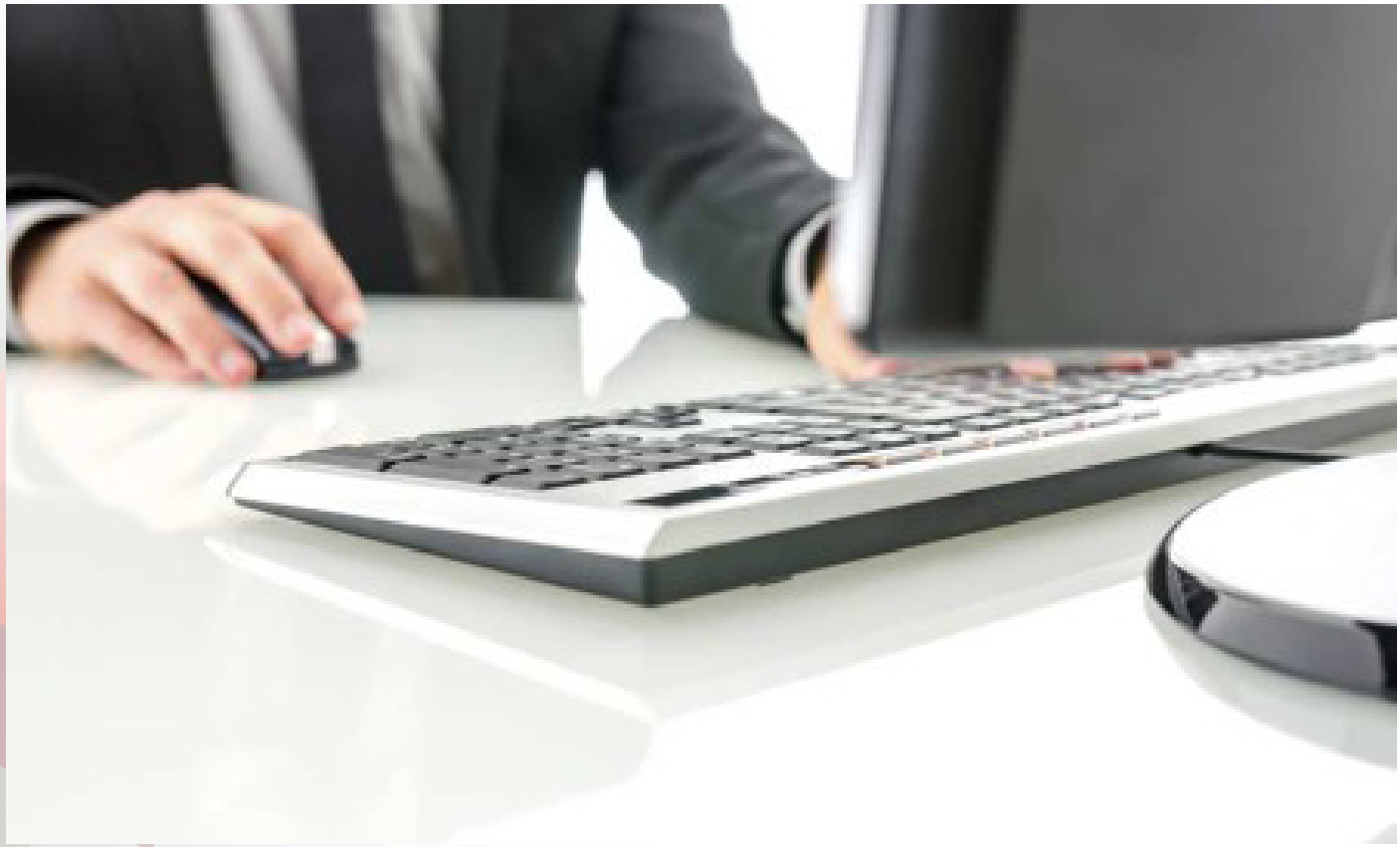
The dangers of computing, where risk is a certainty

FRANÇOIS SETTEMBRINO

Is that only a catchy title to attract the reader's attention, or does it represent a realistic view of the situation? We are all so swamped with information by computers, contacts, e-mail, and other interposed networks that we don't even realize our actual unhealthy dependence. The medical profession invites us to unplug as often as possible to avoid putting our health at risk, and to ensure an adequate vigilance at work, when driving or in real social relations; its only concern is to allow us to maintain a vital balance that could otherwise disappear very quickly and before we realize it, as mentioned, through the interspersion of machines. The problem area is much more extensive than we imagine, and we will humbly address a few aspects of it.

Let us begin with a date: April 8th, 2014! This is not very long ago, but the day set by Microsoft to let Windows XP go; beyond that, there would be no further security updates and no further assistance. So Microsoft is not going to indefinitely nurture a program that has had its day and has been replaced several times in a much more efficient manner. Can we still upgrade older computers, because being forced to acquire a new one is sometimes too heavy for an available budget? For some machines, an upgrade could be done, but its use would not necessarily be easy. In many cases, the machines being too weak, it would become impossible, and so the problems would increase overtime. Yet the situation is more serious than it seems. Many individuals have already decided to assume the risks and therefore continue to use XP because they do not have the resources or do not want to make a new purchase. In companies, this could be even more serious. In Great Britain just in the health sector, more than a million machines are said to be running on XP… The same is apparently true for a majority of the world's ATMs. All this is subject to confirmation and hypothetical, of course, and Microsoft may one day be required to revise or soften its position, but that may be wishful thinking because the longer the wait, the greater the difficulty will be. Anyway, it should be kept in mind that there are more than one and a half billion PCs in use worldwide, of which more than 90% operate under Windows. All do not use XP, but there must still be quite a few that run on it to the satisfaction of their users. Those that are still in use in companies, mainly at SMEs, would benefit from being upgraded when possible, or replaced to maintain a sufficient level of security. They may need to call on specialists, who will not work for free.

For machines being used by individuals, security also needs to be protected; unrestricted PC banking may become too easy a target for criminals, and bankers might even deny access to XP clients to protect themselves. Individuals who have a good "guru" among their friends should call on them as soon as possible. Otherwise they will be able to use the services of professionals, but that could be very expensive with protection that will never be absolute.



ISSUES TO CONSIDER

What else must we monitor, fear, or fall victim to? The following considerations are only a few examples among many. We are superficially familiar with some issues after having seen imperfect media coverage on the subject, and we know others in a little more depth thanks to some revelations, among which those of a certain Snowden are the most recent and also the most serious. It starts with the widespread looting of data through the use of an e-mail system. Even less visible, entire contracts go through online translation services that, if attacked by pirates or if they are leaky, allow the competition to become too quickly aware of everything and anything. Under these conditions intellectual property has no valid system of defense, and Western European nations have no more secrets; their very economies are in danger. Basically, there is no efficient regulation of data; when the first loyalty cards began to proliferate in stores, no-one wanted to face up to the treacherous ways of using customers' personal data and finding out everything about them. The protection of personal data has been praised, information that everyone has the right to inquire about and correct at will. But how many have ventured to do so? If you are customers of an international chain, you have no idea of the use made of your personal data, but it would appear to have an incalculable value. The files of the big chain stores enable a restriction of the random portion of purchasing decisions since on gets insight on almost every aspect of the buyer's profile. If you add that to everything that each person leaves as traces behind them: various cards, telephones where everything is recorded, strolls on one or more social networks, various e-mails, possibly a medical record, even GPS, anything can be used to trap you. Do not forget the thousands of cookies that serve as an indelible halo for you and contain a lot of information on your person… They make it possible to track you, detect your preferences, and reconstruct your behavior. Google does not miss an opportunity to extol the merits of cookies, but they will soon be replaced by an anonymous identifier, more efficient and more insidious, of which it will be the sole owner.

So you will no longer have a say on the matter. And the time will come when businesses and industries that do not use Google Chrome will become blind and can no longer customize their advertisements. Thus, for the individuals that we are, nearly nothing is our own or secret; if it is not already being used, our personal data and all of the traces we leave behind us will be used at all times, whether for a new job, insurance, a court case, etc. In addition, all of this information is collected by companies, Google and several others, which are subject to foreign laws and courts and can do virtually whatever they want. But those among us who would like to remove something from our folder no longer have the power to do so. It's so modern to have one's profile on Facebook or any other network, before one understands that the disclosure of one's private life can only turn against oneself. In case of conflict, good luck to whoever is prepared to litigate, mainly before a US court, since the large-scale offenders are subject to U.S. law. Do not forget that to qualify for American legal protection, it is also necessary to be a US citizen.

RECENT HISTORY

Looking back a bit in history, let us remember that it was the American military that allowed the rise of personal computing, or the PC. It is from the military that the demand and sponsorship for this amazing tool, also called informatics, came from. Few recall that the name itself is just the juxtaposition of two simple words INFORmation/AutoMATIC. And indeed, over time the development of increasingly powerful computers, with bewildering speed, and equipped with almost endless memory, has made nearly automatic the possibility of ever more sensitive data mining, even of the most secret type, enabling almost universal surveillance. The problem is that once again the US military has reserved all of the power for itself.

The power of the American machinery keeps on growing as these events unfold. They appear to be capable of covert intrusion almost anywhere. First, into the affairs of us private persons, through the "back door" of our computers, and into the affairs of any organization, even the police. The power of their own machines is said to be stunning, allowing them to tamper with the most minute settings of any system or network, industrial or military, to render it obsolete or inoperative. It is they who have their security systems concocted in common. A powerful cryptography is a matter for great specialists and apparently the only way to effectively protect industrial and administrative entities. When you buy a computer, the system is 90% Windows; who will ensure that the cryptographic protection you paid dearly for is not equipped with a small relay that only the designer knows?

The title of the article refers to our new environment; the risk is no longer random, and its presence is a constant. Every day we receive new evidence and here is some more:

- The Canadian Revenue Agency has discovered a flaw in its encryption software, implying the possibility of piracy of the personal information of a large number of people.
- In Belgium, the computer system of the SPF Finances seems to have an incredible vulnerability involving flaws at all levels.
- ING stood out by offering to sell information about the purchasing behavior of its customers. Security and privacy are at risk of becoming the big losers because customer files are worth a lot of money and are sold or rented at exorbitant prices.

These are just a few examples, and it is likely that illegal practices are taking place with impunity in absolute secrecy. We the users also share responsibility because too few among us check the small box used with many forms where one can refuse to allow one's information to be communicated to unknown 'partners'.

From several sides people are trying to attract the attention of policymakers about the dangers that exist from doing nothing. Even Europe does not see the danger and only plans to address the problem in 2015. But in the meantime networks rake in huge sums of which we will only receive crumbs, never providing our economies with a new boost. Have things improved for the practitioners of Risk Management? The well known Institute of Risk Management in London has examined the issue of Cyber Risk, concluding that the situation is appalling:

- 360 million bank accounts appear to be in the market and, according to KPMG, 160 million people in 2012 suffered data leaks.
- 70% of Risk Managers have no qualifications or experience in this area.
- 53% of the surveyed companies undertake no specific management in this area.
- Only a small 27% have studied the integrity of the security measures in place in their "supply chain".
- As if that were not enough, 45% of respondents did not know whether their company had already suffered cyber attacks or damage.

Given the urgency of the matter, can something be done? Those who want to explore the issue more deeply cannot be content with reading this modest little article. Here are two paths to guide them:

- First, a remarkable book in French; "La Souveraineté Numérique" (Digital Sovereignty) by Pierre Bellanger, Stock Publishing, 2014, which examines this question.
- Second, in English, the Cyber Risk report and a summary from IRM, available for download from the Institute's Web site (www.theirm.org.)

CONCLUSIONS

Who is to blame if the risk has become a certainty? First, ourselves, for blindly trusting networks presenting multiple hazards, then IT managers for underestimating the dangers and, finally, Risk Managers, who failed to monitor and react to the trend. It is they who should have educated their superiors and executives, but the latter are even more responsible for having too little concern about the phenomenon. The political world did not come through, when it should have anticipated the disasters that await us. Let's leave the last word to Pierre Bellanger:

> **"The internet and its services are controlled by the Americans. The internet is siphoning off our jobs, our data, our prosperity, our taxes, our sovereignty".**

This is the certainly at present. To deserve its name, it's high time that Risk Management react.