Interview with Dr. Călin RANGU

Dr. Călin RANGU is director of financial services Consumer Protection Directorate of Romanian FSA, president of Insurance Management Institute, former deputy director of Integrated Supervision Directorate, responsible for operational risks generated by IT and cybercrime. Double licensed in economics and engineering, MBA in banking and finance and with PhD in neural networks applied in financial series processing, Dr. Călin RANGU is lector at Financial Banking University from Romania, MBA lector for City University of Seattle and Romanian Banking Institute, having a broad experience in management, banking, operational risks, IT and financial services, products and technologies.

Dr. Călin RANGU acted over 13 years as CIO in National Bank of Romania and Raiffeisen Bank, and general director of Romanian subsidiary of Raiffeisen Informatik Austria Group. He acts in more associations, being president of Romania-Iceland Bilateral Chamber of Commerce. He published two books and over 100 articles, being organizer or speaker in major Romanian conferences related to financial and banking technologies, cyber-fares and operational risk management.

1. In the autumn of 2014 you organized the Conference *CyberRisks in Financial Services* and the Conference *CyberThreats* with the theme *Cyberthreats between extremes: operational risk management and business needs.* What new elements did these events bring in the landscape of professional conferences?

Conference CyberRisks in Financial Services 2014

The two conferences moved the speeches from the general aspects of information security, aspects repeated to every conference from this field, to the concrete benefits in terms of business benefits, reducing operational risks generated by computer systems, the importance of information protection, identity theft and the need to implement structured processes related to change management and the related specific standards ISO 20000 and ISO 27001.

Conference CyberThreats 2014

Most of the risks are related to company organization or to actually lack of the internal organization of companies, major damage being produced from inside, not only because of external cyber-attacks.

2. The need for a financial CERT correlated with the new legislation related to cybercrime and critical financial infrastructure of national importance was discussed during conferences. Why is it important to establish a financial CERT and how effective would be his collaboration with CERT-RO and other similar structures?

The specific level of this domain, the costs of taking individual measures is very high. Many companies in the financial sector, for example hundreds of brokerage companies of insurance or capital market, can't afford to invest in technology and people specialized in computer security.

The financial CERT should have a preventive and support role of these companies. Cyber-attackers will be always ahead of security measures, most of these measures being reactive.

Because of this reason we need a professional entity to prevent and to combat cybercrime. Anonymous information exchange is very important. When a financial entity is attacked, another one will follow.

3. How urgent the need of regulation of operational risks is, from cybersecurity law to banking and financial sectorial regulations?

Cyber-attacks and losses are constantly increasing. The need for regulation is very urgent as the measures that will be applied will take time, one to two years, they can't show their benefit immediately and therefore we should start early to be prepared in a medium time perspective. A company takes its own measures pretty difficult, especially when it looks at immediate business-case.

Fighting cybercrime is a long-term fighting. Because of this reason the authorities have a role to impose measures and not to expect companies to take them, because they will not get measures until the damage is high.

The most affected are actually business customers, the financial service consumers. That's why the authorities should protect them with regulations, supervision and control.

4. What is the current degree of awareness of the benefits of cybersecurity regulations and the optimal level of security for financial institutions?

It is low because the maturity level is still low. The role of continuing education in the field is very important. It is need for concrete examples, real cases, to perceive risks and to realize the need for action.

5. Cyber-attacks are becoming increasingly sophisticated and most of them are aimed towards banking system. Are you worried about the evolution of cybercrime?

Yes, and not only me. The scourge is expanding. Many actions are taken at the state level, NATO level, so it is a concern that it is extending. As you know more, you understand the implications and the major risk of life of everyone.

6. What do you think would be useful for a faster response in emergency cases, in case of large-scale cyber-attacks?

CERT is probably the best solution, with everything it means, plus the financial specialization part.

7. Few companies have risk management plans or measures for continuity assurance. What factors could cause companies to implement such measures?

Education and the concrete examples. Examples can be obtained by requiring penetration testing, ethical hacking. When the manager will see how you can steal money or substitute identity with criminal connotations, he won't stay without doing nothing.

8. Customers want to use their bank cards to make purchases, pay bills or book directly from the Internet, with maximum safety. Persons that do such banking transactions are exposed to risks?

They are exposed to risks because identity theft is on trend, but there are insurances from banks that if they follow some minimum safety rules (not like you give

to somebody else the PIN code), the banks will assume the risks, will take the losses and customers will not have to suffer.

9. You will continue the series of conferences in the field of cyber risks and cyber threats in finance field? Can you describe some of the most interesting topics of the following events?

I think it's important to continue, the conferences *Cyberthreats* will reach in 2015 the eighth edition! Points of interest will be the interests of the market. It is an area where new things occur annually. The attackers don't let us get bored. And as we know more, more needs have to be done.

Many European regulations appear and these regulation have to be implemented, not only formally. In this case it is necessary to debate them. There are many things to do to protect the financial services consumers. The level of practical and behavioral education, for entities that provide services and for clients and beneficiaries, has to be increased. I think there are still many things unsaid in this area of prevention through approach and the behavioral education in cybersecurity field.

Interview made by Ioan-Cosmin MIHAI
Vice President of RAISA