Timur kHrotko

**1. If elected, what would be your top three priorities for your first year on the board?**

#A) To create common understanding among the stakeholders of the Foundation regarding the contemporary mission of the community, its initiatives, the projects we promote and fund. #

The mission may not be about the visibility of the software security (it is visible enough now), rather about practical accessibility of the preventive appsec measures. Accessibility to the real world organizations who are not much disposed to adopt appsec practices. Accessibility in terms of coverage and ability to deploy.
One challenge is in that a lot of security aware effort fails on managerial and contractual negligence regarding appsec. Another challenge is that an average software developer is not disposed to devote much time to security. I believe raising awareness does not change the situation much. This negligence is not evil, it can coexist with rather conscious understanding of risks. Security is not practical, it's not payed for, it's an obstacle in the normal business process.
In order to be more successful in our efforts we must package the security aware approach into easy working practices. Practices more easily adoptable by business organizations and bureaucratic institutions. Requirements more accessible for managerial decision making and more controllable by legal instruments. And practices more usable by developers. By practices I mean requirements packaged into uncomplicated guides and templates (see T10 cheatsheets as an example, see Application Security Procurement Language). By practices I mean turnkey installable tools accompanied with dead easy guidelines, youtube videos, active support communities and well known prescription regarding when to use. By practices I mean replicable patterns of security aware behavior in the business process and behavior in the development cycle.
We probably have to make the standard requirements more adaptive, more accessible to require and to fulfill. For example T10 can not be an annex to a general software vendor agreement, it is too complex to comply with and too strict as an obligation, especially when sanctions are imposed. It can be our job to make T10 variants for the real world contracting.
Projects such as the CISO guide are very important, though has to be reviewed with usability in mind.
And probably we have to be an ecumenical movement, cooperate with non-web requirements (eg. CWE 25) and to promote initiatives of others (eg. MS SDL).

#B) Make OWASP propaganda more popular. #

Do we have popular animations or similar easy materials on youtube (presentations do not count)? Yes, some. But we have to build up more professional propaganda regarding the cause we care for, promoting T10, explaining our portfolio of solutions, making our accessible practices visible. (professional: see FTCvideos.)

#C) Review the practice of project making. #

The practice of making collaborative projects has changed in the last couple of years. Hype is generated via fb. Code and coders meet on github. Answers to developers' questions concentrate on stackoverflow. Okay, we have internal google apps and g+ community, and wikimedia still

rules. But to attract general public, businesses and developers we need to add social and html5 sugar to our projects, their packaging.

**2. What is your style for dealing with complex situations that may impact many people or where other decision makers hold differing viewpoints?**

Collective decision making itself is about differing viewpoints and interests of stakeholders. My style of dealing with differing viewpoints can be confrontative and can be caring. It may depend on the iteration of a decision making: after being introduced to the problem I usually declare my point of view and tend to formulate it provocatively, and I can insist on my viewpoint unless convinced regarding the flaws in it. I will represent my differing view further if the choreography of that decision making is that I'm to represent that important aspect (security for example). But if we are to conclude to a decision, I will turn to absolutely constructive strategy, since the decision is a collective, consensual product. I can be empathetic, especially if the other viewpoint is represented by a powerless party. Decisionmaking is an interesting game.

**3. Describe your experience leading organizations. Were they non-profits or community based? Please explain both your role and the nature of your involvement.**

I have never been in charge of a larger organization. In past ten years I was leading small businesses, always focusing on information security, be it a vendor developing and supporting its own IdM solution used by a large corporation, or an appsec consulting company. Being the leader of Hungary Chapter is my first engagement in a non-profit organization.
It might be important that I am a researcher too. My PhD research was too folded, partly it was about seeking a way of nesting environmental friendly patterns of behavior into corporations, and partly it was about researching the importance of dispositions in decisions of senior executives (I suggested that changing their dispositions can make corporations care about the natural environment). So as a researcher I acquired certain experience regarding how to approach non-profit requirements in business organizations. And I have certain knowledge about the workings of leadership.
In the micro circumstances of my functioning as a leader I try to apply my managerial studies. I always try to apply my organizational approach in enterprise security, and I look at the corporate situations I get involved in and people I work with through my researcher's glasses as well.

**4. Describe your most successful contribution to the OWASP community (Project, Chapter, Conference, or other).**

My most successful contribution is in the close future I hope.
The Hungary Chapter was created by my friend Bálint Szabó, I took over the chapter as he left to Brazil this April. In May due to certain circumstances I had to organize two OWASP events simultaneously almost on my own, a conference and a CISO workshop. The conference attracted about 50 visitors, lasted 4 hours with 8 presenters, we discussed several aspects of how to make "hacker-resistant" software, and the feedback was positive from both, audience and speakers' side. Next day morning at the same conference room of KPMG we held a joint event of KPMG, OWASP and ISACA moderated by me. It was a round table for CISO-s, where our role was to facilitate their dialog about the current issues they face, the topic was appsec-centric. Now we

are holding the second such event, now the topic will be vendor management. And if it is the beginning of a regular CISO meetup, then a significant contribution to it might be mine. If not, then it was a nice try. )