Chapter 10
Security Technologies and Policies in Organisations

Nickolas J. G. Falkner
The University of Adelaide, Australia

ABSTRACT

The ability to perform actions that were previously impossible or unfeasible has been one of the most challenging aspects that has accompanied the introduction of electronic systems for data management. This, in turn, has required a rethinking of a number of behaviours that had apparently been driven by a strong ethical code but now appear to have been more strongly controlled by the impossibility of the action. This chapter proposes a hybrid ethical approach to address the complex issues surrounding modern computer systems, having first identified the reasons why a simplistic approach is insufficient.

INTRODUCTION

When invasion of privacy required a search of numerous buildings and searching through boxes, the action was restricted to those who had strong motivation – the 'average' employee had neither the will nor the access required to carry out the act. With the ability to search, link and change data at the press of a switch, an ethical vacuum has become apparent in that the perceived impact of a highly invasive or destructive act is not recognised by those carrying out the action and, when confronted, there is not sufficient ethical context for the perpetrator to judge the gravity of the situation. In addition, the existence of the notion of 'Hackers' Ethics' provides a basis for immoral and unethical actions from a business perspective. While a person may react to being caught, it does not necessarily follow that they will integrate this into their worldview to imply that the action itself was wrong.

In this chapter, I will provide a set of case studies and general rules that can be applied to provide an ethical basis for the development and implementation of security policies. In the second half of the chapter, I will address the teleological, deontological and virtue-oriented aspects of the

DOI: 10.4018/978-1-60960-573-5.ch010

ethics surrounding organisational ICT security policy to provide a more theoretical basis for an ethical organisation.

INFORMATION FOR MANAGERS

Your business is not secure in the absence of a formal policy on the responsible, secure and ethical use of technology. An individual's capacity for rationalisation, the possibility of unethical or ethically-ignorant employees, and the capabilities of modern technology combine to make it possible for an organisation's security to be compromised quickly, easily and with devastating effect (Harris & Ogbonna, 2010).

As we will discuss, existing professional codes of ethics may be useful, but there must be a well-established code of ethics that binds the organisation as a whole. These codes of ethics must be flexible, extensible and practical. Because of this, we are going to take the most suitable aspects from all of the frameworks, and propose a system that can be adapted to any business.

The core points of this chapter, for management, are:

1. Be ethically consistent. Apply one rule across your company, your employees and your clients.
2. Use as much security technology as you need to protect your systems and to carry out work efficiently.
3. Consider the impact on your staff of encouraging (or forcing) them to act unethically, even implicitly.
4. Clearly identify what the core ethical rules are for your business in plain language.
5. Provide clear guidance as to which professional ethics bodies you believe are the closest fit for your organisation.
6. Provide clear and explanatory duty statements to all of your staff.
7. Do not presume 'common sense' or a shared notion of reasonable behaviour. Your corporate culture cannot be based on "Well, you should have known that", it should be clearly written down and available.
8. A perfect security policy is only as good as the staff and equipment that implement it.

BACKGROUND

As more technology enters the workplace, we have seen the development of new professions and trades, or trade specialisations, to support office staff and business activities. Electricians are now often licensed as network cabling experts, systems administrators maintain software, hardware and networking systems, and business information specialists spend a great deal of time analysing and optimising the business processes for their clients. Information, and access to it, is a valuable commodity.

Information and Communication Technology (ICT)-rich businesses may be generally characterised as businesses that have a high proportion of their staff using a computer on a daily basis and depend upon the availability of the data stored in the firm's computer systems. There is also active use of the Internet.

ICT-rich businesses require at least two different staff roles: those staff whose core activities relate to the delivery of the company's products and those staff whose core activities provide the ICT support required to allow this to occur. Depending on the size, nature and maturity of the business, this second staff role may be provided by a third party, through a dedicated person or team of people, or through placing additional support roles onto another staff member.

Professional staff may already have a professional code of ethics that they can draw upon. The educational background required to perform competently, the level of accreditation required for employment in a number of sectors, and the