IT professionals play a key role in protecting IT resources, however, when making misuse of their knowledge and rights, they could form a huge security threat. To counter security threats and decide upon the best protection at company level, we should learn to involve cross-departmental IT teams. But, protection does not only consist of a selection of tools and their design. That's why I dare state "Tools are not the solution, you are!" The purpose of this series of articles is to trigger your thoughts and senses about security activities at company level. I would like to create awareness about the importance of going beyond team boundaries in order to stay ahead of the game. At the same time, I will provide guidance on how to foster connectivity across all teams dealing with security activities, and overcome the intradepartmental Conflict of Interest within a company.

We built fortresses and dressed our IT infrastructure in armour

It's hard to deny: today's IT defenses are under heavy attack. Not only did our opportunities to exploit IT as a product grow significantly, so did the possibilities to attack IT and reap the benefits of someone else's data. IT is all about data and who owns and controls that data. Data is worth gold.

While IT evolved, our defenses often remained at medieval security level. Before data started to grow on us, we shielded any attacks from the outside in an ancient way: we built fortresses and dressed our IT infrastructure in armour, just like medieval knights; we relied on our technical shields and tools like firewalls, hardening, dashboards, and the like -all based on the principle to shield and protect specific attacks from outside our premises, and to protect our property.

You might want to think this metaphor does not affect your line of work. The environments you take care off may be defended "ninja style": with inner strength, which is the best and most flexible defense mechanism, since you don't rely on external shields, but on your own capabilities instead.

Although these ninjas are much more sophisticated than most knights, their defense mechanism won't stand the current attacks either. It is still based on the principle of protecting the property, which in current times is still worth defending. However, the attacks focus on the treasure: the data itself. Given the latest news, you must be aware your data is not as protected as it should be.

We might have misjudged the impact

In the past ten years, our world of IT and its interactions have shifted more and more across all kinds of infrastructure, intelligent devices and gadgets. Its interconnectivity has evolved rapidly, to the extent we no longer have the control, nor the overview. We might have misjudged the impact and we seem to be running after the facts to try and get IT back in control.

I believe it started to get out of control with the rise of smartphones and tablets, combined with companies like Google and Apple, who started to shift the concepts of IT and its data. They transferred knowledge gained from our personal data into service offerings. Not only to facilitate us but to benefit from it as well: our data became a new product in itself. But no free service comes without anyone benefiting from it.

While we aimed our fights and battles against the bad and ugly outside our premises, we got more and more vulnerable from the inside through our smart devices and gadgets. And, we were not prepared, because our dashboards showed lovely green, measuring the state of our fortress instead of our treasure.