IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12683

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Small Business Experience and Governance of Employee Owned Personal Digital Devices

W. Brett McKenzie, Computer Information Systems, Roger Williams University, Bristol, RI 02809, P 401-254-3534, wmckenzie@rwu.edu

ABSTRACT

This research examines the policies regarding the use of personal digital devices in Small to Medium Enterprises (SME), with an emphasis on small business. Where larger enterprises have focused attention on the potential exposure to data compromise through deliberate or inadvertent misuse of data, SMEs appear less concerned. This study uses interviews and a local survey to examine both the use of digital devices and the policies for security of digital devices.

INTRODUCTION

In 1999, Wen Ho Lee, who was accused of downloading classified, nuclear material to a 150 MB digital tape, brought pubic attention to an individual's ability to download large quantities of data and the possible motives and consequences of such action (US vs. Wen Ho Lee, 1999). Since then, portable digital devices have grown in capability, such as cell phones and PDAs being able to operate on an IP network via wireless. Similarly, they have expanded in storage, such as the MP3 players with gigabyte size hard drives. Connectivity to the network raises security issues just as storage allows replicating and removing from a site large quantities of corporate data. Additionally, the use of portable digital devices in the workplace raises management issues because the devices may be owned by all levels of employees, from the hourly warehouse laborer to the CEO as well as contract employees, such as a cleaning service. Their governance and use in the workplace has become an increasing issue.

With the proliferation of these digital storage devices, the trade press has indicated concern for the possible compromise of proprietary or privacy data through deliberate or inadvertent storage of corporate information on portable media (Rosten, 2005). Flash memory with gigabyte storage capacity included in mundane objects, such as pens, Swiss Army knives, and watches or jewelry, has increased the potential to store and transport large data files surreptitiously. In 2004, Gartner created a stir by recommending that companies ban all digital storage devices, in particular, the Apple iPod (Contu, 2004).

Large enterprises frequently control the presence of digital devices in the workplace through issuance to an employee of trusted devices. A centralized institutional unit or service provides a cell phone, laptop, or mobile device and integrates it into the enterprise. This form of control minimizes, but does not eliminate individual use of personally owned devices. Subsequently, security companies, such as Safend (http://www.safend.com/), Reflex Magnetics (http://www.reflex-magnetics.co.uk/), and SecureWave (http://www.securewave.com/sanctuary_DC.jsp), have introduced products to manage USB/Firewire ports and the Plug-and-Play features of the desktop operating systems. These electronic control systems are integrated into the corporate security policies and may be coupled with polices to prohibit personal devices. These latter policies, however, seem to be associated with the more formal corporate environments.

Ownership, for the purpose of this study, considers individually owned devices and extends the concept of ownership to an individual's exclusive control over a portable device, such as a laptop or cell phone provided for the individual. Additionally, the study does not consider activities to prevent data compromise through loss or mechanisms to recover misplaced portable digital devices, which can also compromise business data (Herold, 2005).

SMALL BUSINESS ENVIRONMENT

Small businesses, however, face a very different environment. This study uses the UN Economic Commission for Europe (UNECE, 1996) definition, which defines small business as having less than 50 employees, revenue of less than EU 7 million, and is independently owned. These businesses are usually more personal and frequently operate without a dedicated IT staff. In this world, personal and company portable technology, such as cell phones, are often blended with one device serving both roles.

Security experts recommend considering three dimensions when creating security policies: confidentiality (protecting private information), availability (allowing authorized access), and integrity (reliability of data). When conducting a Google search on security policies for digital devices using the search terms and variations of "policy for portable devices" it is interesting to note that colleges and universities, especially those with health care facilities, dominate the results. This may be attributed, not only to the more open academic environment, but also to universities having to face the issues because of a younger and more digitally well-informed population. Secondly, the focus on medical areas reflects the social practices of those entrusted with medical data, whose privacy must be protected in the United States under the HIPAA (1996) statutes.

The Texas Workforce Commission provides the most comprehensive guidance for small business. Their *Internet, E-mail and Computer Usage Policy* includes a recent addition on the use of digital camera devices, including cell phones, and personally owned computers (Texas Workforce, 2005). It, however, does not include policies for USB storage devices or portable players. In the supporting discussion on employee workplace rights, the issues of portable players are considered. This, however, is more from attributing liability of possible hearing loss to workplace environmental conditions rather than from listening to too loud music.

USAGE PATTERNS

The majority of the small businesses interviewed to date have employees who spend more of the day in the field than in an office location. The cell phone has become a critical item for all employees. No businesses have noted instances of abuse either by employees incurring unreasonable charges or management harassing the employees by calling at inappropriate times. These businesses have discovered that providing a cell phone and limiting or preventing the use of a personal cell phone has improved productivity.

For one company, a cell phone provided to employees is a significant "perk" for the hourly field workers. Management has discovered that

keeping workers on the job towards the end of the day is much less fraught when the employee can call home. This has been a great advantage for employee moral and has increased productivity.

Interestingly for the same company, lower level employees were issued a basic phone, while management had phones with cameras because of cost differences. This policy was formalized so that all job supervisors would have camera phones. As the work often entails installing custom furniture and fixtures, sending a photograph electronically allowed management at the home office to verify site conditions against the plans saving on a visit to resolve a discrepancy.

In discovering other consequences of new technology, one company learned the pitfalls of eavesdropping facilitated by the technology. The original cell phones included a push-to-talk feature. This was changed to allow only handsets, because a client had overheard an inadvertent comment broadcast via the push-to-talk mode.

In the medical practices, more restrictive policies were expected. However, many small medical practices still maintain most of their records on paper. For example, it is only within the last nine months that they have converted to an electronic patient scheduling system. This may reflect national practices of complex third party billing which discourages a centralized system. The recent change in the US government support for medications, however, is causing a reassessment of these practices.

In these instances, the companies have discovered, counter to the recommendations of the larger corporate environment, which are to discourage use of employee owned devices, that defining and allowing technology is better than trying to prevent it. It has, however, required experimentation because the technology has changed the nature of the work. In neither case, have the owners instituted separate policies for the office staff governing either USB or MP3 devices. It is possible that the culture of the smaller company is such that these items have not become an issue.

CONCLUSIONS

The concern expressed by the larger enterprises regarding security that is not seen among these smaller businesses, may reflect the shift to knowledge work in large corporations. The smaller businesses investigated to date are more concerned with reliable employees and quality of work in the field. The proprietary company data is restricted to a much smaller circle than in a larger enterprise with the consequence of lower levels of concern for compromise.

REFERENCES

Contu, R. (2004), *How to Tackle the Threat from Portable Storage Devices* Downloaded from: http://www.csoonline.com/analyst/report2714.html

Herold, R. (2005) *Privacy Policies For Portable Devices*, Security Pipeline, Sept 01, 2005. Downloaded from: http://www.securitypipeline.com/handson/170102450

Locking down USB ports: Interview with Vladimir Chernavsky, CEO of Smartline, Network World, Sept. 27, 2005. Downloaded from: http://www.networkworld.com/research/2005/0926radio.html

Rostern, J. (2005). *Dangerous Devices* The Internal Auditor. Oct. 2005. 62:5 p. 29-33

Texas Workforce Commission (2005) *Internet, E-Mail, and Computer Usage Policy* Downloaded from: http://www.twc.state.tx.us/news/efte/internetpolicy.html

United Nations Economic Commission for Europe. *Definition Of SMEs In The European Union* Downloaded from: http://www.unece.org/indust/sme/def-eu.htm

US Vs Wen Ho Lee, (1999), United States District Court For The District Of New Mexico. downloaded from: http://www.fas.org/irp/ops/ci/docs/lee_indict.html