physical security functions. When business continuity was included, about half (52%) of respondents converged two or three of these functions. In this study, JSS found that the needle has moved – that 60% of survey respondents had partially or fully converged and that 45% of those who had not yet converged, planned to do so in the near future (compared to 30% in 2019). These findings, and more, are discussed in the report.

Within this research, JSS asked the following questions:

1. What is the contemporary view of convergence, business continuity planning, and security?

2. How does convergence, business continuity planning, and security vary by region (internationally) and within the business sector? Has the needle moved over the last two years?

3. How have major events (e.g., COVID-19, natural disasters, and protests) affected convergence, business continuity planning, and security alignments?

4. What are the lessons learned for convergence, business continuity planning, and security?

The research involved a multi-method approach to answer the research questions, including a literature review, international survey, and intensive interviews with high-level business executives.

The literature review found several definitions of convergence but the common theme and agreement among researchers and practitioners is that convergence takes on various forms, and has different meaning, largely dependent upon factors such as size of organization, industry, skill and expertise of staff and other factors. Convergence is simply bringing differing security functions under a single planning process.

While the literature indicates that definitions of convergence are not uniform, a convergence model emerges from the literature. ***There is agreement and common thought that convergence requires communication, coordination, and collaboration. This is particularly important across groups or individuals who are responsible for some form of asset protection and risk management, and continuity of operations.*** This also must be fully supported by executive and senior management if an organization is to realize and achieve convergence as defined by the organization.

The literature supports the notion that convergence can be structural, or an organizational philosophy, or a combination of both. It is clear, however, that convergence is guided by a set of principles, or factors, that shape and guide the leadership, communication, coordination, and collaboration process needed to support convergence.

ASIS Definition

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. (Beck et al., 2019, page 2)

In 2019, 52% of survey respondents said they had partially or fully converged. That increased to 60% in 2021.

Survey and Interviews

An online survey of 25 questions was administered to ASIS members. The response rate for the survey was 15.5% with 1,092 individuals answering questions from 90 countries.

These are the major findings from the survey:

1. Organizations are moving toward convergence. In 2019, 52% of survey respondents said they had partially or fully converged. That increased to 60% in 2021. Further, more businesses said they anticipate converging than before – 45% in 2021 compared to 30% in 2019.

2. The results indicate respondents perceived that convergence strengthened their organizational capacity for business continuity, physical security, and overall security --over 80% of respondents believed that convergence strengthened functions.

3. Respondents from small and micro companies across the globe (73.9%) reported that they were fully or partially converged at a higher rate than their large (52.5%) and medium sized (64.4%) counterparts.

4. Overall, 66.3 % of respondents from international companies indicated that they were partially or fully converged compared to 54% of respondents from companies in the U.S.

5. Approximately 82% of respondents indicated that the COVID-19 pandemic had an impact on security practices in their organizations.

6. Sixty-two percent of respondents reported that demonstrations and social unrest affected security within their organization, while 25% of respondents were not impacted in this way

Interviews

Twenty-one interviews were conducted, 19 of which participated in the global survey. Two experts on convergence and business continuity were added to the pool. The interviewees represented large, medium, small, and micro-sized businesses and were from the U.S. (n=12) and other countries (n=9).

Major findings from the interviews:

1. Interviewees across the board and from organizations of every type cited communication, coordination, and cooperation as key aspects of converging and maintaining business operations post-convergence.

2. Interviewees described their security practices along a continuum of convergence. Depending on the organization's structure, size, industry, and other factors, interviewees described various approaches to security planning and functions.

3. Functional and procedural approaches to convergence were implemented to varying degrees. Functional approaches took the form of actionable items such as structural changes, security trainings/awareness courses, meet-

ings, and policy development. Procedural approaches to convergence took the form of organization missions, ideals, and the adoption of a holistic framework for security functions. These methods were more concerned with the organization's problem-solving approach.

4. Smaller organizations approached convergence with more procedural methods than functional ones. This generally occurred because the smaller organizations did not have enough staff or resources.

5. Larger organizations used both procedural and functional methods. Procedural methods (e.g., high-level executive buy-in) were useful in achieving functional goals (e.g., merging security departments) and vice versa. Larger organizations frequently mentioned the necessity of both approaches in achieving convergence.

6. The type of industry of an organization affected convergence. For example, utility companies with government regulations to follow were more likely to converge than others. Similarly, organizations in a higher 'threat environment' were likely to converge as well.

CONCLUSIONS AND RECOMMENDATIONS

In two years, converging physical, cyber, and business continuity planning has increased.

The literature shows that there is agreement and common thought that convergence requires communication, coordination, and collaboration. Convergence also must be fully supported by executive and senior management if an organization is to realize and achieve convergence as defined by the organization.

The survey results support the notion that organizations view convergence providing value for enhancing the operational security and business continuity planning for their organization. This was further substantiated in interviews with senior executives, split among U.S. and international interviewees, despite having a broad and diverse range of opinions regarding the definition of convergence.

Lastly, COVID-19, disasters, and social protests impacted organizations in 2020. About 82% of respondents indicated that the pandemic had an impact on security practices in their organizations.

Overall, this research also shows that the method for convergence varies by size and type of organization and global location. Unfortunately, with all of the material that was reviewed, there was no 'silver bullet' that answered the question of "what is the best, step-by-step way to converge physical, cyber, and business continuity?" Instead, based on the findings of the research JSS has developed a set of recommendations to assist organizations that have not yet converged physical, cyber, and business continuity planning.

Recommendations

Recommendation 1: Clearly define convergence and the benefits of convergence to organization members, and the organization.

Recommendation 2: Assess the need and determine whether convergence is practical.

Recommendation 3: Create and develop a convergence strategy that fits the organization's goals.

Recommendation 4: Recognize the inherent difficulties in merging different personalities, people, and processes.

Recommendation 5: Implement evidence-based best practices aligned with the overall goals of the organization. Create metrics and conduct surveys and audits to measure implementation and efficacy of the strategy.

Recommendation 6: Conduct and provide convergence training and educational opportunities for staff.

Security Convergence and Business Continuity:
Reflecting on the Pandemic Experience

Executive Summary

Primary Authors:
Darrell Darnell
Craig D. Uchida
Marc L. Swatt
Kyle Anderson