Protecting Digital Personal Information from the Company Point of View

Abstract

Companies' IT systems manage personal information of different types that require different measures to protect it. The first difficulty that a company should address is to discover and map the personal information that is managed by its IT systems and to devise policies and procedures for the personnel to process it in such a way to reduce the risks which could occur from breaches or involuntary disclosure.

Companies have always managed personal information, both of customers and of personnel, but in recent years due to the fact that most information is in digital form and managed by IT systems, the risks involved in managing it have increased enormously and very fast. At the same time, companies have not fully realized what has been happening: on one side, managing in digital form personal information made it faster, cheaper and has introduced new approaches and new uses. On the other side, if the information is easier to access, and it also means that it is easier to "lose".

From paper to digital

To better understand the new risks, it is useful to consider what has changed. A few years ago personal information managed by companies was mostly in physical (paper) form like contracts signed, dossiers on personnel etc. It is true that some information was already managed in digital form, but now all information is in digital form and collected in few large systems or databases. Today it is much easier to make a copy of the information since it is not needed a physical work, like making a photocopy, but it is enough to give a command to a computer; it is much easier to transfer the (copy of the) information in very short time and, thanks to internet, anywhere in the world. Finally, due to how easy and fast it is to copy and transfer digital files, instead to copy a single document it is convenient to copy and transfer the full database and afterwards to search it

for the information of interest.

The same tools provided by the digitalization of information that make it so useful and so easy to access the information, are the same which create the new risks of "losing" the information.

By "losing" the information we mean any treatment of the information which was not intended by its owner or which could provide damages to the owner of the information or the company that manages it. Recently there have been many incidents in which information has been stolen from the IT system of companies by hackers, thieves, organized crime, political opponents, competitors etc. In this cases the information lost by the company has been voluntary stolen by someone with intent to damage the company directly or indirectly, even just by making public information which should have remained private and damage the brand name.

In other cases the information has been made public, by mistake, by the company itself. But it makes a very big difference if a single (paper) dossier is left on a desk inside the company, unguarded so that anyone passing by can pick it up and read it, or if the entire database containing all information about the company is publicly accessible by anyone in internet, that is in the whole world.

New types of information

Another important point, is that the information collected in a company has increased vastly: not only there is all the structured information that was present also before, but also most of the internal and external communications that before were mostly verbal, in first person or by telephone, now are in digital form like email, chat etc. Again this is very useful for companies since history, data, information of communications are stored and can be searched, retrieved etc. At the same time, this information becomes part of the digital information of the company, whereas before it was not.

But the information stored is not only of the company, that is business related: it is quite normal that company personnel uses some IT instruments, like email, also for personal reasons. In many cases the companies themselves suggest their employees to use their own mobile-phones and smart-phones for work, called Bring-Your-Own-Devices BYODs, or employees work at home using telephones, PC etc. both for work and for personal use.

In this way the type and amount of digital information about employees and customers collected by companies has increased greatly in the last years.

Today companies collect customers' information also in new digital-only form. This information comes for example by tracing people, customers or potential customers, when they visit the website of the company or they display the digital advertisements of the company. Information is also collected by having people registering on the company website or app even for free services, and having people follow the company marketing on the social networks.

Most of the time when people, customers and employees, have information managed and stored by the company, they expect that the information is kept private, at most shared with other business associates, but surely not made public on the whole internet.

In many countries this is also a legal requirement where laws require companies to treat personal information according to some mandates and to declare publicly or inform directly those interested in case of a breach and of a disclosure of information. Usually these laws go under the general term of "Privacy" legislations.

Protecting which information?

The first problem for a company is to understand that the issue of protecting digital personal information is real, it is not only a compliance issue but it is a real business risk.

Given this step, which is fundamental and requires the awareness and intervention of the top management, the second problem is to understand which digital personal information is present in the IT systems of the company, including IT systems of providers and outsources. Indeed from the point of view of the user, and often also of the law, it does not matter too much which is the IT system that manages the data, but it matters which is the company that has collected it from the user since in case of breaches it is who has collected the information that will be responsible towards the final user. So if a company collects some personal information of customers or personnel, even if the data is managed by some other company, it is in principle responsible for the treatment of the collected information. Vice-versa, a company can collect personal information using the services of other companies (this is very common with on-line we services) and again it is in principle responsible for the treatment of the collected information.

So the first hard problem is to draw a map of all personal information which is collected directly or indirectly by the company and that it is managed and stored either in-house or by providers and outsourcers.

It is also extremely important that this map is updated regularly. A nice way of doing it is to be sure that each IT project small or large and each modification to the production IT services which modifies the treatment of personal information, automatically updates the company map of the personal information, for example by hooking it into the IT Change Management process.

At first sight this could look easy to do, but in practice very seldom works as expected. Often after an initial success, the managing of this map is forgotten and in short time the map does not correspond any more to the real situation.

A very difficult problem that each company has to solve is the level of detail to which to map the personal information. There is no general solution for this, each company has to find and adopt the best approach for its own purposes.

Finally notice that this problem is strictly related to the "data classification" problem of IT security, which is a kind of mythical "Holy Grail" of all IT security management processes and it shares with it most of the difficult issues.

How can we protect the personal information?

The first step is to understand which personal information is managed centrally by the company and by its providers and outsourcers and which personal information is managed directly by the employees or the customers somehow avoiding a central management control.

On the personal information that is centrally managed by the company with its IT systems, the first issue is to decide if it really needs to be collected and processed at all. Very often personal information is collected because "it is there and it could possibly become useful one day". This argument has its own value, but it should be always complemented with a clear understanding of the risks of collecting, processing and storing this personal information.

So the question which should be asked is: what would happen if the company collects this personal information and due to a breach or any other reason, one day it is made public? Does collecting this personal information add some new risks or increase existing risks?

The answer is usually "Yes", which means that collecting personal information which has zero or almost zero value and use for the company is most likely difficult or impossible to balance with the risks it creates or increases. Then the simplest way of managing these risks is not to collect this personal information or to collect it in anonymous statistical form.

At the other end of the security spectrum, there can be personal information which is too valuable to be managed in the company's IT systems. Also this crucial personal information must then never appear in digital form.

For the personal information which is then collected and managed by the IT systems, based on a risk analysis, the company should introduce protection measures which can include for example:

- procedures for the personnel to collect and process it;
- compartmentalization of IT systems and restriction of the personal information to only the few systems that are needed to manage and store it;
- encryption at rest and / or in transit of the personal information;
- advanced authentication and authorization procedures to access the personal information;
- secure document management, data loss prevention, digital rights management and intellectual property protection systems;
- etc.

Personal information not centrally managed

But the real issue is how to manage and protect personal information which is not centrally managed by the company and how to control the associated risks. This is the most complex and most difficult area to approach mostly because it is very seldom structured and well defined.

A first type of personal information which falls into this group is all the personal information which is given to the company by external people, for example customers and supporters, and that the company must somehow manage. We can give some examples of this kind of personal information.

Many companies have on-line services to support their customers, a very common service is a “chat”, another a “board” or a “blog”. In practice people external to the company can write a message, which can be private to the company employees or public to the whole internet, describing a situation or a problem and asking for support, or giving an evaluation on a company's product. Through these on-line services it is quite possible that unstructured personal information of external people is uploaded to the company's IT systems and managed and stored in them. The company's IT systems usually require external people to accept the company's conditions of use, privacy and other

legal requirements. Still the external person expects and feels that her personal information given to the company will be treated at least in a fair way and protected with the appropriate measures.

The same is true for all the personal information that can be associated to the company and present in the social networks. This point would require a specific and detailed discussion which we will not look into here.

Similarly emails are a vector for the arrival of personal information in the company IT systems from external people. Information of all kind and types is found today in emails and emails are one of the biggest targets for breaches. How can personal information be protected in emails when most often we are not even aware of its presence?

Emails are one of the most difficult form of personal information to manage: not only a company can receive information from external people by email, but also they are used often by internal personnel also for private purposes. Indeed most of IT devices can be used by company's personnel also for private purposes, in particular if the company allows Bring Your Own Devices (BYODs) and remote- or tele-working. Thus on the company IT systems are present both company information and personal information of the employees and their family, relations and acquaintances.

The first step to manage all this personal information is to map, even not precisely, the type or category of information and the IT devices and systems that can manage it.

Then policies must be enacted which instruct the company's personnel on how to manage this personal information. This is right now the most important point since each individual company's personnel should recognize the value of each personal information and treat it accordingly. The company's personnel should in practice implement a hand classification and sorting of this personal information, in accordance with the company's policies, and in case distribute or assign the personal information to the corresponding IT systems which can manage it appropriately.

To implement these policies, the company should organize the IT systems and devices in such a way as to render easy, not only possible, for the company's personnel to manage the personal information. A very crucial issue is the usability of the IT solutions adopted: if they are not intuitive and easy enough, with time they will not be used and the personal information will be distributed in unknown ways in the IT systems.

As one can see, the biggest issue at the moment, is to find ways to classify and organize the personal information in such a way that it is possible to manage it appropriately and protect it

within the company's IT systems.

As mentioned above, many technical IT solutions are available, from encryption to compartmentalization, to data loss prevention systems or digital rights management systems but we can efficiently adopt them only after we know where the personal information is and we have decided how we should manage it.

Andrea Pasquinucci (PhD CISA CISSP)