Mr. Timur Khrotko: I am Russian, born and currently living in Budapest, Hungary, but visit Russia often. I was educated as an economist and have a Ph.D. in organizational management and environmental problems. You can find my book on Amazon.com, but it is untitled at this time and still in progress. In the security field, as an economist, I am deeply involved in information technology as viewed from an organizational or business perspective. I have extensive experience in constructing, project management and negotiations. I view OWASP and its challenges from this organizational perspective also.

Summary of Community-Submitted Questions and Answers

Question: What is the biggest challenge you see for OWASP?

Answer: To gain broad adoption of Top 10 as a requirement in verification quality control, application procurement, and certification of software production; make standard requirements more adaptive, more accessible to require, and to fulfill, based on different situations; have more emphasis on tools supporting the security requirement definition and contractual implementation.

Question: The mission of OWASP is to make software security visible so that individuals and organizations worldwide can make informed decisions about true software security risks. How do you see OWASP furthering its mission in the next year, and what about in the next five years?

Answer: That mission is completed. Software security is visible, thanks to hackers. As a result, there is application security work as a side effect. Next, OWASP must change to organizational decision-making and priorities, focusing more on non-visible items such as stakeholders, budgets, corporate governance, compliance policies, perception of issues, habits, and other embedded issues.

My proposal: Make Top 10 more accessible as a requirement and certification criteria; develop tools supporting Top 10 adoption in organizations; support brokers who help organizations adopt Top 10-like requirements; and produce written material to promote corporate understanding that security and quality is important. OWASP should also rethink the mission of chapters, add more brokerage activity, and have ready-made guides to assist them in fulfilling their initiatives.

Question: If elected, how will you prevent conflicts of interest between OWASP responsibilities and the duties of the organization where you are employed or active?

Answer: There is a basic conflict of interest for most of us, since we are engaged in professional for-profit work in the field of application security. I would say that in most cases, the OWASP representative and the broad-project professional is not a conflict of interest per se. There should be conscious representation of professional identities and they should not be blended in any one project. For example, I will be holding an OWASP workshop soon, using my OWASP identity. Though what I say will not be biased by my business interests, my motivation to spend time on non-profit activities is for most part practical. I gain a respected position in the application security field, so can expect more profits than if I remained a for-profit player only. I guess that this is applicable for most of us; our motivations are not altruistic only. So this is my point of view on this issue.

[End of Audio]

Timur Khrotko