South African Journal
of Information Management
[DoE accredited]

Secure notes Vol.5(2) June 2003

Alternatives to *1984*: issues on securing information assets

S.Berner
sberner@ecognus.com

Information security is a necessity, but it raises many social and financial issues – from freedom of information, to privacy and return on investment. In this issue, we look at why it is important to secure information assets and who the primary beneficiaries of the process are.

Information security – a mixed bag of blessings

As a direct result of living in a world full of hackers, cyber-terrors and scripted viral infections, an outcry has risen through the so-called 'democratic' world condemning the curtailing of civil rights in the wake of the September 11 tragedy, accusing those in power of conspiring to clamp down on the most basic freedom of people: the freedom to know. Many social activists perceive information security as the monopolization of power and an important aspect of furthering the digital divide.

Although it is tempting to join the charade of upset social justice activists and outraged librarians, and although we tend to see any attempt at denying us our right to informative material as a breach of our civic rights, one should guard against subjectivity. Free for all is not necessary good for all. Should information be secured, and if yes, why? Who benefits and who loses in the game of assets as intangible as data and information? Finally, is it at all possible to actually secure information totally and comprehensively? Can information be 'securely free'? In this column, I discuss possible answers to some of these questions and shall continue the discussion in subsequent issues.

All of the above questions have been raised in different academic and social milieus and the answers are far from unanimous. On the one hand, there are those who deeply believe that information, like air, is free. It is often those who do not actively make money out of their own intellectual property, but who make it by using that of others who think that information should be free. On the other hand, there are those who make serious money out of creating an information scarcity and then charging for access to it: publishers, record companies, market researchers, management consultancies and, increasingly, academic institutions. When it dawned on information managers that they could sell what they knew, they joined in the fray too, as knowledge managers and information brokers (instead of providers, which is more nurturing).

Issues of concern

Whether or not information should be secured seems to be asking the obvious and yet the issue is far from simple. The trouble starts with the definition of what it means if information is secured. If an agreement is finally reached on the defining terminology, there develops other issues of content, extent and value. After all, information security is expensive – and

for the money paid it always seems to fail somewhere, somehow, sooner or later. We even question what exactly does 'information security' mean. Is it assuring its quality or protecting it from threats. However, unsecured information is expensive too, in terms of lost business, damage to assets and reputation, and outright theft.

Feinman, Goldman, Wong and Cooper (1999) define information security as controlling access to sensitive electronic information so that only those with a legitimate need to access it are allowed to do so. This seemingly simple task has become a very complex process with systems that must be continually updated and processes that must be reviewed constantly. There are three main objectives for information technology security: confidentiality, integrity and availability of data. Confidentiality is protecting access to sensitive data from those who do not have a legitimate need to use them. Integrity is ensuring that information is accurate and reliable and cannot be modified in unexpected ways. The availability of data ensures that data are readily available to those who need to use them.

Most of the damage to and theft of information assets are facilitated by sheer lack of awareness on behalf of the end-users. The freeware and shareware downloaded by an employee, if run on a network, could contain back doors and access 'features' for hackers. When breaking into a digital operation, the path of least resistance is probably not the firewall, but instead, perhaps, a phone call in which a password is revealed to a clever conversationalist.

Part of the problem also lies with the technology. As security holes in products are announced, hackers have a limited time to take advantage of them. A paper from the Bank of Japan (2000) states:

> 'While risks such as system breakdowns and unauthorized acts by employees have existed regardless of closed or open system environments, with the increased reliance on open systems, there are now greatly increased risks such as third parties' impersonating clients and theft or alteration of information transmitted over networks. Furthermore, there is the emergence of new risks, such as unauthorized access from the outside and service interruptions that are specific to open systems.'

Costs and benefits

For one thing, no system can ever be 100% secure. The threat of digital 'peeping Toms' is an ever-expanding one. As the Internet explodes in capacity, so do the deeds of hackers, trick-playing teens, exploring children, fraudsters and serious white-collar criminals. Because information security is becoming such a technically complex issue, many companies are choosing to outsource the function to companies that specialize in the service. As the number of threats increase and the budget dollars for security become limited, companies must choose the solutions that are the most cost-effective: preventative methods are considered reactive and most businesses now opt for intrusion detection as well as a risk-management approach. All this adds to the cost and it takes some ingenuity to explain to funds-strapped management how spending more money is going to produce a return on investment. Perhaps seeing the whole information security process as a form of insurance would be a good approach to breach the subject (Strassmann 2000).

Conventional wisdom seems to suggest that using the economic-based models approach is inappropriate when it comes to expenditure decisions related to the activity of information security. Hence, whereas the technical aspects (e.g. encryption techniques, bandwidth concerns and intrusion detection systems) of information security have been the subject of much research, very little research has been devoted to studying the economic aspects of

information security. The allocation of funds to information security activities must be considered in cost-benefit terms, analogous to the way resources are allocated to other activities.

The benefits from information security are directly related to the cost savings associated with preventing losses that have occurred due to security breaches. The costs of information security are the result of implementing procedures to address the four concerns, namely:

- protecting information from unauthorized users of the information;
- making information available to authorized users on a timely basis;
- protecting information from integrity flaws; and
- detecting, as well as correcting, information security breaches.

The 2001 CSI/FBI survey notes that of the 186 respondents that were willing and/or able to estimate losses due to security breaches, such breaches resulted in losses close to $378 million (Power 2001). This figure is small in comparison to the financial loss associated with information security breaches not acknowledged. Furthermore, accurately deriving the correct figure is problematic. For example, how does a firm derive the dollar value of lost sales due to the negative 'reputation effect' of a publicly known security breach?

Interestingly enough, recent research (Gordon, Loeb and Zhou 2001) shows that information security breaches do not seem to impact the stock market value of firms experiencing such breaches.

No to *1984*, yes to collaboration

Paul Strassmann of Nasa agonised between 2000 and 2001 in a number of articles over the social, business and financial implication of securing information. It is a matter of interest that Strassmann, like many other researchers into information security issues, has a military background, while most writers on information sharing and freedom of information come from social sciences and humanities niches. We can almost see an imperceptible pitting of forces on the two sides of the contested matter: law and order on one, the intellectual renaissance on the other.

Strassmann's position is typical of a knowledge management guru: he states that real wealth is not in tangible resources but in the know-how of manipulating them (Strassmann 1999). This know-how resides in two main places – as intangible knowledge in employees' heads and as tangible knowledge in computer systems and documents. Loss of intangible knowledge results from human action (Strassmann 2001), while most of the damage done to tangible knowledge results from human action. Knowledge, information and/or data have to be protected from humans, who also carry it in their heads and use it to do anything productive. This, however, costs money, is full of pitfalls and results in endless bad will and frustration among humans. By now, we seem to be in a vicious circle – secure we must, but we cannot do it very well – and the worse we do it, the more we need to secure it, etc. Human nature is perverse, if you push too much it rebels. Too much pressure on securing information in the workplace leads to surveillance, breach of privacy and consequently to bad will, lowered productivity, lowered morale, etc. The circle closes on itself when the stressed employees start exhibiting socio-pathological behaviour, wilfully breaking the regulations imposed on them. This generates a need to secure information assets further.

Shrage (1997) stipulates that information security will only pay off if it is designed and managed with the recognition that it must be based upon the culture and politics of the enterprizes it is intended to support. However, studies in the fields of organizational psychology are increasingly showing that corporate cultures are often inimical to

psychological health, are often enforced from above and do not take human emotional needs into account.

Information security policies are necessary to ensure that important data, business plans and other confidential information are protected from theft or unauthorized disclosure. If employees of any organization are not aware of these policies, they will not know what is expected of them when they handle such confidential information. Every organization should have the physical aspect of security well taken care, but if the staff are not educated on information security policies, their lack of education, awareness and training would result in confidential information simply walking out the front door. A good information security awareness programme is needed to highlight the importance of information security and to introduce the information security policies and procedures in a simple, yet effective way so that staff are able to understand the policies and are aware of the procedures.

General Robert Marsh, the Chairman of the US President's Commission on Critical Infrastructure Protection, was quoted to have once said: 'Information sharing is like breathing – you have to do it to survive. How well you do it affects your strength, but if you overdo it, you will pass out. And you have to be careful what you breathe' (Cartney 2000). Which brings us to the important point of alternative information security: *building trust* and *raising awareness*. Technology is only a partial solution to information security, say the experts. The best prevention is employee training, not technology. More than ever, the best information security solutions combine people and processes with technology for effective prevention techniques. Proper standards enforcement and training should give guidelines about downloading safe and functional software. This solution requires a combination of well-trained people, good processes and technology to be successful.

References

Bank of Japan. 2000. The importance of information security for financial institutions and proposed countermeasures. [Online]. Available WWW: http://www.boj.or.jp/en/set/00/data/fsk0004b.pdf (Accessed 7 May 2003).

Cartney, M. 2001. The art of balancing information security and information sharing. Programme for information resources policy, Harvard University. [Online]. Available WWW: http://pirp.harvard.edu/pubs_pdf/cartney/cartney-p01-4.pdf (Accessed 7 May 2003).

Feinman, T., Goldman, D., Wong, R. and Cooper, N. 1999. Resource protection services, security basics: a white paper. Pricewaterhouse Coopers LLP.

Gordon, L., Loeb, M. and Zhou, L. Stock market effects of information security. Working paper. Robert H. Smith School of Business, University of Maryland.

Power, R. 2001 CSI/FBI computer crime and security survey. *Computer Security Journal* 27 (2):29–51.

Shrage, M. 1997. The real problem with computers. *Harvard Business Review* (September–October):178–188.

Strassmann, P. 1999. Knowledge metrics-ticker-tape charade. *Knowledge Management* (November). [Online]. Available WWW: http://files.strassmann.com/pubs/km/1999-11.php (Accessed 7 May 2003).

Strassmann, P. 2000. Art of budgeting: How to explain spending on information security?

[Online]. Available WWW: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci342423,00.html (Accessed 7 May 2003).

Strassmann, P. 2001. How to value information security risks. *Knowledge Management* (February). [Online]. Available WWW: http://files.strassmann.com/pubs/km/2001-2.php (Accessed 7 May 2003).

Further reading

Barman, S. 2001. *Writing information security policies*. Indianapolis: QUE Publishing.

Barnum explains that security policies are a component of the planning aspect of the security process and as such can provide three advantages. The first is to insure security interoperability across an organization. The second advantage is the visibility given to the policy by management's participation in it, which provides a greater impetus for implementation. The third is to mitigate liability, presumably by the legal value of the policy and the advantages to security that a policy-driven approach proves.

Mitnick, K. and Simon, W. 2002. *The art of deception: controlling the human element of security*. New York: Wiley and Sons.

Much of Mitnick's security advice sounds practical until you think about implementation: you realize that more effective security means reducing organizational efficiency – an impossible trade in competitive business. And anyway, who wants to work in an organization where the rule is 'trust no one'? Mitnick shows how easily security is breached by trust, but without trust people cannot live and work together. In the real world, effective organizations have to acknowledge that total security is a chimera.

Schneier, B. 2000. *Secrets and lies: digital security in a networked world*. New York: Wiley and Sons.

The book is neatly divided into three parts, covering the turn-of-the-century landscape of systems and threats, the technologies used to protect and intercept data and strategies for proper implementation of security systems. Moving away from blind faith in prevention, Schneier advocates swift detection and response to an attack, while maintaining firewalls and other gateways to keep out the amateurs.

Related Web sites (not exclusive)

- Commonwealth Films: http://www.commonwealthfilms.com/infosec.htm
  This site has a good selection of information security videos on areas such as computer security, information protection, e-mail and Internet abuse.
- Green Idea: http://www.greenidea.com.
  The company produces a visually exciting, 3D animated software program fostering awareness in information security. A free evaluation demonstration can be downloaded for viewing.
- Search Security: http://searchsecurity.techtarget.com.
  A great Web site full of news, expert advice, discussions and much more. It is worth losing a few hours in exploring.
- The SANS Institute: www.sans.org.
  The SANS (SysAdmin, Audit, Network and Security) Institute was established in 1989 as the trusted leader in information security research, certification and education. It enables more than 156000 security professionals to share the lessons that they are

learning and find solutions to the challenges that they face. The Web site has news digests, research summaries, security alerts and award-winning papers for free, as well as fee-based publications.

About the author

Sam Berner (B.Ed., Dipl. LIS, Postgraduate Diploma in Information Management) is a principal of the company ECognus (Brisbane, Australia). She is a knowledge management consultant, assisting small to medium enterprizes to benefit the most from their intellectual assets. ECognus also provides services in the area of tailored software applications and the digitization of business processes.

ISSN 1560-683X
Published by InterWord Communications for the Centre for Research in Web-based Applications, Rand Afrikaans University