

## HOW NEW INFORMATION TECHNOLOGIES CAN REDUCE INFORMATION AVAILABILITY AND SECURITY

### JAK NOWE TECHNOLOGIE INFORMATYCZNE MOGĄ OGRANICZAĆ DOSTĘPNOŚĆ I BEZPIECZEŃSTWO INFORMACJI

**Andrzej Michalski**

Faculty of Organisation and Management, Silesian University of Technology, Poland

**Keywords: Information Technology, information availability, information security**

Słowa kluczowe: technologie informatyczne, dostępność informacji, bezpieczeństwo informacji

### Introduction

Regardless of the approach used, a company's information availability and information security are two sides of the same problem – how to run the business smoothly and safely (Michalski, 2007). In the contemporary enterprise organization all information resources (including resources of the GIS systems) are a valuable part of the enterprise property and the availability and security of the information plays very important role in everyday business activity. Usually, new technological developments help maintain information availability on the proper level and make information management tasks easy and secure. This paper discusses the opposite effect, where new information technologies can reduce information availability and make information resources vulnerable.

### Negative Aspects of Information Technologies Development

The main negative factor relating to information technology development is an information overflow. As a direct result, we must cope with a situation where, before the information can be used for our needs, we must perform a series of laborious and complex search processes to extract the useful information from that which is useless for our purposes (Nielsen, 2003; Levy, 2006; Bray, 2007). This means that the main definition of information processes, established in the early years of computer science development (Shannon, 1948; Orilla, 1986; Microsoft, 2005), which includes information acquisition, storage, processing and

presentation (make available), has changed. Today we must specify additional information processes to handle information overflow, sorting and selection.

Information overload has stimulated the development of technologies designed to extract the desired information. These include Data Mining (ACM, 2007; DZMOZ, 2007), Data Warehouse repositories and the Data Mart (Oracle, 1998). Other strategies to cope with the excess of information include OLAP (Codd, 1993; The OLAP, 2007), Software Agents (Nwana, 1996; Stanek et al., 2004) and the Semantic Web (SemWebControl, 2007; Semantic, 2007).

It is necessary to be aware that all these solutions are a direct result of information technologies developed independently of the user, his habits and activity. The human factor can lead to hazardous situations, when user abuses the technology, or uses it the wrong way.

## **Wrong Usage of New Technologies by Users**

In 2007, the Gartner Group published a series of reports on the invasion of consumer technologies into the enterprise and the challenges that this phenomenon has created for IT departments. Gartner collected these into a special report called Consumerization: *The IT Civil War* (Smith, Prentice, 2007). It is important to identify what IT is losing in this war. We will analyze the six consumer technologies that are causing IT the most trouble and then consider what IT can do to turn around a situation that is, in many places, going quickly from bad to worse (Hiner, 2007).

### **USB portable (flash) drives**

External portable storage devices have been used for many years. In the eighties, the main devices were floppy discs, with the capacity measured in single megabytes. The size of those old floppy discs was a critical factor that limited the amount of data which could be taken outside the company. Today, with low priced 4-GB USB flash drives (flash drives with the capacity of 64 GB and portable HDD drivers up to 160 GB are also available), it is possible to copy not only the "My documents" folder but also a lot of other files onto a portable drive from the company's computers. In the worst case, a large part of a resources of the company's file server can be copied to an unencrypted USB drive and taken away from the enterprise.

### **Wireless access points**

Wireless networks are used widely in the home applications and also provide an important part in the company's data exchange. But a problem rises when home Wi-Fi network users haven't wireless access to the corporate network in their workplace. As they know how easy wireless link can be created, they often implement it in the company, e.g. in the conference room or for other "brain-storm" use, or to eliminate ugly cables. It is often implemented using hardware designed for use in the home (the cost of a Wi-Fi access point is now below \$100), and very often the "private corporate network" propagates out of the building walls and can be accessed from outside, giving everyone on the street access to the corporate intranet.

### **Web mail with GB of storage**

Another method to transfer large files (including company data) is to use a web mail account, such as Gmail, Yahoo Mail, or Hotmail. Currently available free web mail services offer much larger storage capacity and allow larger file attachments than typical corporate mail accounts. Employee use of such services raises at least two problems: the first, that these systems are less secure than corporate mail servers, and the second, that all of them employ an indexed messages and files mechanism which, if used to transfer sensitive corporate data, results in information about that data being stored on external servers.

### **Direct connections (P2P networks)**

The transfer of big files, within a company, is often restricted by security policy, making this difficult for most users. These restrictions are mainly related to internal and external e-mails; the FTP protocol is often too slow and not user-friendly and is quite often blocked by the company's firewall. For this reason some users employ P2P programs, as used at home and often illegally, to transfer music and video.

### **Personal smart phones**

Mobile phones such as the Apple iPhone, BlackBerry, Palm Treos, and Windows-based phones are now inexpensive (usually below \$200) and are offered by many cellular operators with very attractive agreements. It is, therefore, quite easy for the employee to buy that smart phone, if the company do not furnish him with one, and to forward their business e-mail to their personal smart phone, creating a substantial risk regarding security and data privacy.

### **Instant Messaging (IM) software**

Current analyzes show that, in the US, nearly 20% business users are running instant messaging software, like Yahoo Messenger, Windows Live Messenger, AOL Instant Messenger, Skype, Google Talk, etc., at work (Hiner, 2007). The percentage is higher in some countries and younger workers everywhere use this technology much more than do older ones. In the company, the employee usually installs the software himself, often against IT policy. Most of the IM software send data unencrypted, so that workers of the same company exchanging information in this way can send corporate secrets out onto the Internet, making them available to third parties and hackers. In addition, IM file transfers are not usually scanned by antivirus software (Nowy, 2007; Worm\_Skipi, 2007).

## **Conclusion**

Gartner Analyst Stephen Prentice said *The critical thing to understand is that your employees are not doing any of these things to be awkward. They're not doing it because they're trying to break security. They're simply trying to get their job done...* (Smith, Prentice, 2007). Because company users must be able to easily transport their files in order to work from home, on the road, or to transfer documents to partners, etc., the IT department must find

ways how to make it simple for users to do so, whilst protecting sensitive corporate data at the same time. The approach to order workers to stop such practices, without providing corporate solutions, simply does not work. Because of the company information resources security, the IT department should educate users, about portable drives security, provide encryption software for those who need to use flash drives, or furnish employees with flash drives that are preconfigured with encryption and other security standards (Hiner, 2007). A similar approach must be implemented with all other information technologies.

Last but not least – information confidentiality. One Canadian University has discovered a big obstacle with the deployment of the Google web mail application (Dawson, 2008). This University used Google’s free online email and server-based document tools for group working to replace the internal e-mail server and workstation-based collaboration applications used before. The problem is not in the deployed solution itself, but *because the US Patriot Act (The USA PATRIOT Act, 2001) give the US government the right to access virtually any data, at any time, hosted by US companies (Google included) (Dawson, 2008)*. University workers say that the *Google deal broke terms of their collective agreement that guarantees members the right to private communications (Doctorow, 2008)*. This is an important factor which prevents the deployment of these tools in many organizations.

### References

- ACM Special Interest Group on Knowledge Discovery and Data Mining Curriculum, 2007: [www.kdd.org/curriculum.php](http://www.kdd.org/curriculum.php) (available September 2007).
- Bray DA, 2007: Conceptualizing Information Systems and Cognitive Sustainability in 21st Century "Attention" Economies (Includes Syllabus), Emory University – Department of Decision & Information Analysis, Atlanta, April 2007.
- Codd E.F, Codd S.B., Sallery C.T., 1993: Providing OLAP to user-Analysts: An IT Mandate, E.F. Codd Associates, Hyperion Solution Corporation, Sunnyvale CA.
- Dawson C., 2008: Patriot Act preventing Google Apps adoption in schools, <http://education.zdnet.com/?p=1597> (available March 2008).
- Doctorow C., 2008: Companies that use Gmail abroad break the law because PATRIOT makes it possible for US spooks to spy on Google, <http://www.boingboing.net/2008/03/26/companies-that-use-g.html> (available March 2008).
- DZMOZ Open directory project: Databases: Data Mining, 2007: [www.dzmoz.org/computers/software/databases/data\\_mining/](http://www.dzmoz.org/computers/software/databases/data_mining/) (available 2007).
- Hiner J., 2007: Sanity check: The six consumer technologies that are destroying traditional IT, <http://blogs.techrepublic.com.com/hiner/?p=548&tag=nl.e138>, CNET.
- Levy S., 2006: (Some) Attention Must Be Paid!, *Newsweek*, 27.3.2006.
- Michalski A., 2007: Dostępność informacji w organizacji gospodarczej, monograph, Wydawnictwo Politechniki Śląskiej, Gliwice.
- Microsoft Encarta Reference Library 2006, 2005: Microsoft Corporation, Redmond USA.
- Nielsen J., 2003: Information pollution, article dated 11.8.2003, [www.useit.com/alertbox/20030811.html](http://www.useit.com/alertbox/20030811.html) (available September 2007).
- Nowy robak, wykorzystujący Skype’a, 2007: Bezpieczeństwo informacji od A do Z, Wydawnictwo Wiedza i Praktyka, Warszawa, available also as a weekly e-letter. Additional information on website [www.bezpieczenstwoinformacji.wip.pl/index.php?wipx=BI-397-1278](http://www.bezpieczenstwoinformacji.wip.pl/index.php?wipx=BI-397-1278), September 2007.
- Nwana H.S., 1996: Software Agents: An Overview, *Knowledge Engineering Review* No 11, Cambridge University Press.
- Oracle Data Mart Suites on Compaq ProLiant Servers, 1998: Data Mart Sales Kit, Compaq and Oracle.
- Orilla L.S., 1986: Computers and Information. An Introduction, Third Edition, McGraw-Hill.
- Semantic Web, 2007: W3C Technology and Society domain, Semantic Web Activity, [www.w3.org/2001/sw/](http://www.w3.org/2001/sw/) (available September 2007).

- SemWebControl, 2007: Open Source Tools for the Semantic Web, [http://projects.semwebcentral.org/?page\\_id=12](http://projects.semwebcentral.org/?page_id=12) (available September 2007).
- Shannon C.E., 1948: A Mathematical Theory of Communication, *The Bell System Technical Journal*, vol. 27, July-October 1948.
- Smith D.M., Prentice St., 2007: Consumerization Gains Momentum: The IT Civil War, Gartner Research Report, ID Number: G00149305, 5 June 2007.
- Stanek S., Mazur M., Sadecki B., 2004: Zastosowanie kreatywnego agenta oprogramowania w module giełdowym (KGSW) wspomagającym inwestycje kapitałowe, Systemy Wspomagania Organizacji SWO'2004, Wydawnictwo Akademii Ekonomicznej, Katowice.
- The OLAP Report, 2007: Business Application Research Center, [www.olapreport.com/contact.html](http://www.olapreport.com/contact.html), (available September 2007).
- The USA PATRIOT Act, 2001: Preserving Life and Liberty, Department of Justice USA, available on website [www.lifeandliberty.gov/highlights.htm](http://www.lifeandliberty.gov/highlights.htm) (available April 2008).
- Worm\_Skipi.A., 2007: TREND Micro Virus Encyclopedia, [www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM\\_SKIPI.A](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SKIPI.A) (available September 2007).

#### **Abstract**

*In the contemporary enterprise organization all information resources (including resources of GIS systems) are valuable parts of the enterprise property and the availability and security of the information plays a very important role in the everyday business activity. Whilst new technological developments often help maintain information availability on the proper level and make information management tasks easy and secure, this paper is discusses the opposite effect, when new information technologies can reduce information availability and make information resources vulnerable.*

#### **Streszczenie**

*We współczesnym przedsiębiorstwie zasoby informacyjne (włączając w to zasoby systemów GIS) stanowią jeden z najcenniejszych aktywów organizacji, a dostępność i bezpieczeństwo informacji odgrywa pierwszoplanową rolę w codziennej działalności biznesowej. Nowe technologie informatyczne z reguły pozwalają podnieść poziom dostępności informacji i ułatwiają bezpieczne nią zarządzanie. W artykule zostanie omówiona sytuacja przeciwna, gdy nowoczesne technologie informatyczne mogą spowodować ograniczenie dostępności informacji bądź obniżyć poziom jej bezpieczeństwa.*

dr inż. Andrzej Michalski  
[andrzej.m.michalski@polsl.pl](mailto:andrzej.m.michalski@polsl.pl)