End User Computing and Information Security: a retrospective look at the de-centralisation of data processing and emerging organisational information risk

Richard Henson and Joanne Kuzma

Business School, University of Worcester, Worcester, UK

Email: r.henson@worc.ac.uk

Abstract (around 150 words – style 'Abstract Title')

Information security assured on centralised systems through application of principles previously established for paper-based systems. The advent of personal computing and distributed computing potentially turned that model upside down. It seems that the eagerness of organisations for encouraging technology (Availability part of the CIA acronym) seemed to take precedence over the finer meaning of Confidentiality and Integrity, in spite of (in the UK, at least) changes to legislation.

The huge increase in portable data storage capacities ensured that what may have been perceived as a minor irritant in the 1980s became a potential nightmare scenario by 2007, which caused two government reports to report "systemic failure". This paper looks at the development of end-user computing, and suggests that the problem occurred because of a lack of information risk assessment over many years

Keywords: Confidentiality, Integrity, Availability, end-user computing, information security, information systems management

1. Introduction

End user computing became very popular in the late 1980s, and had become the norm in organisations by the mid 1990s. This paper examines the opportunities and challenges presented to organisations by end-user computing, and the emergence of information risk in connection with this (then) new phenomenon.

2. Information Security Procedures before End-User Computing

2.1 Pre-Digital Information

Stored information, and its security, has been an issue whenever civilised society has emerged and organisations have made records. Information was kept secure either in people's brains or held in paper-based systems. The management and security of organisational information held on paper became more of a challenge as more paper was generated, and the main issue was to keep the stored data physically safe (integrity), make it readily available to those with authorisation (availability) and restrict access to it to those “with a need to know” (confidentiality). In that respect, the oft-quoted C-I-A acronym is nothing new. When information was on the move outside a secure trusted environment, greater safeguards (more physical protection) may have been necessary depending on the sensitivity of the information. The “insider threat” was anticipated in the UK through the passing of legislation, “The Official Secrets Act” (HMSO, 1911) making the disclosure of classified information a criminal offence. It is interesting that legislation was at that point regarded as an aid to the use of physical security, to control sensitive information. However, it seems that the combination of legislative and a “secure facility with request desk” approach – akin to the secure section in a public library - was successful in maintaining the integrity of organisational information through the first half of the 20th century, and on into the 1960s.

2.2 Early Digital Security Model (Business as Usual?)

The emergence of digital media for storing information, and computer programs for processing information immediately provided new challenges for information systems professionals, but not immediately. Only very large organisations had computing facilities at all, and the computing facility of the 1960s/70s was designed around a vast centralised computing area and request desk to provide controlled access to information. Although processing was digital, the digital information stored was only available through being printed out and checked out to someone who was able to physically show that they had appropriate authority.

The printed information itself would be subject to the same safeguards as anything else recorded on paper, so existed well tried-and-tested systems were considered adequate, and no new systems needed to be devised.

2.3 Taking Digital Data outside the Data Centre

During the early 1970s, most organisations continued to use their own derivations of the existing security model for information, merely applying these well-tried-and-tested principles to digital data. However, with technological advances it had become possible to present digital information on a TV screen, as opposed to a paper print-out, which would be useful to management for analysis and decision-making. Consequently, when a viable commercial Visual Display Unit product (VDU) was launched by the Wang Corporation (Kenney, 1992), organisational pressures from management rapidly built up to allow information to be at least displayed, if not printed out, outside that secure data processing area. An influential report from the RAND Corporation in the USA (Ware, 1970) at the start of this decade had anticipated some of the problems that became apparent as digital information started to become available outside a centralised secure area for the first time.

The mere use of a VDU system with no processing or storage ability should not in itself provide a security threat. The main danger would appear to be the leaking of information that had been printed out, and provided that existing procedures for dealing with computer print-outs were adhered to there was no reason to think that this was a problem. There was a further difference here, however, in that data could also be processed by people "outside the centre" and the move to VDUs opened up the potential for user-computer interactivity and ultimately for what became known as "end-user computing". Also, through invention of the modem, it became possible for digital data to be transmitted from through public systems such as the telephone network. There was now the capability for users to both store data and send it to others – for example to other parts of a national or multi-national company, or a government department, or a bank ATM machine.

As digital data was now able to be sent from place to place within and beyond the organisation, rather than merely sitting on a mainframe, it clearly needed more protection. Cryptography, once the domain of the secret services, was now used for the first time commercially using a system with a 56-bit key known as The Data Encryption Standard, DES, (FIPS, 1975). This would secure commercial data sent between sites by encrypting/decrypting at the communication ends. Also, the danger of unauthorised external access to the mainframe became a potential issue and a security device was invented (Caudill et all, 1976) that would ensure password only access (series of digits).

As the end-user phenomenon continued to grow, it was perceived at EU and UK government levels (Hansard, 1983) that public concerns about the leakage of their personal data from organisations were rising. In Europe a legal directive was passed by the European Union (EU, 1981) to protect such data. In the UK, this debate mentioned earlier eventually became the 1984 Data Protection Act (HMSO, 1984), but the emerging issue of end-user computing did not feature highly in the eight data protection principles enshrined in that act (Appendix 1). However, at this stage in developments, encryption was generally not considered for the storage of organisational data because the data was stored safely and securely on a mainframe or minicomputer.

3. Organisational Issues with End-User Computing

3.1 Local Processing with the Desktop Computer

As users became accustomed to using local VDUs interacting with a central storage facility, and management benefited from rapid access to information through this new source, consumers started to buy microcomputers for their homes. Organisations could envisage uses for computers on the desktop. This encouraged to IBM release their own microcomputer, the PC (Personal Computer), and "end-user computing" (EUC) began in earnest within organisations.

The first research articles on EUC and its management began to emerge in the early 1980s. A field study by Rockart & Flannery (1983) correctly predicted the meteoric growth of this phenomenon and identified as many as six different types of user. A study in the St Louis area, in the USA (Benson, 1983) involving interviews with management clarified that use of IBM PCs in the US was widespread. Many reasons and benefits were reported including, higher speed of processing and greater richness of data than VDU units and consequent increased employee productivity. This was much more significant than previous developments relating to information security; the IBM PC was a potentially huge threat to integrity and confidentiality because data could now be processed and saved locally by users inexperienced in dealing with digital data.

Further research (Henderson & Treacy, 1986) based on the Rockart & Flannery model spelled out the complexities of managing end-user computing more clearly, and identified security of data on end-user machines as a potential issue that needed to be managed. They also spelled out the benefits of end-user computing and saw potential competitive advantage for organisations that used it wisely.

2.2. The uncontrolled growth of organisational End-User Computing

The use of the microcomputer in organisations seemed assured by the late 1980s. In theory, however, there was nothing to stop an employee copying to floppy disk and taking the disk out with them, but issues such as data protection on a microcomputer or personal computer (PC) was not seen as high priority. Academic research had highlighted the potential security issues presented by digital data that could be processed by and extracted from a computer by the user at will. However, it seems that security of digital data often did not become the organisational priority it should have been. The call for better management of end-user computing (Rockart & Flannery, 1983) was often seen in terms of maximising organisational benefits (i.e. productivity gains and cost savings), rather than management of security – which also came out of the research. The result was an encouragement of employee engagement with the microcomputer and the facilitation of competent use, in priority to training in secure handling of digital information. It may have been perceived that too much focus on security would increase cost and possibly reduce productivity. Academic end-user computing research during this time (e.g. Doll & Torkzadeh, 1988) tended to focus on end-user satisfaction, rather than security concerns.

In these early days of the microcomputer, a PC would be working in standalone mode. As there was no physical or logical connection to larger, centralised systems containing organisational data, this provided some kind of safeguard against both internal and external threats. Organisational data would not have seemed to be under any particular threat. However, Data Processing (often now rebadged MIS (Management Information Systems)) departments with appropriate expertise and centralised control of organisational data would have been looking with some concern at what Yourdon (1990) called the "cocky novice" – the self-taught employee who handed departmental data with independence and lack of supervision, but had an exaggerated opinion of their own knowledge and understanding. MIS managers were aware of this already (Benjamin et al, 1985) but had not yet come to terms with what to do about it. They could expect that their role would become more distributed, but not yet how this would be managed strategically from an organisational point of view. One of the authors of this paper worked in such an organisation in 1990 and heard the MIS manager regularly articulate such concerns. It seems reasonable to conclude, therefore, that, although end-user computing grew in line with expectations, and key issues had been clearly identified (Brancheau & Brown, 1987) a coherent model for its management had not been either acknowledged or implemented – PCs were typically held within departments, and outside the control of MIS.

By the early 1990s, it had been widely recognised (Brancheau & Brown, 1993) that the benefits emerging from end-user computing were of two distinct types: organisational, and individual. The "individual" benefits of training in the use of applications would subsequently benefit departments, an in turn this would benefit the organisation. The siren voices of MIS managers had not, in many cases, been heard, and most PC users would not have received the rigorous information security training on that their MIS colleagues had previously received, even through they were handling organisational data. Some organisations did start to apply risk analysis techniques to their information systems (Rainer et al, 1991) but most relied on file system security, without properly assessing the increased risk of saving to portable devices.

2.3 Security Consequences as Technology moved relentlessly on

The rapid transition from centralised multi-user systems to PC-based systems may not have seemed a big step at the time, but retrospectively, it was the quantum leap in terms of what followed. Certainly, a greater consideration should have been given to the way microcomputer systems locally save applications data, as opposed to merely reading data that is only held centrally. The term "read only" meant something in the days of centralised storage, but a "read only" Word document, for example, is automatically saved locally on a temporary basis when it is used, and can easily be saved permanently with a different filename. This was a BIG change from systems conventionally available in centralised multi-user systems, and again a possible cause of security concern. A "mixed environment" network including Unix terminals and PCs with fileservers had been subjected to academic investigation over several years, but PC security had not been considered as a problem and indeed the author of an evaluative report based on this investigation (Stayanarayanan, 1989) suggested a rejection of the more secure diskless PC workstations from a performance perspective. It should be remembered that at this time, PCs were not very powerful, and the focus on helping employees to get the job done was understandable.

Huge advances have been made in the processing capabilities and storage facilities associated with organisational information systems from the early 1990s to present day. PCs became routinely networked and were consequently given access to corporate and personal data within information systems that had been designed for storage and processing a centralised approach, with a legal framework assuming such an approach (HMSO, 1984). Yet the author can find no research in the literature that explores the legal implications of organisational use of PCs to store and process data.

Capabilities for the local storage of data were enhanced a thousand times as first the CD, and later the DVD became widely available. As personal computer networks became connected to other networks via the rapidly growing Internet, this offered the capability for such data to become available beyond the organisation without the normal security safeguards associated with centralised data processing. This not only involved copying locally to portable media, but the sending of data directly through cabled and even wireless media. In the UK, an opportunity to tighten up the eight data protection principles in view of the hugely increased role of PC data was overlooked in when the act was updated in 1998 (HMSO, 1998). It was not until very recently that, as a result of the loss of huge amounts of personal information and a consequent inquiry reporting “systemic failure” (Poynter Report, 2008), there has there been a slight strengthening of this legislation (HMSO, 2008). A further announcement from the ICO on strengthening the legislation is due on April 6th 2010.

3. Conclusion

The emergence of end-user computing in the 1980s and the file security issues raised with PC-based systems challenged the conventional centralised information security model for organisations. Whilst many aspects of end-ser computing have been positive, and computing has concern about end-user computing extended to security matters, this one fundamental security issue with local computer file systems, especially when connected to distributed networks, has still to be fully addressed.

References

Amoroso, DL, 1988, “Organizational issues of end-user computing”, ACM SIGMIS Database, Volume 19, Issue 3-4 (Fall/Winter 1988) pp: 49 - 58

Benjamin RI, Dickinson C Jr, Rockart JF, “Changing role of the corporate information systems officer”, MIS Quarterly, 1985

Benson D. H., 1983, “A Field Study of End User Computing: Findings and Issues”, *MIS Quarterly Journal*, Vol. 7, No. 4 (Dec., 1983), pp. 35-45

Brancheau JC, & Brown CV, 1993, “The management of end-user computing: status and directions”, ACM Computing Surveys (CSUR), Volume 25, Issue 4 (December 1993), pp: 437 - 482

Brancheau JC, Wetherbe JC, 1987, Key issues in information systems management, MIS quarterly, March1987

Caudill HT, and Euler EE, 1976, Computer Terminal Security System, US Patent 3,984,637, 1976. Available from: http://www.google.com/patents?hl=en&lr=&vid=USPAT3984637

Doll, WJ & Torkzadeh G, 1988, **“**The measurement of end-user computing satisfaction“, MIS quarterly, June 1988

EU, 1981, EU Directive on Data protection, 1981

FIPS, 1975, Proposed Federal Information Processing Data Encryption Standard. Federal Register (40FR12134), March 17, 1975

Henderson & Treacy, 1986, “Managing end-user computing for competitive advantage”, Sloan Management Review, Winter 1986.

HMG, 1911, “The Official Secrets Act”, HMSO

HMG, 1984, “The 1984 Data Protection Act”. HMSO http://www.swarb.co.uk/acts/1984DataProtection01Act.shtml

HMG, 1998, “The 1998 Data Protection Act”, HMSO http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

HMG, 2008a, “The Criminal Justices and Immigration Act, 1998” section 77, HMSO Available from: http://www.opsi.gov.uk/acts/acts2008/en/ukpgaen_20080004_en_7

HMG, 2008b, “The Poynter Review of Information Security at HM Revenue and Customs”. Available from: http://www.hm-treasury.gov.uk/d/poynter_review250608.pdf

Hansard, 1983, “discussion on proposed 1983 Data Protection Bill”, 11th April 1983, Available from: http://hansard.millbanksystems.com/commons/1983/apr/11/data-protection-bill-lords

Kenney, C.C., 1992, Riding the Runaway Horse: The Rise and Decline of Wang Laboratories, Little, Brown and Company.

Rainer RK, Snyder CA, & Carr HH, 1991, “Risk analysis for information technology”, Journal of Management Information Systems, Volume 8, Issue 1 (June 1991).

Rockart JF & Flannery LS, 1983, “The management of end user computing”, Communications of the ACM**,** Volume 26, Issue 10 (October 1983).

Satyanarayanan M, 1989, “Integrating Security in a Large Distributed System”, ACM Transactions on Computer Systems, 1989

Ware, W., 1970, “Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security”, Rand Report R609-1 (Feb. 1970)

Yourdon E, 1989, “Structured Systems Analysis”, Chapter 3. Available from: http://yourdon.com/strucanalysis/wiki/index.php?title=Chapter_3

Bibliography

de Leeuw, K., & Bergstra, J., 2007. “A History of Information Security”, Elsevier