Sietse van der Gaast, submitted august 2013, theme issue on Security

Insider trading by outsiders

When we consider the protection of company confidential information, security as a concept is almost outdated. It is almost impossible for a company to hide information, and there is a high chance that promoting real security will be labeled as a waste of money or as trying to hide something that is possible illegal. Whatever you do, you can count on the fact that someone tries to make money with your information. Confidential, or not.

We all profit from the internet as a worldwide cloud of knowledge, information, interesting ideas and banal entertainment, and as an opportunity to stay in contact with old acquaintances or to make contact with new strangers. Because individuals and companies like to make use of these services, this also creates opportunities to collect information about these consumers, citizens and companies. Why would anyone collect this kind of information on a large scale? Because this is very useful from a commercial, business strategic or security point of view, and also because collecting, storing and analyzing data becomes cheaper and cheaper. People nowadays seem to care less that personal information is available for third parties. They think that they are seen as anonymous users and that they have after all, nothing to hide. Companies are in general more reluctant to share information but also there the reality of information security is a lot less strict than the company policy aims to achieve in theory. Most companies would not think of sharing their organizational structures, department names and locations and employee details with the world, but nowadays websites such as LinkedIn receive this information up to date from the employees themselves. I suspect that confidential company (or customer) information is sometimes - by a considerable percentage of employees - sent using non-company email accounts or using free web storage sites like Dropbox, translated using a free translation program because it is so difficult to find a translator on short notice, or converted to another data format using a free program or web service. With the chance that the information can be seen and analyzed by others.

I think that large internet players, especially by combining different sources of information, can obtain a detailed and real-time view of the situation inside a company, even in matters that would be classified by a company itself as strictly confidential. It may even be the case that there are internet players that are more aware of some aspects of a company than upper management of that company itself. Already money is made using publicly available information for 'high frequency trading': using fast automated analysis of, for example, company news on internet stock is sold or bought. It is not unlikely that this is also possible – and even more effective – when also not-public information on companies can be taken into account.

Governments that analyze even larger amounts of public and private data for instance in order to counter terrorism theoretically can obtain an even sharper and more complete view of what is going on inside and between companies. After all, if dozens of terrorist attacks can be prevented by storing and analyzing large amounts of data then a range of other applications is also possible: I presume the average employee is likely to be less careful than the average terrorist.

Insider trading, the trading of a public company's stock (or other securities) by individuals with access to non-public information, is illegal in many countries. But can non-public information be sufficiently protected? What if stock trading based on company confidential information is done by people that have no relation with the company in question whatsoever, people living and working in countries where that information should not even be in the first place? Automated trading (in not too large quantities to avoid suspicion) of company stock based on the information of large amounts of confidential information seems to me a very lucrative business opportunity, especially

when you already have access to the necessary information. The main questions are: is it possible, is it allowed and is it already happening? I am convinced that it is theoretically possible. If it is possible, and it is allowed, shouldn't inside trading then also be legal? So for this moment it seems only logical that it is illegal. If it is possible but illegal, how can we detect it so it can be prevented? To me that seems very difficult. Possibly governments can monitor companies and individuals to detect such behavior, but governments are likely not to focus on suspicious trading which is only harmful for foreign companies or individuals. And how can misuse by browsing governments themselves, or their employees, or their employees' families and friends effectively be monitored and stopped? In the US an attempt is made to prohibit inside trading by government employees, and to make such trading transparent: the 'Stop Trading on Congressional Knowledge Act, or STOCK Act'. However, opinions differ whether this law in its current form ensures that this kind of inside trading can be detected and countered.

But all this complicated reasoning only stirs up unnecessary turmoil. We have to assume that in friendly nations with access to valuable and confidential information of our citizens and companies no government employee has ever done - or will do -funny things with that information just for his or her own benefit (also not sneaky), or to make this data available – on purpose or by accident – to third parties. And if such undesirable situations should happen, this probably will be detected and made public by governments and secret services, and those affected will be properly compensated. It is just a simple matter of trust.