Information Security Policies for Networkable Devices

Julia Kotlarsky
University of Warwick, USA

Ilan Oshri
Rotterdam School of Management Erasmus, The Netherlands

Corey Hirsch
Henley Management College, UK

INTRODUCTION

Recent years have seen a surge in the introduction of networkable Windows-based operating system (NWOS) devices. Some examples are home entertainment systems (e.g., Xbox), smart phones (e.g., Motorola i930 and PlamOne's Treo), and Pocket PC (e.g., Toshiba e850). While NWOS devices present an appealing proposition for both software vendors and buyers in terms of the flexibility to add supplementary software applications, such devices also introduce new challenges in terms of managing information security risks. NWOS devices are particularly vulnerable to information security threats because of the vendors' and buyers' lack of awareness of the security risks associated with such devices. In addition to the direct damage to business operations that an infected NWOS device might cause, other consequences may also include alienated customers and a tarnished reputation (Austin & Darby, 2003).

In this article, information security risks in NWOS will be explored and practices applied by one vendor will be outlined. First, some definitions of the key concepts discussed here will be provided and a review of recent discussions in the academic and practice literature will be presented. Following this, a discussion about the information security risks and the practices applied will be developed. Lastly, future research in this area and conclusions will be offered.

BACKGROUND

The information security literature has indeed discussed at length prevention, detection, and recovery strategies related to information security management (e.g., Joseph & Blanton, 1992; Jung, Han, & Lee, 2001); however, these studies mainly focused on computer- and Internet-related information security threats and highlighted practices associated with the management of software development and information systems that could offer protection from malicious software. In this regard, NWOS devices present an extended set of challenges that call for the development of additional capabilities by the vendor. Indeed, several studies have recently discussed the need to integrate software development and operational processes with strategic business objectives when building security into products (McAdams, 2004; von Solms & von Solms, 2004, 2005; Taylor & McGraw, 2005). Clearly, the careless management of information security of NWOS devices will not only risk the vendor's or the buyer's network environment, but could also harm the relationships between vendors and buyers, as malicious software may be transferred between their networks during production, sales, and after-sales activities. In a recent article, Arce (2003) acknowledges that networkable gadgets pose unique information security risks to vendors; however, little is so far known about the challenges faced and solutions applied by vendors when managing the information security of NWOS devices throughout the product lifecycle.

INFORMATION SECURITY RISKS IN NWOS DEVICES

While the literature on information security has addressed various issues relating to (i) best practices in managing information security programs (e.g., Joseph

& Blanton, 1992; Austin & Darby, 2003; Farahmand, Navathe, Sharp, & Enslow, 2003), (ii) risk management and evaluation of security management programs (e.g., von Solms, van de Haar, Von Solms, & Caelli, 1994; McAdams, 2004), and (iii) the links between the management of information security and operational activities (McAdams, 2004), recent studies have claimed that there is a serious lack of empirical research in this area (Kotulic & Clark, 2004), and in practice, firms rarely apply a systematic and methodological approach (Austin & Darby, 2003) that aligns their information security strategy with business objectives and operational processes (McGraw, 2004; von Solms & von Solms, 2004, 2005; Taylor & McGraw, 2005). Indeed, most vendors of off-the-shelf computing products will either "bundle" an information security solution into the product or give the buyer the freedom to select a solution that fits their needs. In this regard, the market for NWOS devices presents unique challenges, as a vendor of such devices is required to consider information security measures during different stages of the product lifecycle. This is mainly because most buyers of NWOS devices do not consider their devices to be a target for malicious attack by viruses or worms. However, being a NWOS device puts such a device under the same category of most personal computers and servers that operate on Windows platforms. Because of the large installed base of Windows-based platforms, these are subject to a large majority of hackers' attacks. Consequently, the risk for NWOS devices has become acute, and the challenges that some NWOS devices present to vendors and buyers may require the development of new capabilities. For example, NWOS devices that are designed for a particular usage (e.g., digital microscopes, digital storage oscilloscopes) impose interactions between the vendor and the buyer during the lifecycle of the product. Consider product demonstration activities during which an NWOS device could be connected to the local network to demonstrate its printing capabilities. Without considering the information security risks involved in connecting this networkable device to the buyer's network, in doing so, the vendor puts at risk the buyer's network and the demonstration product by allowing the transfer of malicious software from the buyer's network to the NWOS device and vice versa. The risk can be even more acute should the salesperson use the same device while visiting other clients, without protecting both the client's network and the demonstration device.

Table 1 summarizes information security risks that vendors and buyers of NWOS devices face which may lead to an information security incident if such risks are not managed properly.

In this article we consider information security measures in three stages in the product lifecycle. The stages are: *production, sales,* and *after-sales* activities. It is important that vendors approach each of these stages with awareness to the risks reported above and align operational activities with information security measures to reduce the vulnerability of the NWOS devices. Furthermore, from buyers' perspective, it is important to create awareness about the vulnerability of NWOS devices and offer tools that can protect the devices as well as assess vendors' practices to this problem.

In the following sections we discuss each of the three product lifecycle stages and offer a checklist of information security measures that can be useful for both vendors and buyers of NWOS devices. Vendors can learn from the checklist how to improve their information security measures at different stages of the product lifecycle. Buyers can use this checklist during vendor selection by inquiring bidding vendors about how they, the vendors, ensure security at each stage. We based these recommendations on research conducted at LeCroy, a supplier of data storage oscilloscopes.

Stage 1: Production

Because the production environment can also be a source of malicious software in itself, there are four key issues that vendors should consider:

- isolating the production environment from other networks
- educating the workforce not to bring portable memory devices into the production environment
- placing warning labels near connectors, and
- providing an antivirus package with shipment

The Implementation at LeCroy

LeCroy took some steps to isolate the production environment and improve engineers' awareness of information security issues relating to its NWOS products. To increase awareness, the company introduced an annual information security fair at which issues relating to