“Organisations should adopt a comprehensive and integrated strategy that encompasses all areas of security risk” (ANSI ASIS PAP Standard).

Volker Wagner, Deutsche Telekom AG, Senior Vice President Group Business Security
Alessandro Lega, Chair, ASIS European Security Convergence/ESRM subcommittee
James Willison, Founder, Unified Security Ltd
PRINCIPLES FOR CONVERGENCE & ESRM FROM THE ANSI ASIS PAP STANDARD
The right diagnosis and cure

- What has happened?
- What is the problem we face?
- What is the cure?
- We need to establish these issues if we are to recover.
Security Convergence

Security Convergence – Introduction

1) How we manage security – alignment of functions to achieve effective security and share information – awareness of blended threats – creates a fusion of ideas and a more comprehensive strategy – business security.


3) Ongoing relations – SLAs – a team approach right across the IT/Info/Cyber and Physical arena.
2012 – A New Security Standard

- ANSI/ASIS PAP. 1-2102 Standard
- Holistic approach to risk management
- Alignment of functions
- New section on Security Convergence
- Recognises interdependence of Business Functions
- Convergence provides a common platform to assess risk in a shared environment
- Cross functional Risk Assessment treats all security risks in a singular managed process
- The PAPMS – what is it? Goal is to develop protective measures. A systems approach which recognises interdependencies of security systems
Principles of ESRM in the PAP

Physical asset protection (PAP), also known as physical security management, includes the protection of both tangible (e.g., physical, human, infrastructure, and environmental assets) and intangible assets (e.g., brand, reputation, and information assets).

- In order to effectively protect its assets, an organization needs to recognize the interdependencies of various business functions and processes to develop a holistic approach to PAP.

- Physical asset protection is intertwined with other security-related disciplines, such as information technology systems and continuity management. In order to understand the shared risk environment, the organization should consider:

(From pages xiii & xiv)
ESRM Principles (cont)

A common basis for risk ownership and accountability;

- An integrated Organisation wide Security risk assessment and harmonized treatment strategy;

- Common lines of communications and reporting for assessing and managing risk in a cross-disciplinary and cross-functional fashion; and

- Establishing cross-disciplinary and cross-functional teams to achieve a coordinated pre-emptive and response structure.
When implementing this Standard, organizations should adopt a comprehensive and integrated strategy that encompasses all areas of security risk. This should be reflected in all elements of the Standard.

The organization will be better able to achieve its objectives by understanding and incorporating the convergence of PAP, information technology systems, and risk management in all of the elements of its management system.

Security Governance
Physical asset protection is viewed as part of an overall good governance strategy…and is seen as an integral part of enterprise-wide risk management.
4.8 Convergence of Perspectives

Top management and asset protection professionals need to recognize the relationships and interrelationships between PAP and the other disciplines.

Analysis, planning, implementation, evaluation, documentation and review activities need to take an enterprise security risk management perspective, integrating all facets of the functions and processes in the organization. Teaming with other business functions and processes is key to success in protecting the organization’s assets.

6.2.3 Management Context

The organization shall define and document its risk and resilience management context, including: The nature and types of threats and consequences that can occur to its business and operations, How combinations of multiples risks will be taken into account.
A.6. Operation and Implementation

- The organization should establish planning, implementation and evaluation cross-discipline and cross-functional teams with defined roles, appropriate authority, adequate resources including effective and safe equipment, and rehearsed operational plans and procedures.

- The organization should identify competencies and training needs associated with PAP management, including the interdependencies of various business functions and processes. It should provide training or take other action to meet these needs, and should retain associated records (p 16).
The value of the asset, the output from the risk assessment, the organization’s risk appetite, and the relative cost-benefit of the control measures will determine the number and types of layers needed to adequately protect the asset. Evaluation of interdependencies is critical to a successful protection in depth strategy given the reliance of many physical countermeasures on electronic, telecommunications, and information systems. (p 18)
A.7.3 Design of Controls and Countermeasures

- Determining cross-functional and cross-disciplinary interdependencies in a team effort;

- The PAP risk assessment process should be aligned to the overall organizational risk considerations to the facility, asset, or operation where the PAP system is considered for implementation. This should identify the requirements of a single physical asset protection system application, integrated PAP systems implementation, or a fully converged security system that provides a holistic security risk treatment.
B.1.2 Security Survey

- The objectives of the security survey include:

- Identifying critical factors including interdependencies affecting the security of the facility, asset, or operation;

- Developing the security survey into a comprehensive and integrated security analysis and risk assessment across the organization;

- Assisting in the development of enterprise security risk management.
In many organizations, different aspects of security risk management (e.g., PAP, people, information, communications, and continuity management) are managed as separate activities. The recognition of the interdependence of these business functions and processes has led to the development of a more holistic approach to PAP management.

The benefits information and communications technologies provided to PPS can be significant (e.g., in implementation, operability, replacement, and overall cost efficiency); however, this creates additional risks and vulnerabilities to the individual and collective systems.

A cross-discipline and cross-functional risk assessment and management framework that identifies, analyzes, evaluates, and treats all security risks within a singular managed process;
Security convergence applies a comprehensive and holistic view to the converged security risks, enabling a broad strategic approach that encompasses all areas of security risk as well as providing for integration with technological advancements.
Business Support Functions


- Leading associations representing different functions recognise that we need to collaborate more to ensure the business is more efficient.

- Convergence benefits – recruitment, investigations, crisis management, faster response times. Do you know where your people are?

- The need for inter-functional solutions to cross functional problems.
The blended threat

- Can you identify blended threats?
- What can you do to respond to these?
- Common reporting processes. If both teams use the same system risks are more likely to be seen together.
- Duplication, gaps, overall risk is measured and monitored. If different systems then more difficult to prioritise or compare.
Convergence – What can we do?

- So you’re still in the silos and not much happening

- Raise awareness of the blended physical/cyber threat to your business

- New “converged” security policies/strategies and site surveys.

- PSIM and SIEM. Identify risks in real time across the functions. Consider implementing these kind of technologies.
Build Centres for Physical and IT security teams to analyse real time threats. To see the build up and respond before the attack is launched. These space ships are the future of our industry. The need to see cyber attack and physical compromise of building management systems to prevent the destructive cyber attack.
The Future

Could you build such an operations centre? We need to change our whole way of thinking. We have been in the bunker far too long.

Can we rise to the challenge? Please get in contact with us and visit the website for more details.

e) jameswillison@unifiedsecurity.net
http://www.unifiedsecurity.net

Quotes on slides 5 – 14 are from the ANSI/ASIS PAP. 1-2102 Standard.
All pictures are from Dreamstime LLC
Carrying out the PAP Standard (Physical Asset Protection)

ASIS International 12th European Security Conference & Exhibition
Gothenburg, April 14-16, 2013

Volker Wagner, Deutsche Telekom AG, Senior Vice President Group Business Security
Security is a lot.
Standards like “PAP” and “Deutsche Telekom Physical Security” provide guidance.

- Suitable for all businesses and kind of buildings
- Implementation in general and per subject

- Business specific
- Risk- and building related, focus on data centers
PAP provides valuable guidance. 80% - 95% similarities, but different perspectives.

**Contents**
- Principals, leadership, governance
- Documentation, planning, targets, procedures, evaluation, reviews
- Elements: lighting, barriers, intrusion detection, access, entry and access control, video surveillance, alarms

**Structure**
- Organizational issues
- Implementation physical security

**Contents**
- Objective, motivation, scope, roles and responsibilities
- Protection of buildings
- Access control, property rights, fire protection, fire detection, ID-Cards

**Structure**
- Policy physical security
- Requirement physical security
- Additional national documents

- 80% - 95% similarities, but different perspectives
- Both cover physical security as a whole, both are suitable for operation
- Broad approach of PAP versus DT specific approach
- PAP more into details of implementation per subject; DT more into building specifics
- PAP more on processes and continuously improvements; DT more on responsibilities of security, users and facility management
From Risks to Residual Risks. No measures can cover all threats.

**Risks**
Espionage, terrorism, fire, flood waters, burglary, bomb threat, etc.

**Standards**
ASIS PAP Standard, EN-1047-2*, EN-1627** policies and requirements, etc.

**Prevention**
Access control, enclosure, fire protection, awareness campaigns, etc.

**Residual Risks**
Be prepared for treating the unexpected incident

*Crisis Management

* Fire Protection Standard  ** Burglary Protection Standard
Threats to physical assets become true every day.

- **Flood waters in Saxony**  
  August 2010  
  High water flooded a building hosting a switching center  
  2,400 customers could not use the services for nearly a week

- **Bomb threat to HQ**  
  November 2011  
  A bomb threat caused the complete evacuation of a central building  
  6,000 employees can’t work for many hours

- **Fire in switching center**  
  January 2013  
  A fire in a building hosting telecommunication core network elements  
  90,000 customers partly could not use the services for up to 3 days
If your rich uncle (or Father Rhine) has never visited you before – would you be prepared to greet him well?

Flood waters in Saxony
August 2010

High water flooded a building hosting a switching center

2,400 customer could not use the services for nearly a week

- Legal requirements
- Standards & Internal requirements
- Regular Checks
- Contingency Plan
- The unexpected
How can you evacuate successfully if you don’t know where to run to?

- Legal requirements
- Standards & Internal requirements
- Regular Checks
- Contingency Plan
- The unexpected

Bomb threat to HQ
November 2011

A bomb threat caused the complete evacuation of a central building

6.000 employees can’t work for many hours
Why didn’t the fire know that 20 minutes are defined as sufficient reaction time having an early smoke detection in place?

**Fire in switching center**
**January 2013**

A fire in a building hosting telecommunication core network elements

90,000 customers partly could not use the services for up to 3 days

- Legal requirements
- Standards & Internal requirements
- Regular Checks
- Contingency Plan
- The unexpected
You can only protect your business by 100% in doubling your company and cloning all experts.
Comprehensive approach to meet the unexpected.

Key: Sustain the Ability to Decide and to Act

- Early recognition of dangers
- Prevention
- Dealing with security incidents
- Audit and monitoring
Questions?
Security Convergence

ASIS CHAPTER ITALY WORKSHOP

The CSO and CISO : as they are seen by the Human Resources Directors

Milan, 12 February 2013
The CSO and CISO: as they are seen by the Human Resources Directors

- **February 12, 2013 – ASIS Italy Chapter Workshop**
  - Chairman Gensèric Cantournet (ASIS Italy President)
  - Supported by Alessandro Lega (Europe Security Convergence Sub-Committee Chairman)
  - Official organizations attending:
    - AIDP (Italian Association for People Management)
    - FEDERMANAGEMENT (Italian Association of Managers)
    - European Advisory Council of ASIS Europe
    - AFCEA (the Armed Forced Communications & Electronics Association)
    - Odgers Berndtson
    - Cesim - a Singularity Company (education)
    - (ISC)2
  - Active participation of many Security Managers (CSO&CISO)

- **This was the second event on the subject**
  - November 2012 a similar ASIS workshop was held with emphasis on “Head Hunting & Security: Competences and Market”
The CSO and CISO: as they are seen by the Human Resources Directors

✓ The Workshop

- Large number of participants: CSO, CISO and HR Managers
- CSO & CISO figures analysed by the expert eye of HR Directors associated to AIDP and FederManagement
- Identified the main Security characteristics:
  - Participative
  - Integrated
  - Rationalized
- Two way communication, between organizers and participants, confirmed:
  - International need to have a holistic view and approach to Security
  - Harmonising and converging the role and responsibility of both CSO & CISO
  - the need for companies to establish within their own organization the function of Security in an ever more articulate way
  - Security requirements are derived from actual potential threats, vulnerabilities and risks, therefore the security response has to be aligned to the security needs
  - Security requirements should not be addressed as an independent item but within the scope of a wide “security convergence”
The CSO and CISO: as they are seen by the Human Resources Directors

✓ The Workshop

➢ It was noted:

• While there are various organizations in different regions, focusing on particular Security pieces, a global picture does not exist yet. This is the time to pull and converge the different pieces together.

• Emphasized the concept of "centrality" of the human factor, outlining the reciprocal trust that was in place and still needed between the company and the employee.

• There is a need to establish a set of fairly simple collaboration procedures to describe how the CSO & CISO can have their relevant Security standards converged, harmonized and incorporated in the daily business.

• Convergence between CSO & CISO, dialogue between Associations and collaboration between Functions must ensure the protection of company assets.

• The business needs to look out to other possible convergences within the functions being part of the same business organization.

✓ Next Step

• Future meetings are scheduled in the near future and participants proposed to consider holding the next meeting in conjunction with the Financial Directors.

The meeting ended with a wide satisfaction on the progresses made.