Convergent Security

A holistic approach to enterprise security

www.pwc.com/it

pwc

We are living in a fast-changing world where the complex nature of new markets, increased competitiveness and labour mobility mean new needs for organisations. Globalization, easy access to information, exponential growth of immigration and society diversity, worldwide political and cultural conflicts, all these phenomenons have impacted the threat paradigm of security that has also been immutably changed by domestic and foreign terrorism. The “Black Swan” event, random and unexpected, is now a pressing reality.
In this context, Convergent Security can thus be seen as a strategic approach to be used as an advantage. Traditional business industries often approach these issues in a more obsolete way than new digital companies where innovation and business change are embedded in the corporate cultures.
Whatever your business, you need people who draw on wide and diversified expertise areas to face new security challenges.

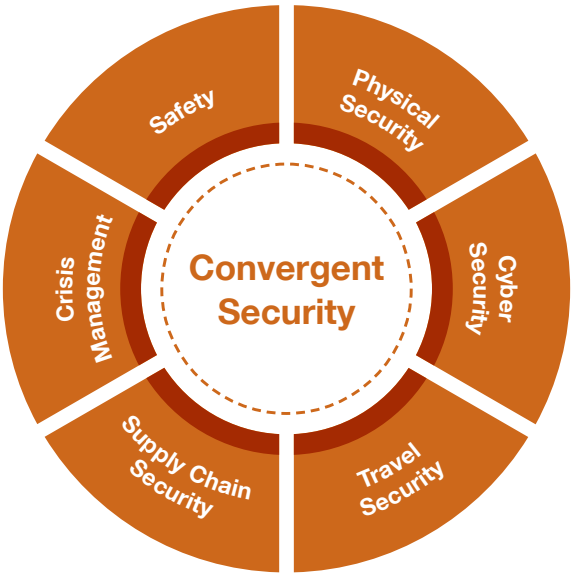
Globalization | **Growth of immigration** | **Easy access to information**

Political and cultural conflicts | **Domestic and foreign terrorism** | **Society Diversity**

What’s on your mind?

What kind of risks is my organisation facing in absence of *Convergence*?
Many organisations have always looked at risk mitigation with a fragmented approach where security functions are managed separately. This fragmentation leads to the mitigation of the risks of individual areas but neglects the cross ones. Moreover, a “silos approach” leads to an increase of redundancies, bureaucracy, costs and inefficiencies. This situation translates into increased risk and complexity that inevitably increments organisation’s risk exposure. The “Black Swan” event, characterized by low probability and high impact, represents now the reality and must be considered in all its aspects.

What do you mean by *Convergence*?
We can define Convergence as the identification of security risks and interdependencies between business functions and processes within the Enterprise, and the consequential development of managed business process solutions to address those risks and interdependencies. This definition captures a significant shift from the emphasis on security as a purely functional activity, to security as an “added-value” to the overall mission of business. This is an important starting point because it essentially changes the way the concept of security is positioned within the enterprise.



Our Point of View

Security Convergence as:

- **Collaboration** by taking the valuable skill sets each respective security function has to offer;
- Combine these skills in an **improved system** and process to ensure the security of people, physical and information asset, and corporate reputation.

You might already have the right resources but they might not be working in the best way.
This new approach will improve overall security and provide a more manageable environment resulting in a competitive advantage over your peers and readiness to continuous innovation.

Avoid the sentence “I have always done this way”, you could start saying “how should I do it?” or “how can I do it better?”

- Classic theories are useful to assess classic risks. In order to face new risks related to this new era, you have to adopt new approaches and methodologies. After all, you can see Convergence as a simple step of technological progress. We went through this when we saw, for example, the integration (or convergence) of access security with video surveillance
- New technologies (i.e. wearables, vassel, drone technologies) and the ways in which they are used, create the need to define innovative approaches. Twenty years from now, we will probably look back and realize that this new era of Convergence actually improved the common definition of security for individuals and organisations

What does “good” look like?

- **Integrated risk assessment** provides accurate measurement to assist the decision making and define a convergent strategy that aligns perceived security with real one
- Risk management has **convergent security objectives** to deal with pervasive risks without waste of resources
- Every aspects of your security’s needs is taken into consideration to ensure the maximum level of **resiliece** for your business and an efficient incident response mechanism
- Holystic approach to Crisis Management & Business Continuity to ensure communication, rapidity, planned resources and **reduction of the «Domino effect»**
- **Cultural and behavioural** programme at every level of the Organisation. The best protection is prevention

How we can help you

- We have a multi-disciplinary team (i.e. safety HSE - *Health, Safety and Environment*, cyber security, counter terrorism, extreme events, large events planning, institutional communication) who provides a unique approach, tools and practical experience in relation to all Security aspects. Our in-depth experience and wide range of skill sets, distinguish us from our competitors
- Depending on your maturity level, we will help you moving towards a more mature approach aimed at defining, prioritising and achieving security objectives efficiently, through a successful programme, based on continuous improvement
- Our Subject Matter Experts will accompany you by supporting your Organisation in every security aspect and offer you personilised services based on your needs

Our Methodology

Thanks to our tested methodology we will help you increasing your maturity level

1

Aspire – helping defining your Vision
We offer you a day with our expert to understand the current security level and define your security aspiration

2

Execute - project planning and deliverable
We identify with you the main critical areas and key risks, building together a forward – looking strategy

3

Simulate - training by examples
We give you real time demonstration of the effectiveness of our approach

4

Subscript - embedded culture and behaviour
We help you during the evolution of your security approach monitoring your progress

What do you gain?

Strategy
You will adopt a comprehensive approach that will assume strategic value to face the global risks your Organisation is exposed to

Focus on your needs
You will achieve your security goals through our expertise that will remain at your disposal

Customised support
We will support you from advisoring to emboding different security roles in your Organisation - or by beeing a Unique Security HUB

Return of investment
A structured security approach change programme which accurately reflects a return on investment for your Executive Board

Risk coverage
With a full workforce that is engaged in every security aspect, you will be agile enough to respond to new threats faced and mitigate vulnerabilities

When to act?

- If you are considering new operating models
- If you have noticed that your organisation (or also your peer) suffers due to unclear roles and responsibilities
- When you need a centralised figure to manage the different aspects of your organisation security
- When you need a customised security offer entrusting it to subject matter expert
- When your security risk assessment results are “high”
- If critical security incidents occurred in the past

Transformation of an enterprise begins with a sense of urgency. No institution will go through change unless it believes it is in deep trouble and needs to do something different to survive

Lou Gerstner (ex-CEO IBM)

Contacts

Giuseppe D’Agostino
Associate Partner | Cybersecurity

+39 347 6466747
giuseppe.dagostino@pwc.com

Gensèric Cantournet
Senior Advisor | Cybersecurity

+39 342 1030532
genseric.cantournet@pwc.com