

Information security

– what kind and how much is enough? –

Initiated in the '60s, the extensive use of computer networks has grown exponentially with the industries, especially in the past few years. Needless to say, so have the incidents of data breaches, information losses, and other security issues. Internet applications, as well as internal networks, are used more and more extensively by companies from all areas of the economy (financial, healthcare, education etc.) as well as by government (military and administrative institutions).

A large number of these institutions deal with personal information, like social security number, bank accounts, and so on. An even larger number (since it includes the first category) deals with corporate-specific information (from employee files to new project development plans, new product budgets, research results, merger and acquisition information for future events, and other documents that would hurt the corporation if destroyed or made public). There's also the military-tactical sector to be considered (usually top secret data). Except for this last category, all other information is usually either processed at the company level or outsourced to another country in order to save costs.

Logically, there's an increasing trend of protecting this sensitive information against various events, like data destruction or information theft just to mention a couple of the existing threats¹. For the first one, different storage media have been developed over time. For the last one, the debate over what should be done to better protect personal data is far from being over. It addresses the network security (firewall, antivirus, intrusion detection system etc.), the protection of data transfers (different methods of information encryption), the software vulnerabilities on any given network, ("bugs" in the application layer that could lead to data loss or facilitate information theft), as well as the human factor (corporate rules-of-the-house for employees' usage of internal information resources).

Hard issue

There are many products available, there are many articles, blogs, forums, discussions, studies – a simple Internet search will return results in the millions numbers – yet supposedly secure information still gets lost or stolen.

This indicates there might be an issue in one or more of the following:

- in the information available on the protection option (for instance, the company trusted a software provider's information in the selection process for the best feasible option – and they could've done better). This happens mainly in smaller businesses, that don't have sufficient funds to spend on developing data security and don't always have very knowledgeable IT people. Bigger companies tend to use more money and resources on finding a good protection measure or even creating their own.
- in the implementation process (ranging from insufficient authentication or authorization in the login process to software bugs that permit outside attacks). At the beginning of last year, Apple's Safari Web browser had a flaw that could allow a hacker to take control of a computer by persuading a user to view a specially crafted Web page².
- in the actual usage of the security measures (for example, an employee forgets to turn on a firewall, or uses a proxy to navigate on a corporate-blocked web site that would install spyware on the host computer – and there could be many more examples here as well). There are even lists of ideas³ about what to do in order to facilitate personal use of company computer with little or no respect to the implications over the corporation's security.

For one thing, most of the information available on the subject comes from vendors of various kinds, which means that data isn't complete (or not necessarily accurate) and questions the usefulness of this information. With this paper, I intend to put together different options of securing information systems and create a reference, along with my recommendations on the problem.

Who cares and why?

In general, the stakeholders for the information security are represented by any institution that handles personal, proprietary or confidential information (as well as by those affected by a breach in the security system). The reason is – to put it in very simple terms – that any organization would have something to lose if this information is in any way affected.

Without trying to be exhaustive, here's a list of the most commonly encountered costs associated to data loss or theft:

- if information was lost or destroyed
 - o costs for retrieving or re-creating the lost data (sometimes impossible to achieve)
 - o legal costs for losing proprietary data
- if information was stolen
 - o competition might get a hold of it and tactically use it against the source company to achieve a bigger market share or even to determine the bankruptcy of this competitor
 - o customer identity theft could happen, along with "regular" data loss, in which case the company may be subject to legislative sanctions for not protecting sensitive information
 - o proven vulnerability, especially if there have been repeated breaches, show that the company can't be trusted with sensitive data. This in turn will usually lead to less business flow, fewer clients and customers, and probably a drop in the stock

price (depending on how big the impact on the overall company trust was affected). The stock price seems to be more likely to fall if confidential information was leaked through the breach⁴.

Any combination of these effects, and others not mentioned here, would simply underline the importance of a well-thought and correctly implemented and applied information security policy.

If the elements of the information security issue are fully understood and applied, here are some of the possible positive effects:

- the company will ensure a better protection against threats
- the loss and theft of information will be eliminated, which in turn will increase the profits by correctly utilizing the resources (toward profits, not for recuperating lost data)
- as a result, more customers and clients will want to do business with the company in the long run, since the better protection will in turn lead to a comparatively higher level of trust.

If, on the other hand, this issue is either not understood or not applied (in most cases, one implies the other), all the negatives from the ideas above might or will happen.

In the case of a partial implementation of information security, the company might actually have a lot more to lose: there's wasted money on the implementation (since it wasn't complete, it didn't do any good), together with the typical loss for the damage (which could come from loss of clients, liabilities from legal proceedings and regulatory fines and so on).

Resources:

- 1) *** – “Computer security threats classification”, CACI Information Assurance (<http://www.caci.com/business/ia/threats.html#Malicious%20Threats>)
- 2) Vauhini Vara – “Tech companies check software earlier for flaws”, May 4, 2006, Wall Street Journal (http://online.wsj.com/public/article/SB114670277515443282-qA6x6jia_8OO97Lutaou7Ddjz0_20060603.html?mod=tff_main_tff_top)
- 3) Vauhini Vara – “Ten things your IT department won't tell you”, July 30, 2007, Wall Street Journal (<http://online.wsj.com/article/SB118539543272477927.html>)
- 4) Ross Anderson, Tyler Moore – “The economics of information security: a survey and open questions”, University of Cambridge (<http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf>)