Security, Risk Analysis and Governance: a Practical Approach

Managing the security of today ICT systems is becoming a daunting job. A few years ago ICT security was mostly a technical job: it meant configuring firewalls, applying patches, checking that the configurations of the applications were done according to security guidelines, being up-to-date on known vulnerabilities and so on. These are all technical tasks left to security technical experts.

But in a few years the situation has changed dramatically:

a) the security level of systems and applications has greatly improved, most of the low and medium risk vulnerabilities have been fixed

b) security devices and applications have improved tremendously, now they offer a wide range of functionalities and are reasonably easy to use

c) today attackers are not anymore *script kiddies* but real criminal, mafia organizations or disloyal employees who act with economical purposes

d) the economical value of today's electronic transactions is enormous, indeed there is practically no economical transaction which does not require at some point a digital processing.

If from the technical point of view the security of ICT systems has greatly improved, looking at it from the point of view of business, that is of the economical risk, the situation today is by far more risky than it was a few years ago.

The Human Factor

The culprit of today situation is *man*, that is the user of the technology. Indeed as we well know, ICT technology has not developed to the point of being completely intuitive and trustworthy, and systems which are so complex will probably never be such. So men must *understand* and *learn to use* the technology.

Just to make an obvious example, it is enough to think about phishing to realize that the problem is

not so much technical but instead is human. Indeed fraud is probably today the biggest ICT security concern, and fraud is perpetrated by using the technology as a means to reach the person target of the scam, the technology is not itself the target of the attack.

The appearance of the user in the ICT security scenario is completely disruptive. Not only we have to deal with the technical issues of managing the machines and applications, but also to create human procedures, teach them and verify that users correctly follow them. This is not a technical issue and does not have a single solution, but each case, business, situation must find its own. All we can do is to follow general approaches, guidelines and best practices which help us in establishing case by case, company by company, business by business what it has to be done.

Indeed recently *Information Security Management Systems* (ISMS) like BS7799/ISO27001, ISM3 but also ITIL, COBIT, CMM, ISF and others have received a lot of attention. On the other side problems like 'which rule to add to a firewall to permit or block a particular traffic' are by now restricted to a few technical experts.

Managing Today In-Security

We all very well know how security should be approached in this wider scenario. Since absolute security does not exist, we have to reduce the risks so to be able to accept them (or transfer them). We have to remember that a security system costs and that the protection should not cost more than the value of what is protected, and so on.

Thus the idea is to find the weakest points, secure and control them, since we cannot secure and control everything. In other words, we should start from a risk analysis to be able to manage the risks. The general principles of risk management are simple and clear, but when we have to put them in practice things become immediately very difficult.

In some particular kind of business, like financial or insurance companies, the core business itself is the management of risks, so all processes are present in the company to evaluate and manage also the ICT risks.

But in all the other cases the situation is often quite different. Usually the management has a good understanding of the business risks in their field, but disregards all what is not core business. In particular in the case of Small and Medium Businesses (SMB) this is quite understandable, since often there are not even the resources or the costs would be prohibitive for making a risk analysis.

For example, most of the Italian companies are small, and they do not even have an IT staff. Often all of the ICT services are provided by external companies, and usually not a single provider as it would be in a kind of small outsourcing business, but many small external providers each realizing a little part of the ICT system of the company. It could be seen as a disorganized and fragmented total ICT outsourcing. But the company does not have any internal ICT expertise and is not able at all to approach an ICT risk analysis. The outsourcers are not interested in providing as an extra service the risk analysis because is expensive, is not understood by the customer as a need and it is simpler and more economically convenient to just sell some direct services. Moreover if something happens, every outsourcer tries to shift the responsibility on the others so that at the end nobody is at fault.

Even in medium and large companies, where IT staff is present, ICT is not perceived as a fundamental *service* which enables the company to exist, but more like an important machinery.

Too often, also in the personal experience of who writes, to solve a security issue the management is ready to buy an expensive device of a well known brand but is not willing to look into the management and the procedures adopted for the company information processing, even if this could cost much less and be much more effective.

A fundamental concept which unfortunately has not yet been understood by most managers is that ICT security is not anymore a technical service provided by some hardware devices, but it is a process which involves the full company.

A Practical Approach

So we have to accept that traditional risk analysis and governance will be restricted to a small

subset of large companies. For all the others it is probably better to follow a different approach (see e.g. [1,2]). For medium and large companies, a practical approach has been summarized as follows [1]:

1. due diligence
2. compliance
3. enablement.

In other words, the risk analysis can be built starting from:

a) the best practices in ICT security adopted in your own business field

b) the laws, regulations, certifications, international standards etc. to which your company is subjected or that it wishes to adhere to

c) the fact that adopting the previous measures and processes can give a competitive edge to your company with respect to the competitors.

From best practices, compliance to standards, laws etc. it is usually easy to extract an empirical risk analysis for example following a *Capability Maturity Model* approach [3]. In this way we do not get quantitative results so to be able to give an economical value to all risks, but we can understand how developed is the security management in the company and which are the most critical areas. For example, if most of your competitors adopt advanced procedures and encryption systems for the backups and you don't, it probably means that your backups are subjected to very high security risks.

In this way it is possible in a reasonably easy and not expensive way, to discover the areas which are more likely to have problems and high security risks. Moreover it is also easy to communicate the findings to the management since they will not be based on technical data but mostly on comparison with competitors, laws, standards and regulations.

But if you want to know for example what is the exact economical risk in not encrypting your backups so to be able to evaluate precisely the value of the countermeasure, then the classical risk analysis restricted to this particular issue should be performed. But this is often not necessary

because the management will fix a maximum budget to cover this risk based on overall business considerations, and accept whatever risk remains without knowing the exact value for it. This usually makes sense from a business point of view and in any case the management is taking the responsibility for it and managing the risk.

Down to Small Companies

The approach that we just described works for medium companies and in some cases also for large companies, but it is still too complicated for a small company. In small companies where often there are no ICT resources of any kind and the management is often also the owner of the company, we should take an even more simplified approach. (There are of course notable exceptions to this situation, for example small IT or risk consulting companies.) A practical approach could be to look at ICT security and risks from the point of view of processes present in the company. It is a kind of simplified version of best practices integrated with law and regulation requirements. By comparing the situation in the company with these general procedures that should be in place, it is possible to understand the level of risk and the maturity of the company in managing its ICT processes.

For example [4] proposes 11 controls divided in 3 groups of importance and listed in decreasing order:

<u>Gold Group</u>

1. network security
2. virus protection
3. backup procedures

<u>Silver Group</u>

4. file access privilege controls
5. IT as part of the organization's long- and short-range plan
6. IT continuity and recovery plan

7. identification and authentication procedures
8. management support/buy-in

Bronze Group

9. risk evaluation program
10. general employee IT security training program
11. data input controls.

By verifying what is present in the company about these controls, how they are managed with respect to the business of the company which can increase or decrease the level of risk of each one of them, it is possible to make an overall evaluation of the ICT risks and of the controls which require more attention.

If the theoretical goal would be to have all these (or similar) controls covered at least to some extent, in practice the more common situation in small companies is to stop at the first two not even completing the Gold Group.

Indeed it is not difficult to understand why small companies stop already at backups. Today the basic functionalities of network security and anti-virus are provided by devices and software present in every company, department, office and house. Indeed even home users have adsl or cable modems with a basic firewall and an anti-virus installed by default by the vendor of the PC. The important point is that the basic forms of network security and virus protection are provided only by technological tools which require practically no human intervention. But for backups we need the participation of the users, in this case the owners of the data, since today's information is dispersed in many different places and devices: from the office PCs to the portable PCs, smart-phones, USB keys, portable disks, mp3 players and so on. Technology is not able yet to manage automatically the backup of data residing in so many different places, so human intervention is necessary and when man comes into play, problems are inevitable.

If we consider the next controls, the ones in the Silver Group, we see that the human role grows and becomes more important in each subsequent step. For example at first sight it could seem that the

fourth control, “file access privileges”, is a purely technical issue, but actually it is quite the contrary. To impose an effective control access on digital data, it is necessary to have at least:

a) an inventory of possible kinds of information present in the IT systems

b) a classification of the information according to business and security value

c) a clear specification of users' roles, duties and privileges

d) a personnel organization so to implement a even minimal kind of separation of duties.

It should be obvious that if users' roles are not specified and there is not a even minimal form of separation of duties, it is not possible to impose control access on digital data, since in practice it ends up that all users have access to all data, and worse still all users are administrators of their PC. So if everybody has access to everything and everybody can manage at least her/his own PC, file access privilege controls cannot be imposed. This is not to say that the first two points are easy to implement, but being of a more technical or practical nature, there is a bigger chance that they can be realized.

Conclusions

The more relevant role of the user in the security of ICT has changed the way in which the associated risks should be evaluated and managed. In most situations it is not possible in practice to follow the traditional approach to risk analysis and management. We need to develop more practical and effective approaches which will make it possible to govern not only the technological aspects of ICT security but also the company-wide processes of Information Security Governance.

Andrea Pasquinucci

PhD CISA CISSP

http://www.ucci.it/

References

[1] D.B. Parker, *Making the case for replacing risk-based security*, ISSA Journal, May 2006

[2] R.S. Lindberg, *Nimble Risk Management*, ISSA Journal, August 2006

[3] Capability Maturity Model, http://www.sei.cmu.edu/cmmi/

[4] B. Busta, K. Portz, J. Strong, R. Lewis, *Expert Consensus on the Top IT Controls for a Small Business*, ISACA Information System Controls Journal, 6, 2006