INFOWATCH®
WE WORK TO PROTECT

Ph.: +7 (495) 22-900-22
+7 (499) 37-251-74

Russia, 121357, Moscow,
29/134, floor 7, Vereyskaya street
BC "Vereyskaya Plaza"

www.infowatch.ru

Putting a stop to cyber attacks is all but impossible
While security is still not priority for most businesses, bad guys gain upper hand

Natalya Kaspersky is one of the most accomplished executives and investors in the global cybersecurity community. She co-founded Kaspersky Lab in 1997 and served as its CEO through 2007.

Kaspersky then moved on to become CEO of InfoWatch, a group of German companies that supplies enterprises and small- and medium-size businesses with endpoint and data leakage protection technologies. In 2012, Kaspersky acquired a 17 percent stake in G Data Software, a long-established European anti-virus company, and joined G Data's board of directors.

ThirdCertainty sat down with Kaspersky at G Data's recent 30th anniversary event in Bochum, Germany. The mathematics graduate shared some of her frank views on cybersecurity blind spots still prevalent in the corporate realm. Text has been edited for clarity and length.

3C: Have company decision-makers begun to take IT security more seriously in the past year or two?

Kaspersky: I don't see significant improvements. The board of directors and the top management, especially, always have something else to do, and security is not the No. 1 priority. They always think the business is more important. Quite often they start to think about security only when an accident happens. Then they ask, 'Why haven't we been protected?' And usually the answer is, 'You didn't (provide) the budget,' so that's why.

3C: Meanwhile, the bad guys keep innovating and advancing.

Kaspersky: We still witness plenty of virus attacks, and G Data rejects many of those daily. But also we see more targeted attacks, where an enterprise is being attacked from different angles. Quite often the attackers use insiders to get internal information about the organization. They use any method that allows them to go through, and that's very dangerous and something that is very difficult to protect.

One of my companies recently found a massive targeted attack, which developed very quickly through the whole network in a large Russian bank. We called them immediately. They didn't have a clue. They had an anti-virus system installed; they had everything installed. But that attack was specially developed against this particular bank and used the vulnerabilities that the bank had in its IT systems.

3C: Protecting the network perimeter is hard if you aren't clear where the perimeter begins and ends.

Natalya Kaspersky, Kaspersky Lab co-founder and cybersecurity expert

Kaspersky: Right. The Bring Your Own Device trend is abbreviated BYOD. I like to read that to mean Bring Your Own Disaster. At the moment there are 4,500 different devices with different operational systems. People come with their own devices, and they're unprotected. This is a big hole in the enterprise protection.

The cloud is another big problem. When you put your information into the cloud, you actually don't know what happens to this information. You may feel more secure if you encrypt it, of course. But even then, there could be a man-in-the-middle attack, or some other attack, so the information goes outside of the cloud.

3C: But we rely on cloud services. Companies like Google have made it very easy.

Kaspersky: And they do business on that, they sell you the goods through Gmail. Basically they monitor what you're writing and get advertising. That represents another problem with the security of personal information and identity security. Somebody knows everything about me, or too much about me. Of course, many people would like to maintain their privacy, but they don't even know that their privacy is somehow violated.

3C: And the cloud also provides more avenues for data leakages.

3C: You've been in the security game a long time. Where are things heading?

Kaspersky: Honestly speaking, we are losing the game. The black side is working faster, and they are always one step ahead. That's the problem with any protection methods and software and tools. It didn't get better, unfortunately. I would love it if it got better, but I don't see any trend.

3C: Getting back to company decision-makers, do you see any signs that they could become more proactive?

Kaspersky: I think there is a need to teach them. We need to somehow change this prioritization in the minds of people; maybe then the world could be become better.

3C: Aren't security vendors, your companies included, trying to help close the gap?

Kaspersky: Some time ago, I had an idea when I sold my Kaspersky shares, I thought I would create the company that would protect against different threats. We searched the trends and found the threats we thought would be the most popular. And we were trying to find the protections against those.

And now I understand that that’s a game that is impossible to win. Because there are more and more new technologies, and with any new technology, there are new threats. And you need to have another solution to protect against this new, particular threat. Unfortunately, the efficiency of the security software—I can’t say about the total protection, which includes services and organizational methods—but the security software is less and less effective.

3C: What can be done?

Kaspersky: I don’t know what to do. Maybe in the future I can invent some other new other way. But I think the security industry stands in front of a big challenge right now. We’re not able to effectively deflect the majority of possible threats. And we need to somehow change ourselves, maybe invent new solutions, and maybe do some absolutely unexpected steps in this fight, because we are not winning.

Source