GORAN CHAMUROVSKI

EXECUTIVE DIRECTOR OF INTEGRA SOLUTION

OVERCOMMING THE OPERATIONAL RISK IS A SOLUTION FOR INFORMATION SECURITY!

INTEGRA SOLUTION IS PROFILED AS A COMPANY FOR PROVIDING ICT BASED SOLUTIONS AND CONSULTING SERVICES FOR THE INDUSTRIES WHERE COMPLIANCE WITH INTERNATIONAL REGULATIONS IS REQUIRED. OUR SERVICES AND PRODUCTS ARE REGULARLY SUBMITTED TO STRICT EXAMINATIONS BY CERTIFICATION AUTHORITIES AND REGULATORS.

- **You are one of the Sheffield scholarship awardees of (*late*) President Trajkovski. How much have your Executive MBA affected the contemporary profile of the company?**

Definitively, the consistency upon which the company was set up, its perfectionism in regards to offered solutions and services, dedication to clients and internationally recognised services and solutions are characteristics of that education.

■ Which services are offered by INTEGRA Solution in the Macedonian market?

We would not like to limit our solutions geographically, as we are present with our services and solutions in the broader region. The seminar for certifying professionals in the field of information security CISSP, organised by us, was the only successful one in the region, even though it was simultaneously organised in Belgrade and Sofia. Aside from the services and solutions in the field of information security based on ISO 27001 (concerning several regulations and industries, such as Basel II) and overcoming the operational risk in the banking sector (PCI for card base operators, HIPAA concerning confidentiality of electronic healthcare files, SOX Section 404 concerning IT controls of information systems for financial reports), just recently, ten days after the worldwide premiere, we promoted the BS 25999 Standard for Business Continuity. Additionally, our services include solutions for electronically managing business processes in regulated environments, which is the only practical way to achieve efficiency and compliance at the same time. One such system supported an ISO 9001 certification-completely electronic quality management system for all business processes within the organisation, including creation, review, approval and publication of the overall system's documentation, as well as the records and processes ongoing within the company without printing even one hardcopy document. So, there is a certified environment for management of business processes completely realised in an electronic format.

■ What kind of approach should our business entities take when addressing information security?

Firstly, each entity should assess its risk exposure level due to its scope of business activities and should adequately set up its strategy, that is, the level of “risk appetite” for overcoming risk should be declared. Business entities should be zealous in regards to the risk their clients are exposed to, but also in regards to regulatory aspects, that can, aside from penalties and low performance evaluations, fragment and seriously deplete their compliance efforts. Research conducted by The Economist in June 2006 on a sample of 175 senior managers showed that 65% of the entities are audited by five or more regulators and greater than 90% of them stated that regulations will grow in complexity and scope. Therefore, the recommended approach for them is proactive creation of a system that will integrate the efforts for compliance and moreover attain a competitive advantage by introducing integrated controls for mitigating the operational risk. Finally, concerning the industries within which we work, i.e. banking, insurance, telecommunications and the government sector, avoiding one medium impact security compromise is sufficient to make the whole project cost-effective.

■ Would you please explain: How did INTEGRA Solution manage to become the first one in the broader region of South-East Europe (SEE) to certify a business entity for information security within such a complex industry as the banking sector?

Above all, our solution provided a good definition of information security, which entailed not only confidentiality, but also integrity and availability, as well as placing a strong emphasis on the business aspects of information security. Then, Integra Solutions performed a relevant analysis of the operational risk, defined as failure of people, technology and processes specific for the organisation, supported by a business impact analysis and business continuity assessment using a simulated environment of external catastrophic effects. Finally, we employed a systematic approach during the development of the risk treatment plan and introduction of controls designed to mitigate the operational risk. Nevertheless, the adroitness is in the cost-effective integration of controls of the organisation's business processes, since the certifying authority is concerned about the business benefits, i.e. the return on investments, reduction of incident caused damages and business continuity. Defined in such way, our offer is internationally competitive and leads to certain certification when being supported by the top management and the organisation's commitment.

■ Are subjects such as compliance, certification, information security too advanced for us as a society?

Free markets are regulated in order to prevent and avoid deviations that may disrupt their freedom. Almost unnoticed was the appeal of the civil works companies who asked for regulation of the misuses affecting their market. This means that the compliance is already being required in a functional form by the industries, in order to protect the market and establish the competitive basis for provision of services and products, and not view them as a barrier for business operations. Capitalism functions on trust, but that trust is always verified, and certification is one form of verification that excludes the possibility of non-transparency, con-flict of interest, corruption and ensures competitiveness and international recognition. Ignoring subjects related to the level of integrity, reliability and availability achieved within our infrastructures is the most visible way for misuse and abuse to prosper through financial embezzlements, lost and falsified documents in the administration's archives, along with leakage and misuse of personal information. Therefore, dedicated work in this field is a necessity for a contemporary society and, fortunately, our society is starting to realise that.

■ Which approach should be adopted by our institutions regarding the regulation setup pertaining to infomation security?

Global experience shows that regulators monitor the practices of industries; that is, the standards which they established in their operations. So, the standards are not created by governments, but regulators make references to and incorporate them in the by-laws intended to operationalise the legal and fiscal enforcement. Therefore, it is not a coincidence that a number of countries accepted ISO 27001:2005 as a national standard for information security (Ireland, Great Britain, Finland, Czech Republic, The Netherlands, Norway, Sweden, Australia... are only some of them). Hence, countries provide a transparent and solid basis for industries upon which they can build their information security management systems, as well as adhere to the regulations adopted by the country. The regulations specified by the institutions within their competencies are the actual policies they are trying to implement in certain industries. Our good examples include the Circular for the banking sector by the National Bank, which is in essence based on this standard. However, there are several grey areas related to the protection of personal information, where, in spite of the enforcement of misdemeanour sanctions (the legally prescribed transitional period during which the organisation(s) were supposed to comply with the Law on protection of personal information ex-

On the INTEGRA SOLUTION Team

Comprised of senior managers with over 10, 15 years of experience in deploying and supporting critical ICT infrastructures, INTEGRA Solution's Team is its largest competitive advantage, source of success. The collective team talent, knowledge and education are the fabric upon which we base our services and solutions.

pired), our entities are not ready to abide by the requirements stipulated in the Law.

- Many discussions pertaining to the Law on protection of personal information took place. What is your experience with organisations which should implement the provisions of this Law and what is its most sensitive part?

Discussions were carried out, however, one side of the equation, namely the unjustly prosecuted organisations, deems the regulator as a prosecutor. This imbalance usually leads to the worst possible status for the institution enforcing the Law, for the organisations subject to this Law, as well as for the entities who should be protected by this Law that creates an unsurpassable gap among these entities. Provisions for monetary penalties do not significantly contribute to the establishment of compliance among industries, healthcare being the most sensitive sector, as confirmed in a worldwide statistic (CIO Magazine, sample of 433 entities) that showed existence of twice as much Chief Privacy Officers as compared to the industries wide average and that even at that density only 64% of the entities addressed the requirements for protection of personal information in their policies.

The other element is reaching a society wide agreement, that is, the relationship between protection of privacy, preservation of citizens' security and efficiency of the governmental sector. Let us say that presently in London, each individual has their picture captured up to 300 times each day when moving around the city. However, even though the intent of this project was to protect the citizens, on the one hand the citizens have been exposed to the risk of their right to privacy in favour of security, which means that on the other hand the state bodies who possess and process the data should provide a proven capacity to protect the individual privacy and show that they will not misuse this information. This becomes a credibility issue which forces large numbers of government agencies, ministries and directorates to become certified to prove that they will not misuse the given trust.

- Do our regulators possess the capacity to implement controls in the domain of information security and how can they improve it?

The person in charge of conducting information security controls should be given the role and authority of supervisor. In order to achieve that, they should evaluate and define an industry standard set of system controls at the organization under review, where the control framework of that system and its compliance should be the first objective achieved by the regulator at the entities they are supervising. Otherwise, the entities will follow and address the last findings created by the institution establishing the regulation, thus not helping the process of overcoming the risk concerning information security.

When the institution, which is subject to audit, establishes an Information Security Management System (ISMS) the issues become simpler. That is, employment of personnel skilled in the information security domain where auditing techniques are required. Concerning this domain, if institutions will educate their supervisors and certify them the outcomes will be even better. The International Register of Certificated Auditors (IRCA) accredited ISMS Lead Auditor and qualified CISSP practitioners belong to the most renowned specialists in the domain of information security. The US Government, in recognition of the importance of information security (specified as Information Assurance in the USA context) has allocated a budget for CISSP certification of 50.000 employees during the course of next five years. At the same time, it gives our institutions the opportunity to enforce a policy for human resources based on certification and professional improvement, since the salary structure concerning the ICT personnel is currently not competitive.