References:

1. Dworzecki J.: *Podstawy prawne wykonywania zadań ochrony osób i mienia. Wybrane zagadnienia*, Gliwice: GWSP, 2009. ISBN 978-83-61401-20-9
2. Korzeniowski L.F. *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS 2008. ISBN 978-83-925072-1-5. **http://www.sbc.org.pl/dlibra/doccontent?id=13871&dirids=66**
3. Lev B.: *Knowledge Management: Fad or Need?* "Research Technology Management", September/October 2000, Vol. 43, Issue 5.

DEVELOPING A STRATEGY AND POLICY FOR ELECTRONIC TRADING SECURITY

Rumen Varbanov,
D.A.Tsenov Academy of Economics (Bulgaria)

This study substantiates and elaborates on one of the crucial issues directly related to the success of every initiative regarding electronic trading - its **security**. This is accomplished along four key lines:

- Giving proof of the significance and trust for the successful development of electronic trading;
- Systematizing and analyzing the dangers in terms of electronic trading security;
- State of the art technologies for securing information security in electronic trading;
- Working out an approach towards the establishing of a policy of electronic trading in small- and medium-sized enterprises /SME/.

Many concrete data and figures are produced supporting the author`s thesis of the incessantly growing dangers in the Internet and of the need for systematic and purposeful work. The risks engendered by the continuous development of electronic trading on a world scale are growing so rapidly that the experts in information security are not relevantly capable of responding to them and assuring reliable functioning of the information systems. This entails urgent development of entirely new methods and technologies for securing the businesses` security in the Web.

We analyze the state of electronic trading security in Bulgaria and particularly the outcomes of the poll

survey conducted by the author with regard to SME.

We examine in detail the dangers to electronic trading at the stages of informing, contracting, delivering of the purchased merchandise, and servicing and maintenance from the perspective of three core aspects of security – confidentiality, data integrity and accessibility. The concrete manifestation of the various kinds of dangers as per their nature is classified in 5 key points: those related to the communication medium; affecting the system`s hardware components; the process of payment when purchasing a merchandise on-line; the cryptographic methods and technologies employed, and other types of danger. We take into special consideration the spam whose impact on electronic trading in the Internet as a whole is becoming incrementally negative and is a real impediment to the traffic in the Web.

Our studies indicate that a big portion of SME which are definitely ambitious to effectively perform in the Web, make effort primarily towards the development and functioning of the site, missing in their strategy the problems of the security of the on-line trading processes. Thus from the very beginning they leave unaccounted for several key requirements for successful electronic trading and as a consequence this has a negative impact on their endeavors. And there are many reasons for one to assert that the information environment of small- and medium-sized enterprises is more vulnerable in terms of security breaches.

We propose an approach for setting up a policy for electronic trading security in SME based on several fundamental assumptions: identification and authenticity; data preservation; processing of orders; gradualness and step-by step proceeding; implementing state of the art technologies and proven decisions based on products of leading firms in the relevant field; protection of investments; protection of transactions.

Finally, several key recommendations are laid out in view of establishing and optimizing a policy of electronic trading security.