Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law
&
Security Review

The prospects of easier security for small organisations and consumers

Roger Clarke [a,b,c,*]

[a] Xamax Consultancy Pty Ltd, Canberra, Australia
[b] Australian National University, Canberra, Australia
[c] University of N.S.W., Sydney, Australia

Keywords:
Data security
Information security
Baseline security
Security profile
SME

ABSTRACT

Safeguards exist that provide at least a reasonable degree of protection for IT security. With so much accumulated knowledge in existence, why aren't consumer devices delivered with convenient security facilities? This paper identifies the reasons why neither consumers nor providers of these technologies take responsibility for security. It presents a framework within which simple baseline security can be established for small organisations, and consumers can also achieve lower levels of insecurity than currently prevail. It then investigates the scope for interventions to achieve 'easy security' for small organisations and consumers.

Nell picked up her new handheld, excited at the prospect of telling her friends about its new features. An avatar appeared on her screen, and introduced itself as Segard. Segard chatted with Nell about the main uses she wanted to make of her handheld, and what address-book she wanted to be loaded onto the device. Segard offered to set a number of defaults on the device that would balance convenience and security about right for Nell. Segard outlined how Nell could change those settings later, and how she could override them.

For Nell, Segard needed to take account of a couple of sensitivities about personal data, particularly health data, and who was to have access to her current location. Nell also wanted to not only keep apart her family and social networks, but also to segregate two incompatible groups of friends. The interactions were just interesting enough that Nell's patience hadn't quite run out before Segard completed the configuration process and relinquished control of the device.

[With thanks to Neal for the loan of one of his characters in 'The Diamond Age' (Neal Stephenson, 1995*).]*

1. Introduction

Large organisations should be capable of undertaking a rational approach to the security of their data and of their information technology (IT) artefacts. In Australia, for example, there are about 6000 large business enterprises (LBEs) and 6000 government agencies that are subject to legal requirements in relation to risk management and that are subject to frequent cyber-attacks. In addition, perhaps 25,000 medium-sized business enterprises (MBEs), 50,000 small-to-medium enterprises (SMEs), and even some micro-Enterprises (μEs), have adequate security expertise and reasonable safeguards in place.

Many other organisations, however, despite having considerable dependence on information and IT, have at best a hazy understanding of IT security. In Australia, these number perhaps 50,000 MBEs, 700,000 SMEs, and 250,000 μEs, or about 1 million organisations. Comparable

[*] Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman ACT 2611, Australia.
E-mail address: Roger.Clarke@xamax.com.au.

http://dx.doi.org/10.1016/j.clsr.2015.05.004

figures for the USA and the EU are 15–20 times those for Australia.

Meanwhile, many millions of individuals use IT artefacts. Particularly since the explosion in smartphone usage since the launch of the iPhone in 2007, and tablet adoption since the launch of the iPad in mid-2010, a lot of people operate multiple IT devices, are greatly attached to them for social purposes, conduct transactions on them that have financial implications, and generate, store and disseminate a considerable amount of data, some of it sensitive.

A further concern is that, at any given time, some 2–5% of the population are 'persons-at-risk', whose physical safety is dependent on their location not being apparent to one or more other individuals or organisations that bear a serious grudge against them (Clarke, 2001b; UKICO, 2009 p.19, GFW, 2011). A proportion of these individuals are aware of security risks and take at least some steps to address them. But the large majority of individuals, even of those at risk, are ill-informed, ill-prepared, and exposed.

Consumer devices now also play a major role within corporations and government agencies, because, as employees and contractors, many people use their devices in their workplaces, subject to more or less official Bring Your Own Device (BYOD) arrangements. This has the effect of extending the scope of each organisation's security risks well beyond its own devices to encompass those of its staff-members.

This paper investigates the various ways in which serious shortfalls in IT security might be overcome. It considers regulatory mechanisms, including the impacts of relevant laws, but it does not present legal analysis. The paper commences by identifying the reasons why consumers and small organisations fail to protect their own interests. It then outlines the shape that a suitable IT security framework might take, and provides specific proposals relating firstly to a baseline level of security for small organisations, and secondly to three levels of security profile for consumers. The later sections consider the prospects of IT providers addressing the problem, and identify alternative interventions to achieve security outcomes that are effective, efficient, and Nell-friendly.

2. Individual responsibility for security

In mature societies, self-protection is an element of functional literacy. People know to take precautions relating to the value of their home, the contents of their home, and their car. Small organisations also understand that it is their responsibility to look after their assets, and that without safeguards they will lose a lot of money. There is also widespread understanding that, to share some kinds of risk around, insurance is needed. The personal and business processes imposed by the insurance industry have the effect of reinforcing the message that property security matters.

Over many decades, the workings of the insurance industry have been adapted to deal with some of the blind-spots in individual self-responsibility. A great many individuals and even many small organisations fail to appreciate that a range of contingent liabilities exists in relation to harm to other people and their property, and that these liabilities may be sufficiently large to lead to bankruptcy. To cope with this, parliaments commonly make third-party personal cover obligatory for car-owners, and public liability cover is incorporated within home and contents insurance.

Whereas security safeguards for the home, its contents and cars are common, the same cannot be said in relation to data and IT artefacts. Many organisations and some individuals have sufficient assets, and are subject to sufficient threats, that considerable care is warranted. An organisation and its directors, if they take no precautions, are readily argued to have failed to fulfil their legal responsibilities. Nonetheless, some organisations and many individuals assume that the risks that they face are sufficiently limited and/ or unlikely that they can take quite limited precautions. Meanwhile, some organisations and most individuals simply do not, and will not, even think about security.

IT has always been a mystery to most consumers and indeed to many small organisations. The core of each device is microscopic, and its workings are complex, intangible and ephemeral. The technologies involved are difficult for most people to even conceive, and few grasp them in sufficient depth to enable them to conduct risk assessment, and to design and implement risk management plans. Hence, even in the current, fourth decade of 'personal computing', IT remains mysterious. Moreover, the IT mystery is deepening still further, as general-purpose computing devices are swamped by limited-function appliances, and data and processing disappear into the cloud (Clarke, 2011). This results in a lack of awareness among consumers about the security risks that arise from their use of IT. Small organisations also lack expertise in relation to the hardware, networks, systems software and applications software that they use, and even in relation to the associated personal and business processes.

Further barriers exist. Many consumers have strong tendencies towards hedonism and away from considered, reflective and responsible attitudes towards the use of their devices. Security features intrude into consumers' enjoyment of their devices, because they require a considerable degree of understanding and concentration in order to approve the installation of software, changes to terms of service, and changes to settings. The explanations provided are commonly incomprehensible to most consumers. In addition, it is entirely rational for consumers to value convenience highly – because they experience it continually – and to value security very low – because they experience the impacts of insecurity only occasionally and are largely unaware of the security incidents that affect their devices, their transactions and their communications.

Given that safeguards involve certain costs, but unseen and uncertain benefits, it is unsurprising that individuals and small organisations under-spend on security. For individual responsibility to become a significant factor in addressing the problem of inadequate IT security, a large number of conditions would need to be fulfilled. IT would need to be more transparent. There would need to be widespread awareness, education and training. Enough individuals and small organisations would need to incur liabilities, such that the public generally would come to appreciate the need for self-protection. In addition, IT security safeguards would need to become much more transparent, would have to be