Software pioneer InfoWatch outlines the country's high-tech future at VTB Capital's RUSSIA CALLING! forum

by Elliot Wilson

Trailblazing software specialist InfoWatch has long been one of Russia's brightest tech-sector prospects. Spun out of software giant Kaspersky Lab more than a decade ago, it now bestrides the industry, helping leading Russian and global firms to combat cyber-attacks and protect against internal breaches. We spoke to InfoWatch CEO and founder Natalya Kaspersky about the firm's – and Russia's – increasingly bright future.

Few entrepreneurs truly push back the boundaries of a product or service in any given country or region. Even fewer are capable of spotting the niche in an existing market, and then having the belief and the drive to exploit it in order to create a new global industry, virtually from scratch. Natalya Kaspersky is one of the very few.

Natalya Kaspersky, InfoWatch Talking at VTB Capital's annual RUSSIA CALLING! forum, the chief executive of InfoWatch describes how she was among the first people to spot the rising threat presented by cyber-attacks, and how they could be used on a grand scale to target not sovereigns or consumers, but the world's leading corporates.

By 2003, after stepping back from Kaspersky Lab, the international software security group she co-founded, she understood all too well the importance of defending companies against cyber-attacks, using a new form of technological defence called data loss prevention (DLP) software.

Thus was born InfoWatch, which detects potential data breaches and prevents them from happening, while also working as a pre-threat detection system, ensuring that attacks are deflected or repelled (by stiffening up an organisation's internal defences) often even before the perpetrator has thought them up.

InfoWatch's customers differ from Kaspersky Lab's in every way. The latter's roster of clients are typically consumers or very small enterprises seeking low-cost answers to retail problems such as computer viruses and malware. "[Whereas InfoWatch] works mostly with very large firms and enterprises, providing them with tailored and highly sophisticated data protection systems," says Kaspersky.

"The companies we work with range in scale from 5,000 staff all the way up to 100,000 employees or more. Our roster of clients includes many of Russia's largest firms, as well as an increasing number from around the world."

Many of these globally oriented Russian firms, and the international investors who hold shares in them, were in attendance this week at VTB Capital's RUSSIA CALLING! forum in Moscow.

To many, the importance of DLP software may seem clear-cut, given the spate of recent and highly damaging security breaches that can imperil even the largest corporate's global image and reputation. One obvious example was the external November 2014 hack of Sony Pictures Entertainment, though less high-profile attempted hacks that target prominent corporates occur virtually every day.

Yet when InfoWatch was set up, says Kaspersky, "the DLP industry didn’t exist anywhere, either inside or outside Russia. It’s surprisingly advanced now in Russia – there are around half a dozen vendors selling highly sophisticated software, more than any other country."

Part of the reason for this is InfoWatch itself, she believes, adding: "We popularised DLP software in Russia, and explained it so well to our customers, that everyone started to realise that there was a genuine need for enhanced content security."

One of Kaspersky’s early challenges with InfoWatch lay in explaining to doubting CEOs why they needed additional security measures to combat cyber-threats. Many viewed this is an unnecessary and additional cost burden, though that myopic thinking has now been all but eradicated. Corporate chiefs worldwide now understand the threat, and are willing to pay InfoWatch for its world-class services.

An industry that didn’t exist a decade ago is worth $800 million and growing fast. Last year in Russia alone, the market grew by 35% in revenue terms, aided by sleek new software upgrades and rising fears of a new Sony-style hack attack.

Another shift in thinking has come as corporate chiefs recognise and accept the prevalence of another form of cyber-threat: the one that exists internally, perpetrated by a greedy or disgruntled member of staff. This 'Trojan Horse’ attack, wherein the embedded employee damages the firm, is far from new, yet it has long remained surprisingly hard to anticipate or detect.

Advanced DLP software has made huge strides in this territory, helping to target the weak points within corporate superstructures and to identify where internal attacks or breaches are most likely to occur.

This sort of sophisticated bulwark against organised attacks is paramount, Kaspersky believes. "Firewalls do not offer real protection," she says. "We analyse what it is inside that companies don’t want outsiders to see."

It was once startlingly easy to crack open a company’s shell, yet firms are now becoming wise to the problem. One of the biggest threats lies in the medical space, where life-sciences and pharmaceuticals firms, and the makers of complex medical machinery and chemicals, own patents and products that are worth millions and even billions of dollars.

The straight-talking InfoWatch CEO’s eyes twinkle when she talks about the company’s future. Having sold all her shares in Kaspersky Lab in 2007, she has become the embodiment of Russia’s high-tech economy. Lean, efficient, well managed and increasingly international, InfoWatch – many of whose clients attended this week’s RUSSIA CALLING! forum – is at the cutting-edge of Russia’s high-tech sector: a pioneering enterprise carrying its own banner, and that of the country in which it was founded, far into the future.

Since founding InfoWatch, Kaspersky has expanded into, or bought assets in, countries including Germany and Canada. Kaspersky Lab’s holding operations are now located in London, but InfoWatch’s outright owner (the fast-growing private firm has no other shareholders than the founder herself) maintains that she has no interest in locating her firm anywhere but in Russia.

There are good reasons for this. Russia is still InfoWatch’s largest single market, as well as offering a vast repository of highly skilled and affordable engineers and data experts. "It’s not hard to find the right people to employ here," Kaspersky says. "We can get good staff here, and that is a huge advantage for us.

" Growth also means expanding both locally and globally, from an already large base. "We are growing in two ways," she says. "First, we are pushing further into the domestic Russian space, where our business is growing at double-digit levels, and where we are already the unalloyed leader, with a 60% market share. And with import substitution under way in the country, many leading Russian firms are switching to our software.

"I can see good opportunities in many other markets too, from the Middle East and Asia, to Africa and Latin America. InfoWatch is active in India and Malaysia, and we are now expanding into Indonesia. And we are creating new products based on our existing software products and models, which cater to medium-sized firms, which will help us grab a bigger market share, both in Russia’s growing economy and around the world."

Source