

PenTest

magazine

Vol.2 No.5 ISSN: 2084-1116
Issue 05/2012(13) May



Cloud Pentesting

**WOMEN IN IT SECURITY: NATALYA KASPERSKY,
DEBBIE CHRISTOFFERSON AND VAL RAHMANI**

TURNING A CLOUD INTO A THUNDERCLOUD
PENTESTING IN THE CLOUD
RISKS IN CLOUD COMPUTING
BEHAVIOUR-DRIVEN SECURITY TESTING

“Do what you know well, believe in success and be stubborn”
Natalya Kaspersky,
InfoWatch Group of Companies
CEO, Kaspersky Lab co-founder



Natalya Kaspersky is a co-founder of Kaspersky Lab, one of the world’s largest antivirus companies, and CEO of InfoWatch Group of Companies, specializing on developing software solutions for IT security. Natalya’s global business and IT-marketing expertise helped make InfoWatch market leader in the Russian DLP market and continually expand its global operations. Today InfoWatch Group of Companies sells its products in more than 10 countries, including Germany, Switzerland, UAE, India, Saudi Arabia, Bahrein, etc. The Group also includes „Natalya Kaspersky Innovation Center”, which creates and develops new technologies for further submitting to the Group to commercialize. Natalya Kaspersky is active in Russian and international business community life. She is a member of several IT committees of Russian governmental organizations, a member of Board of Directors of the German-Russian chamber of commerce, and a member of the Russian-British chamber of commerce Advisory Councils.

You are an accomplished entrepreneur in the field of IT Security. I am certain our readers would like to know more about your educational and professional background.

Natalya Kaspersky: I was born in Moscow, in 1966. Graduated from Moscow State Institute of Electronic Engineering with a master’s degree in Applied Mathematics. Later on I got a bachelor’s degree of Business Administration in The UK Open University.

In 1994 I came to work for then a big Russian computer company KAMI, to the antivirus department which then had only 3 programmers. My task was to start regular sales of antivirus product. The total sales revenue at the time I came in represented \$ 100 a month. In 2 years we reached revenue of \$100.000 a year. It was enough to open our own company, while Kami at the time got huge problems and had no resources for the antivirus anymore. We named the company Kaspersky Lab and I became its’ CEO.

We were extremely lucky to grow together with the antivirus market as it was at its’ initial stage. So, by the time

I left CEO position in 2007 Kaspersky Lab annual revenue reached \$128 Mln and annual growth was of 159%. Now Kaspersky Lab is #4 vendor in the antivirus world.

In 2003 I initiated the set-up of a daughter company InfoWatch, which focused on developing solutions to protect corporate confidential data. That was a completely new area, where nobody yet worked at the time. We didn’t know if the idea of internal protection would work or not, so created it as a separated company. Fortunately for us, IDC in 2005 announced segment of data leakage prevention (DLP) to be a separated segment on the market. In 2007 I bought from Kaspersky lab the majority of InfoWatch and became its’ CEO.

You were the co-founder of Kaspersky Lab and the company was built with no venture capital. Please, tell us how the company has grown since 1997.

NK: The company has seen four main waves of growth.

First period – Technology Licensing. In 1997, we concluded two contracts to license our technology: with Finnish company F-Secure, and German company G-Data. In essence, these contracts enabled the company to survive its first year of business. I was lucky to convince our Finnish partners to pay us advanced royalties. So, every month, F-Secure paid Kaspersky Lab USD 10,000: at the time, that was enough to ‘feed’ the team of 16 people. Soon we recognized that the technology licensing business is very profitable and decided to concentrate on it.

In three years, we changed the conditions of our contracts, removed exclusivity and took the decision to enter the US market by offering not the branded products, but our AV technology (the engine). Our first attempt did not followed by much success. We resolved the problem by hiring the ‘right’ person and our business took off, securing the company’s future for the years to come.

The second wave was the formation of KL partner network. I began search of resellers for KL business very early – in 1994. We started with small companies. Large distribution companies got no interest in reselling our products: We had no brand and no money for marketing. Over time, some of our small partners either grew with us and became big or we were forced to replace them. And soon bigger distributors started to demonstrate an interest in Kaspersky product, so the size and efficiency of our dealership network grew significantly. In 2001, we had moved to a two-tier distribution system: a distributor with a network of resellers underneath. Such a system allowed us to substantially scale up the business.

Third wave of growth was our extremely successful entrance to the retail market with the ‘boxed’ product. We agreed with first retail distributor in France WSKA to launch our boxes in retail stores French-wise in 2002. In 2003 we made an agreement with even bigger German network.

The launch we made in spring 2004. This moment was luckily coincident with McAfee move out of European retail. McAfee decided to concentrate on the on-line sales, the places on shelves left open. I often think that if we did our ‘retail move’ later or earlier we would get such superior start as we achieved in spring 2004. Of course we had no idea of McAfee plans, it was pure lack.

As a result – in just 2 years Kaspersky lab became #2 in European retail market of AV products. Based on this success we rolled out the retail model to the other countries. And I have to say, it was much, much easier to agree with large retail networks by showing them the success story in Europe. Without it I don’t think we could get up to the 2nd position in AV retail world-wide by 2009.

The fourth driver of Kaspersky’s business growth was geographical expansion, which we also developed in several stages. At the initial stage (1997-2000) we

gave some of our distribution partners a right to use our trademark and so become our representative at the market. For example, Kaspersky Lab Polska or Kaspersky Lab Benelux were not Kaspersky Lab subsidiaries, but distributions partners with the exclusive rights to sell our software in their respective countries. At the beginning of 2000s I recognized that the partner model was not going to bring us quick money. So, we opened our first 100% daughter company in the UK. With that one we made all the possible mistakes, but got an incredible lesson in building of international operations.

In 2001 our new Chinese partner suggested us a new model – Joint stock company, which we opened in China in 2002, in Japan in 2004, in Korea in 2005. The Korean office was our last JSC. Since then we only opened our own subsidiaries: 2000 in USA, Ca; 2003 – in France and Germany; 2005 – in USA, Boston, MA; etc. By 2007 we had 8 local offices in different countries all over the world. They significantly increased our brand power and formed out our sales systems in those countries. We enjoyed multi-digit growth in all the countries with local offices, what of course gave a big push for KL in general.

Over the last 4 years, there have been two major growth drivers for Kaspersky Lab business: retail sales and territorial expansion. The company managed to become #2 in retail AV market world-wide, next to Symantec, and covered all the major international markets. By the time I am writing this both have exhausted the possibilities for further growth. Obviously, the company needs new drivers and new opportunities. What would they be – is the task for the current company management.

Could you share some details about your current company and some of your partnerships locally and globally?

NK: InfoWatch was founded in 2003 as a Kaspersky Lab subsidiary. The idea to create DLP (data leakage prevention) system actually came not from the market, but from the technical side. We just acquired Anti-spam technology from another Russian company and thought that if we could use the technology to filter the information to the company, why could we do it for information which goes out of the company? We made a prototype, it seemed working and then decided to establish a separated company because I wanted Kaspersky Lab to be purely associated to what we did the best – antivirus.

By 2003, InfoWatch already got a product and its first client. DLP market was announced two years later when we established InfoWatch. Even the abbreviation ‘DLP’ was only coined by IDC analysts in 2005. So we were really the initiators and one of inventors of this market. In Russia, InfoWatch established the market for

protecting corporate information from internal threats, and only 2-3 years later other players began to appear.

Today, over 150 companies in Russia and the CIS use InfoWatch's solution, we occupy the leading position in these regions. And now we are conducting an active expansion campaign to the Arabic countries. Here we once again play the role of pioneers: the market in the Persian Gulf countries is still at the very early stage of development. In this region, InfoWatch has a strong unique competitive advantage in supporting linguistic engine for the Arabic language.

Unfortunately, the DLP market itself is very narrow: not all the companies need DLP protection. Our prospects are either large enterprise with multi-thousand employees (to save personal data) or companies with string trade or IP secrets.

By analyzing the size and the speed of market growth in 2009 we decided to expand our business into other areas. As the most relevant for us we've chosen two areas – social media monitoring and protection for endpoints at enterprise.

The first one we addressed by creating a joint company KRIBRUM together with another Russian vendor Ashmanov&Partners. As for the second we simply acquired a small but active German vendor cynapspro GmbH, which we recently renamed into EgoSecure GmbH.

What are some of the challenges you face running a company in Russia?

NK: Well, I read horrible stories about Russian business in 90s. As for us we never experienced those type of problems. Probably, the IT sector was too intellectual to interest those with criminal ties.

On the other side, that time there were no any favorable conditions for the software business in Russia, like they do exist now. The thing we still lack is a particular business environment with investment money available for all stages of the company development – from start-ups to the internationally growing companies.

In Russia such investor communities are only starting. But starting quite active and rapidly, so I believe the situation for the Russian R&D companies might change quickly. At the moment I know several seed funds and angel investor communities, which invest into the start-ups. On the other side, several foreign and Russian VCs are working with the second stage companies. Also, the government started to play active role in these investments. Take as an example Skolkovo Technopark, which gives grants to young R&D companies, or Russian Venture Company, which invests into new technologies. However, there is lack of support for "mid-size" companies, when a business has outgrown the idea stage but doesn't have money for expansion and marketing. It is difficult

to attract funds for such businesses because investors struggle to evaluate their prospects and future returns.

Few months ago you acquired a German GmbH Cynapspro. What value has this acquisition added to your portfolio?

NK: The acquisition of the German company was motivated by several factors. The first one was a chance to entry the SMB market. Cynapspro (now EgoSecure) has about 800 SMB-clients in Germany, Austria and Switzerland.

So, the second objective was to break into the European market. InfoWatch's previous attempts with DLP solution did not have success due to the specific European legislation, which protects employees' privacy in the working place. So, DLP-like software meets the active opposition from local trade unions. The third factor was a significant expansion of InfoWatch Group product's and technology's portfolio, which allows us to exchange of the technologies, and to save cost on R&D.

Because the segment is different we didn't want to put all the solutions under one InfoWatch brand and chose a new neutral name EgoSecure. We presented the new brand and the new version of EgoSecure products in Hannover, at the biggest IT-exhibition CeBit. They called lots of interests. Many visitors noticed unique client-oriented approach of the new EgoSecure product, which is still rare in IT-security market.

We also managed to bring in big distributors from 7 different countries. They got very interested in reselling EgoSecure in their countries. So, I am quite optimistic about EgoSecure future.

You were elected to the board of Russian-German Chamber of Commerce. Please tell us about your responsibilities in that capacity.

NK: I have been the Board member for 2 years, the maximum term, which is allowed for the position. This March the Board was re-elected and now I am dealing with *Russian-German Chamber of Commerce* (AHK) on a less formal basis. My responsibilities were like in every Association – to participate in the Board meetings, approve the new AHK members and make the decisions on the question raised for the Board. For me it was an interesting experience plus a good possibility to improve my German.

What in your opinion are some of the biggest cyber threats?

NK: Our company is doing constant analysis of the following accidents: leaks of important information from companies, and increasing risks coming from the usage of the social networks.

Let's start with leakages... Once every six months, InfoWatch analysts conduct research on ? data leaks, which were ever published in open sources. According to the latest research, we see an increasing number of leakages across the world. For 2011, we recorded 801 instances where companies or government organizations lost confidential information, whereas in 2006, the figure was around 200. But I'd like to stress that this is only the top of the iceberg: we gather the only incidents which have been reported to the press, what represents roughly 1% of the actual number of leaks.

Regarding the social networks. They are a new phenomena in our life and no surprise that many companies and hackers started to use them with negative purposes. Having so many subscribers social networks carry dangers for both ordinary users and businesses. For example, negative PR about a company raised by a competitor and spread through all the social media like Twitter, Facebook, blogs, forums, etc. Unfortunately, the result of such an attack might be much more effective than through press.

We first met these type of attacks 3-4 years ago and decided we must do something about it. This is how we came to the idea of social media monitoring service, which now is calling Kribrum and successfully sold both in Russia and Gulf areas.

What are some of the important skills you look for in an IT Security professional?

NK: It all depends on what particular kind of professional we have in mind. IT specialists must know about infrastructure, managers must have good technical knowledge and an ability to manage projects, programmers must be able to write code, know the languages and have a creative side. Of course, all professionals must have a certain set of skills and knowledge.

You are multilingual, how has that helped you foster business relationships all over the world?

NK: Of course it helped me a lot because international business always requires good knowledge of regional culture, mentality and often local language. In the making of Kaspersky Lab we had to continuously learn how to improve our business knowledge and studied the languages of the most promising markets.

As a self-taught entrepreneur, what tips would you offer our readers who want to follow your footsteps?

NK: I don't have a recipe for success in business. It is impossible to come up with a kind of universal set of rules which will transform a start-up into a multi-million dollar

company. To give an advice one needs to know details of the market, the business, the economic environment and the other circumstances of the company business. As for people who are just thinking to become an entrepreneur I could only say – do what you know well, believe in success and be stubborn in the luck will not come immediately.

Men are still said to be a majority in the field of IT Security. What are your recommendations to involve more women in this field?

NK: Well, I am afraid to disappoint you, but I tend to believe that it is not necessary to create any special conditions for women. Business is a competitive environment, and any added limitations or quotas could only bring additional difficulties. I am not sure that involving more women into the field would somehow help to IT-Security in general. So, why than we would need it?

What are your predictions about the future of the IT Security market?

NK: In my opinion, the number of leaks, harmful programs, instances of all types of electronic fraud and reputational risks is only going to grow. The reason is simple – the fraud of electronic data or money through electronic sources – is still cheaper than any other so called 'normal' fraud. But the probability to be caught for e-crime is much lower than the same for the normal crime. Unless this trend won't change we will see rapidly increasing number of different type of e-crime and e-fraud.

This means that the interest in IT security software and protection systems will increase, and the security market will grow. As a result of the popularity of social networks, the demand for the reputation control products, such as KRIBRUM, will also grow.

You are a very busy businesswoman, how do you strike a balance between your personal and professional life?

NK: When we started selling our first antivirus I didn't have much choice. The nineties were hungry years in Russia and we had to work hard to earn money. That time both my mother and my mother-in-law helped me a lot with raising my two sons.

Today the situation in the country and in my family is different. I have 2 small daughters, but I also have good facilities and nannies who help me to raise them up. Also, my husband is a very careful father and a good supporter for the family despite the fact that he as myself is a successful IT-entrepreneur. We both do business and take care of our children together.

Interview done by Aby Rao