Annals of the Academy of Romanian Scientists
Series on Engineering Sciences
ISSN 2066-8570 Volume **2**, Number **2**/**2010**

21st Century Security Manager

Stelian ARION[1]

Rezumat: *Trăim într-o lume a incertitudii care a provocat schimbări majore în paradigmele managementului riscurilor de securitate. Gestionarea riscurilor de securitate la nivelul unei organizații presupune înțelegerea și aplicarea specifică a guvernației securității, a managementului riscurilor de securitate și a rezilienței organizaționale. Managerul de securitate dintr-o organizație a secolului XXI trebuie să stăpânească mai multe domenii de expertiză pentru a gestiona riscurile de securitate. Articolul analizează perspectiva promovării managerului de securitate din persoane cu experiență în administrația de stat, managementul intern al organizației sau domeniul tehnologiei informației, precum și avantajele, dezvantajele și provocările în fiecare situație. Se evidențiază șase zone de expertiză care trebuie incluse în programele de securitate ale viitorului fie la nivelul managerilor de securitate organizației fie în cunoștințele colective ale conducerii organizației. Acestea sunt administrație de stat, securitate organizațională, tendințele de ultimă oră în domneiu, securitate IT, elemente de business și leadership.*

Abstract: *We live in world of uncertainty that generates major paradigms changing that affect security risk management. Modern organization's security risks management can't be done without a profound knowlegde and daily practice for security governance, security risk management and resilience. 21st Century security manager need to deal with several areas of konwledge in order to succesfully manage security risks. The document presents the advantages, disadvantages and challenges for security managers thah have government backgroud, or IT security backgroud, or are promoted from organization's inside leaders. There are six different areas of knowledge that successful security programs of the future must incorporate, either in the knowledge base of their leaders or in the collective knowledge of the leading staff. They are government elements, security organization, emerging issue awareness, IT security, business elements and executive leadership*

Keywords: security governance; security risk management; resilience; security manager.

1. Introduction

We live in a world of uncertainty; the world is changing at even an accelerating rate. Life, society, economy, whether, international relations and risk are becoming more complex. We live in world where, with each passing year, the pass is less and less a guide for the future. The complexity of globalization, public expectancy, regulatory requirements, transnational issues, multijurisdictional risks, crime, terrorism, advances in information technology, cyber attacks, pandemics have created a security risk environment that has never been more challenging. Security is involved in one way or another in virtually every decision

[1] General Manager SECANT SECURITY SRL, stelian.arion@secant.ro

we make and every activity we undertake. The contributions that security risk management makes to society, personal safety and national stability are easy to underestimate but hard to overlook.

Much of the past practices in security have revolved around 'guns, guards and gates', national security, intelligence and defense, firewalls and cryptography. As important as these are, moving from a focus on threat mitigation to benefit realization is a growing imperative for many security professionals and for most organizations.

We expect our governments, organizations and corporations to continue to meet our needs for food, water, safety, lifestyle and self-actualization. This has less to do with the traditional concepts of protection of assets (people, information and property) than it has to do with functions and capabilities that such assets provide. The ability to sustain the capabilities that meets the needs and expectations of stakeholders is not dependent on any given facility, individual or design, rather it is the capability to continue delivery of services or product that is actually the core asset. For example, it is less important to protect an electrical plant than continuing providing electricity to home and businesses. Weather this is achieved by protecting the electrical plant, running several geographically dispersed electrical plants, or having arrangements in place with other electricity suppliers for the time of crisis is less relevant other than choosing the most reliable and cost-effective solutions.

2. Changing paradigms that affect security risk management

Security risk management adds value to operational performance and, if integrated across the enterprise, can become a significant contributor to organizational resilience and opportunity realization.

Less and less organizations consider security as a cost center rather as profit center. Those that have sound security risk management in place will have competitive advantages in many areas:

- Personnel screening can help to select the best candidates and also increase marketability to clients who may be concerned about protecting their intellectual property and founds;
- Information security management helps to introduce products to market without advance knowledge by competitors;
- Appropriate physical security is likely to increase profitability at a venue when customers know they will be safe and their cars will not be vandalized while they are inside;

- Organizations that have prepared by developing a sound security risk management system can quickly and safely deploy to higher risk locations to take advantage of opportunities ahead their competitors;
- Appropriate security means that managers can focus on opportunity realization rather than filling out incident reports or chasing down missing equipment.

Table 1. Changing paradigms that affect security risk management [1]

Criteria	*Old Paradigm*	*New Paradigm*	*21st Century Paradigm*
	Industrial age	Information age	Networked age
Threat source / actor intent	State versus state	State versus state + State versus violent nonstate actors	Asymmetric
Threat source / actor capability	Mobilized national capabilities	Standing national capabilities	Diffused and uncontrolled multidimensional capabilities
Level of social and technological change	Stability	Change	Constant flux
Exercise of power	Control	Empowerment	Governed
Market	Competition	Collaboration	Both
Focus on organization	Things	People and relationships	Adaptive
Social and organizational characteristics	Uniformity	Diversity	Fit for purpose
Organizational assets of value	Physical products	People, physical products and information	People, physical products and intellectual property
Security governance arrangements	Conformance	Passive and centered on compliance	Active board involvement centered on assurance
Security planning arrangements	Best-case scenario	Worst-case scenario	Most credible worst-case scenario
Security response arrangements	Replace	Recover	Resilient
Communication arrangements	One-way dialog (communicating to stakeholders)	Two-way dialog (communicating with stakeholders)	Multifaceted and interconnected

3. Security governance

Boards or their equivalent structures at the head of an organization need to ensure that they have sufficient oversight and knowledge of the respective elements of the organization's security risk management framework to ensure that duty-of-care obligations are met. Providing strategic direction for an organization requires senior managers and leaders to understand what drives the creation of value and what destroys it. That means that the pursuit of opportunities must entail comprehension of the risks to take and the risks to avoid. Risk exposures are becoming greater and more complex, divers and dynamic. Changes in technology, communications, transportation, global financial networks and the rate of change means that most organizations now operate in an entirely different environment from just 10 years ago.

Security governance deals with the processes and management systems within witch an organization operates. The people, policies and processes that provide this framework need to offer managers sufficient guidance to ensure that the responsible persons are both held to account and can make decisions and take actions to optimize outcomes within respective areas of responsibility.

Security governance requires the design and application of a collective of management systems and frameworks that can assist organizations to ensure that all security functions are designed, implemented and operating effectively.

Security governance starts from the top down and sets the scene for a culture of accountability that shapes and empowers responsible and appropriate security risk management practices.

Security management system establishes policies, processes and related controls within and subservient to the security governance framework. The implementation and maintenance of those security controls becomes the responsibility of security operations executives and line managers.

4. Resilience

A resilient organization is one that can achieve its core objectives even in the face of adversity. It enables organizations to adapt and grow regardless of the exigencies, events and risks within their operating environment. The capacity for resilience lies in the culture, attitude and values of an organization. In the modern world, resilience is less about assets, organizational functions or even delivery of products or services than it is about sustaining a desired capability. The concept of resilience lies in focused on securing organizational vision and objectives rather that loss prevention or rebuilding to pre-event conditions.

Resilience is the ability of an organization, individual or community to minimize the harmful of deleterious consequences of disruptive events and to use the event as a trigger to strengthen and develop. The key here is the ability of the

organization to do more that return to the previous level of productivity but learn, recover and exceed the pre-event level. The event may have caused the loss of life and irreparably damaged or destroyed critical infrastructure, property, equipment and artifacts. Examples of such events include the World Trade Center attack of September 11, 2001, Hurricane Katrina in 2005 or the recent sub prime economic crisis. Importantly, disruptive events may be of any scale or magnitude to require resilience, such as structural review, organizational down-sizing, business merger and car accidents. Each of these examples requires an individual, organization or community to adopt or use a resilient outlook to restore stability and progress.

Resilience is less about creating hardened structures and rigid processes or relying on standard procedures and more about developing a flexible, responsive and adaptable way of thinking, behaving and dealing with the impact of change within both the external and the internal environment.

5. Security manager

More security risks are complex, changing and challenging, more the security manager role is critical for the organization. The changing of paradigms that affect security risk management raises the discussion about the security manager education and background.

Law enforcement and military backgrounds, for example, provide knowledge of investigations and prosecutions. IT security skills help in protection of critical information in both digital and printed formats. Business backgrounds help to align security value and business goals. A background career in corporate security ensures a security leader's intimate knowledge of a company. Executive leadership skills produce a focus on business results. Awareness of emerging issues helps to maintain situational readiness. In addition to law enforcement and military skills, a security leader must understand his or her firm's business from finance and strategy to business continuity, competition and profits. The security leader must employ executive leadership skills appropriate to the corporation as a whole. He or she must be able to communicate, manage large projects, create strategies, assemble cross-departmental teams, execute plans and more.

A security leader must understand IT security and must maintain an awareness of emerging issues that may affect the company. He or she must follow legislative and regulatory trends, developments in globalization, trans-national crime, security research and development, and other trends that may one day alter the corporation's fortunes.

Today's most accomplished security leaders point to four general capabilities that define a modern security leader. First and foremost, a security head must understand his or her industry and company. Second, a security leader must

develop a skill set that blends security, IT, business acumen and the ability to identify and evaluate emerging issues. Third, a security leader must change with the times and grow with his or her company. Finally, he or she must possess an imagination capable of exploring for opportunities that will add value to the company.

6. Government background

Many security professionals have some form of government background, such as military or law enforcement experience. Chances are that background has served them well up to this point, but they may well be seeing their career growth stagnating in the face of new requirements for high-level security positions. Military experience has been a staple of security hiring since the 1950s, when businesses sought to bring the military know-how of servicemen returning from World War II into their security organizations. As private corporations adopted physical security requirements similar to those of government entities, the door opened even further for those with military experience. The Cold War may have also fed business interest in the military background. Emergency preparedness and rapid response took center stage, and these concerns remained important into the 1960s. Organizations hired candidates with a military background predominantly for 10 to 15 years. Then, in the late 1970s and early 1980s, many began to focus instead on a background in law enforcement. Contracting and outsourcing had gained popularity in many business models at the time; the new employee was no longer necessarily someone known and trusted, but a potential risk. Companies experiencing more internal theft needed more investigations, and they began to hire ex-law enforcement officers who had the knowledge to root out the internal problems.

The influx of military and law enforcement knowledge into security provided several advantages for businesses and the security industry. At the same time, it had some lasting negative impacts.

Possible Pitfalls are:

- Those with government backgrounds already know the language of security, including standards and regulations.
- They know the tools of physical security, such as cameras and access systems.
- They are well prepared to deal with certain challenges, such as civil insurrection.
- They maintain a strong focus on external threats.
- Law enforcement knows how to plan and conduct investigations.
- They know how to handle evidence.
- They are comfortable in the judicial process.

- Possible negative impacts are:
- Developing and maintaining the extensive physical security programs often proposed by former government professionals may be very expensive for private business because relying on military knowledge alone often leads to an over-reliance on standards. Securing to standards instead of securing against risks that are specific to a business and location can often lead to unnecessary cost.
- Neither approach stresses the involvement of every employee in corporate security. Unlike fire protection and life safety programs, security programs do not require staff to counsel employees on their roles in security, and management is not assigned responsibility either.
- There is often a culture clash between the corporate environment, processes and behaviors and the culture of law enforcement and military security.

Clearly, the government skill-set retains great value for security today. Emergency preparedness, rapid response, risk assessment and mitigation all remain fundamental elements of enterprise security. An understanding of physical security elements and processes will also always be a requirement of a well-rounded security program, no matter how the world changes. Physical protection of employees and assets remains a necessity for businesses, safeguarding not only their profits but their reputations. And the need for in-house investigative skills has likely only increased with the advent of the new federal and industrial regulations of the past decade.

There are, however, challenges for many security professionals attempting to expand their law enforcement or military skill-sets to meet the needs of today's business-oriented security program. Three challenges stand out for security professionals hoping to transition from this background to a broader context:

- New laws and regulations outline detailed physical security requirements that are tailored to certain types of organizations and market sectors, such as banks, hospitals, ports and government facilities. However, it is becoming increasingly difficult to untangle physical regulations from other aspects, for example, information and business requirements.
- The reach and capability of physical security systems and components has blossomed. Data on alarms and system performance is more centralized and accessible; video quality and affordability has increased remarkably; access control can be situated just about anywhere and can incorporate several levels of security. On the law enforcement side, investigations and prosecutions have been significantly complicated by the ubiquity of electronic data; IT expertise is increasingly important in investigations of misconduct and fraud that's based on data that may have been wiped from employee hard drives.

- The recent rash of high-profile laptop thefts has proven that physical security must be in place for information security to be effective. That said, the increasing inclusion of networked components in physical security systems does require a growing familiarity or comfort with information technology concepts.

Luckily, there are a number of major skills that, while not unaffected by the challenges listed above, align with today's business landscape:

- Businesses and public entities have increased their demand for emergency preparedness and response skills since Sept. 11. These skills include risk and vulnerability assessment and planning, program development, training, information dissemination, development and management of drills and exercises, mass notification and casualty management and evaluation of safety and security needs post-event.
- Events occur every day to remind businesses of the continued importance of physical security knowledge, and their awareness is only heightened with the increasing convergence of physical and information security.
- The list of laws, regulations and voluntary guidelines affecting security in all sectors is longer than one might think. Dealing with these requires a strong understanding of the security program and the business, authority within the organization, knowledge of all applicable regulations and guidelines, an understanding of the market sector and industry and an understanding of legal and business ramifications.
- Maintaining a successful security program means creating leaders at multiple levels of the organization. Leadership training calls for strong communication and interpersonal skills, knowledge of the organization, ability to motivate others, being a strong leader oneself, strong decision-making, management and team-building.
- Probing the underbelly of the organization to find internal fraudsters and thieves has, arguably, never been more important. Strong investigations require interviewing skills, fact-finding, information-gathering, impartiality, knowledge of the organization and employees, awareness of privacy requirements and understanding of legal limits and allowances.
- Once investigations are complete, the security professional must know how to assist in effectively prosecuting the wrong-doers.

7. Leaders promoted from inside the organization

Leaders promoted from inside the organization offer several advantages that help them manage security effectively:

- They work within the organization more easily. Internal leaders are able to shift the focus of the security management position from enforcing to

enabling. Because they already know the other executives in the business and understand how the business works, they have an easier time partnering with other units than their predecessors from government backgrounds, who tended to push their agenda through instead of working with others to gain support. It also helped those businesses since the 1980s have begun to encourage the formation of cross-functional teams for significant projects.

- They are able to anticipate new security concerns dealing with asset protection and supply chain management. In the 1980s, when internal hiring was beginning to pick up steam, businesses began to change in another way. Distribution channels shifted away from warehouses to satellites and distribution centers. This drastically impacts business risks and protection needs, and internally promoted security leaders are able to recognize these impacts quickly because they understand how the business ran before the shift. Leaders hired from outside have a much harder time picking up on the need for security to change with the business in this area.

Security leaders promoted from within an organization also suffer some significant disadvantages that can complicate their tenure. They often have little expertise in physical security, investigations or criminal justice**.** In hiring from inside the organization, management has historically gotten what they wanted: a partner and enabler who knew their business. However, they should consider the important skill sets they lose from the government background. Instead of adding knowledge of the organization to the existing job description, they have often scrapped the old requirements entirely, which means many new candidates have no knowledge of physical security, investigations or criminal justice. Unfortunately, the need for these skills was every bit as important in the 1980s and 1990s — and today — as it had been in the decades before.

This means that new internal leaders have to either hire others with physical security and investigations experience or learn it themselves, taking precious time and attention away from the immediate protection of the enterprise. As those hired specifically for their internal experience work to move to the next generation of security leadership, they will experience some challenges. Chief among these is the potential for being blindsided by new trends. These individuals may focus on the organization to the exclusion of other things. They may also spend so much time trying to get the physical security and investigations knowledge under their belt that they forget to tune into management's changing needs and goals for the department. By taking their eyes off future trends, they may miss important business or industry changes that significantly impact security.

8. IT security background

In many organizations, IT security grew into its own entity outside the "security department." This happened in part because the security leaders of the time, who had been promoted through the organization, were, in many cases, caught off guard by the business shift to IT. Many of these leaders were so focused on gaining the security knowledge they lacked that this new vulnerability developed without their notice. Suddenly, it became so large that it demanded attention. By then, the IT organization had created its own security positions — positions that in some businesses eventually outranked the security director to become the leading security offices in the organization.

Those with IT security backgrounds brought valuable knowledge to their organizations:

- They knew the systems, applications and platforms the business needed to perform at its peak in the information age. They knew — or knew how to discover — the vulnerabilities of these systems, applications and platforms, and they knew how to shore them up. Basically, they enabled the business to expand safely into the Web.
- They enabled regulatory compliance. The information security requirements of the Sarbanes-Oxley Act (SOX) and the Federal Sentencing Guidelines gave IT security a leading role in compliance. Their knowledge of the solutions available and in place helped the business comply more quickly, thus avoiding fines.
- They created a large body of standards and repeatable processes that enhanced IT security across organizations.

IT security professionals also brought some limitations to the leading security role:

- They did not enforce punishment for cyber crime. Because IT security professionals didn't have any background in law enforcement or investigation, they did not work to stop cyber criminals from exploiting their networks. Instead, they focused their attention on patching up the system once the damage was done. This held true in the vast majority of the IT community, and it led to a preponderance of cyber crime that was almost social in nature because criminals didn't fear prosecution.
- There was a perception that IT culture didn't mesh with corporate culture. While many IT security professionals interacted regularly with other departments, other executives often observed their high-tech language and unfamiliar solutions and equated these with arrogance or standoffishness. With that said, certain types of positions often do attract certain types of personality, and the IT personality isn't always team-oriented. In fact, communication wasn't a priority for some IT folks, who created their own

space in the organization and often did not venture out to work with other units.

- IT security professionals may also struggle to show the business value of their contribution and may have a hard time communicating how some technologies can save the business money.

Of course, the IT professional's technical knowledge and innovation will be key to securing the business of the future. As more business communication goes wireless and handheld, IT security expertise will become even more important. And since online and digital business applications will likely grow in acceptance, innovation in information technology security will serve the business well. Information protection has been around since sensitive information was first put on paper. It resided mainly in government agencies and revolved mostly around internal movement. That is, files would move about within the organization, but were rarely passed intentionally to external sources. Documents were moved by courier and were stored in filing cabinets, and securing them was a matter of watermarking and carefully controlling access. With the advent and growing popularity of the Internet in the mid-1990s, information protection changed quickly and dramatically. Businesses were already creating and storing digital data, but suddenly these digital information assets could be moved within or outside the organization within seconds. Information technology security grew to include the protection of files, networks, databases, transactions, applications and much more.

Conclusions

21st Century security manager need to deal with new concepts regarding security governance, security risk management and resilience. [1]

There are six different areas of knowledge that successful security programs of the future must incorporate, either in the knowledge base of their leaders or in the collective knowledge of the leading staff. They are government elements, security organization, emerging issue awareness, IT security, business elements and executive leadership. [2]

There are advantages, disadvantages and challenges when promoting security managers from government or IT security background individuals or from organization’s inside leaders. [3]

REFERENCES

[1] J. Talbot, M. Jakeman, *Security Risk Management Body of Knowledge* (Whiley, U.S.A, 2009);

[2] P. Purpura, *Security and Loss Prevention* (Elsevier, San-Diego, S.U.A., 2008);

[3] A. Calder, S. Watkins, *IT Governance – A manager's guide to data security and BS 7799/ISO 17799* (Kogan Page, London, U.K., 2006);

[4] B. T. Bennet, *Understanding, Assessing and responding to Terrorism – Protecting Critical Infrastructure and Personnel* (Wiley, New Jersey, U.S.A., 2007);

[5] POA Publishing LLC, *Asset Protection and Security Management Handbook* (Auerbach Publications, Boca Raton, U.S.A., 2003).