

available at www.sciencedirect.comjournal homepage: www.elsevier.com/locate/cose

**Computers
&
Security**



Information security in networkable Windows-based operating system devices: Challenges and solutions

Ilan Oshri^{a,*}, Julia Kotlarsky^{b,1}, Corey Hirsch^{c,2}

^aRotterdam School of Management Erasmus, P.O. Box 1738, 3000 DR Rotterdam, The Netherlands

^bWarwick Business School, Gibbit Hill, Coventry CV4 7AL, England

^cAssociate Faculty, Information Systems, Greenlands, Henley on Thames Oxfordshire, RG9 3AU, UK

ARTICLE INFO

Article history:

Received 1 November 2005

Accepted 8 September 2006

Keywords:

Information security

Networkable devices

Organizational capabilities

Management of security risks

Vendor–user relationship

ABSTRACT

This paper explores information security risks in networkable Windows-based operating system (NWOS) devices. While these devices face the same information security risks as any other Windows platform, NWOS devices present additional challenges to vendors and buyers throughout the product lifecycle. It appears that 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. Based on evidence collected from a manufacturer of Digital Storage Oscilloscopes, the paper offers a set of challenges faced and solution applied by this vendor in its interactions with buyers. In order to reduce the vulnerability of NWOS devices, the paper considers several information security measures for the production, sales and after-sales phases. Lastly, the paper outlines the business reasoning for both vendors and buyers to pursue this information security strategy.

© 2006 Elsevier Ltd. All rights reserved.

1. 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 and Darby, 2003).

The information security literature has indeed discussed at length prevention, detection and recovery strategies related to information security management (e.g. Joseph and Blanton, 1992; Jung et al., 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

* Corresponding author. Tel.: +31 10 408 1993; fax: +31 10 408 9013.

E-mail addresses: ioshri@rsm.nl (I. Oshri), julia.kotlarsky@wbs.ac.uk (J. Kotlarsky), corey.hirsch@henleymc.ac.uk (C. Hirsch).

¹ Tel.: +44 2476 524692; fax: +44 2476 5244539.

² Tel.: +44 1491 571454; fax: +44 1491 571635.

strategic business objectives, when building security into products (McAdams, 2004; von Solms and von Solms, 2004; Taylor and McGraw, 2005; von Solms and von Solms, 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.

This paper aims to address this gap by reporting on key information security challenges that vendors of NWOS devices face during the lifecycle of the product. In discussing these challenges, this paper will attempt to bring out aspects relating to the alignment of information security issues, operational activities and strategic objectives that a vendor should consider during the lifecycle of an NWOS product.

The challenges faced by vendors will be associated with three phases, critical to devising an information security strategy, during the product lifecycle: production, sales and after-sales. Furthermore, in this paper the solutions applied by a supplier of digital oscilloscope, LeCroy, a New York based company, to reduce the vulnerabilities presented by NWOS devices will be outlined per phase. Lastly, the paper will offer practical implications for vendors attempting to improve their information security strategy in the NWOS devices market.

2. Information security: the case of 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 and Blanton, 1992; Austin and Darby, 2003; Farahmand et al., 2003), (ii) risk management and evaluation of security management programs (e.g. von Solms et al., 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 and Clark, 2004), and in practice, firms rarely apply a systematic and methodological approach (Austin and Darby, 2003) that aligns their information security strategy with business objectives and operational processes (McGraw, 2004; von Solms and von Solms, 2004; Taylor and McGraw, 2005; von Solms and von Solms, 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 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 sales person 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 of NWOS devices face when managing their relationship with buyers.

Building on existing studies that consider the full lifecycle of software development (e.g. McGraw, 2004), this paper considers three key stages in product lifecycle in which vendors and buyers are likely to interact and in which operational activities can be aligned with information security measures to reduce the vulnerability of the NWOS devices and buyer's network. The key stages are: production, sales and after-sales activities. The design stage, though is important in building security into the product through software development tools and methodologies, presents little interactions between vendors and buyers that require the development of information security measures. The solutions applied by LeCroy, a vendor of Digital Storage Oscilloscopes (DSO) based in New York, will be discussed at length following the research method section.

3. Research background

An in-depth case study was carried out in August 2005 at LeCroy Research Systems, New York during which the challenges faced and solutions applied by this vendor of digital storage oscilloscopes were examined and analyzed. LeCroy Research Systems specializes in the design and production of oscilloscopes and other signal analyzer equipment. The company employs more than 400 people worldwide and its 2004 sales amounted to \$120 million. In particular, LeCroy's line of DSOs, also known as the WaveMaster and WaveRunner series, is of interest in this research. Being a networkable Windows-based operating system device, the WaveRunner posed new challenges to the management of information security of this vendor, which required the company to develop new capabilities related to their information security strategy. The research was designed to capture the information system risks involved in producing and maintaining the WaveRunner throughout the product lifecycle and to collect evidence as to

Table 1 – Information security risks for vendors of NWOS devices

Stage	Risks to vendor
Production	<ul style="list-style-type: none"> Malicious software that attacks the vendor's network may infect the production environment and NWOS devices.
Demonstration activities	<ul style="list-style-type: none"> Malicious software is transferred from the buyer's network to the NWOS device during demo activities. Sales person infects clients' network with malicious software when demonstrating product functionality that requires connection to the client's network, thus ruining the vendor's reputation.
Product delivery	<ul style="list-style-type: none"> Buyers do not consider the device to be networkable and a target for malicious software, so do not protect the device and its network. The product becomes a risk for the vendor upon return to the factory for repair or upgrade.
Maintenance and upgrades	<ul style="list-style-type: none"> Buyers do not update virus definitions, thus allowing malicious software to attack the NWOS device. Upon connection to the vendor's network for maintenance or upgrade activities, the vendor's network is at risk.

the solutions applied and capabilities developed by this vendor.

4. Information security in networkable Windows-based operation systems: evidence from LeCroy research systems

The trigger: In 2003, LeCroy introduced an oscilloscope (WaveMaster) that operated on Windows 2000. This operating system did not offer a firewall protection, and anti-virus software was not offered or installed on this particular product release. One unit was delivered to a LeCroy client in Japan. After a while, the client contacted LeCroy's service department with a complaint that the performance of this unit had worsened. To solve this problem, LeCroy suggested that the unit be sent back to the service department for inspection and repair. Anticipating a hardware malfunction or a software glitch in this particular machine, LeCroy's service engineers were surprised to find that this unit was infected by a malicious worm. LeCroy contacted the client and informed them about their findings. Later on, LeCroy learnt that the client

changed some of the settings in the unit that were supposed to provide some protection against malware, and the client also connected this unit to their network without consulting its own Information Systems (IS) department. Following this event, LeCroy re-evaluated its information security strategy by considering various measures needed in securing NWOS devices, as well as in the practices relating to interactions with buyers.

The change: Realizing that such events put at risk their relationships with buyers and might damage their reputation, the management at LeCroy started paying more attention to issues pertaining to the information security of the DSO. The following case description outlines the measures taken by the management to ensure that their information security strategy is aligned with operational activities and their business objectives. While the information security strategy developed constantly between 2003 and 2005, we have chosen to report the present state of LeCroy's information security strategy with regard to NWOS devices.

4.1. Information security practices for production activities

Acknowledging that the production environment can also be a source of malicious software, the management of LeCroy took some steps to isolate the production environment and improve engineers' awareness of information security issues relating to its DSO products. To increase awareness, the company introduced an annual information security fair at which issues relating to the company's information security strategy were presented and discussed. One engineer described it:

Every year we organize a Security Fair, [...] I do the DSO part because I'm in charge of production and I work on the DSO. [...] we have eight different stands where you can go and learn about security.

In addition, LeCroy introduced an isolated network for production to eliminate the possibility that malicious software would get into the production environment. One engineer explained:

[...] to avoid viruses, Trojan and any security threats, we build these machines on an isolated network. That means this network has no access to the Internet.

In addition, to ensure that the production network was isolated, engineers were instructed not to connect external devices (e.g. memory sticks and laptops) or use CDs on the production network.

The production procedure was updated to include a final virus check of the DSO before shipping it to a customer. Moreover, information package and anti-virus software were included in each product shipment. Buyers were advised to contact their Information System department prior to connecting the DSO to their network and to install anti-virus software of their preference. To ensure that buyers paid attention to the risk involved in connecting the DSO to the network, LeCroy placed a sticker on the Ethernet socket that said "This is a Windows networkable device; visit the security

website". This way, users had to consider the consequences of plugging this unit to the network without consulting their IS department. Lastly, LeCroy offered a recovery disk in each product shipment to ensure that, if a DSO did get infected by a virus, the buyer could always restore the unit to its original settings and start again.

4.2. Information security practices for sales activities

LeCroy invested in educating its sales force about information security issues. The objectives of this training program were twofold. First, it was necessary to educate the sales force to consider information security threats when performing product demonstrations at the buyer's site. This training included several practices that the sales force was asked to follow. For example, before product demonstrations requiring a connection to the local network, the salesperson should contact the IS department at the site and check their information security arrangements. In addition, the salesperson was instructed to perform a virus check following each product demonstration that included a connection to the network. Nonetheless, one major challenge that the sales force faced when attempting to implement these new practices was the difficulty in getting updates of virus definitions while on the road. This was solved through a synchronization process that the company supported, in which the latest virus definitions and patches were transferred to the salesperson, stored on a memory stick, and later on were uploaded onto the DSO.

The second challenge was to train the sales force how to educate buyers about information security risks concerning their DSO. This line of training was particularly challenging, as the sales force was mainly focused on getting "the deal done" and devoted less attention to technical matters. Nonetheless, the management at LeCroy emphasized the importance of educating their buyers about information security risks as a long-term business strategy. Indeed, salespersons, during visits to clients, provided clients with some information about the security risks involved in connecting the DSO to the network and the way to handle information security issues concerning the DSO. One manager explained LeCroy's approach:

We tell the customer if you are going to network this instrument, we advise you to contact your IS department and have them install an anti-virus. And we usually say use Norton's anti-virus, this is the one we use in the company: it's been tested on our products and we know that it works.

In addition, the salesperson walks the buyer through LeCroy's website to get them familiar with how security updates can be downloaded and updated. Finally, the company provides an anti-virus package in every box shipped.

4.3. Information security practices for after-sales activities

There are two key challenges relating to after-sales activities that LeCroy applied as part of its DSO information security strategy. One issue concerns the way DSOs sent back for repair or upgrade were handled upon arrival. The procedure

applied in this case was similar to the handling of products during production. One key difference was the immediate check for viruses of a returning DSO using an independent CD, ensuring that the unit was clean before admitting it to the service network. The second challenge relates to LeCroy's responsibility to test that updates from Microsoft, which often result in new updates for anti-virus software, do not affect the functionality of the DSO. To cope with this challenge, LeCroy tested each new update and informed its clients about the compatibility of the update through its website. One manager described this process:

[...] anytime new updates for Windows come up, new updates for anti-virus come up, [...] I have to test them on all our platforms. I have to make sure that all these do not affect the functionality of our products. [...] if there's a new update that doesn't work, then we will put the warning signs "do not install this update".

Reflecting on the evidence presented above, we argue that NWOS devices indeed pose new challenges to vendors in the way information security issues are managed throughout the product life. In the following section we present the implications for practice.

5. Implications for practice

The main objective in this paper was to report on the information security challenges faced and solutions applied by vendors of NWOS throughout the product lifecycle. Our early discussion outlined the challenges that vendors of NWOS may face in some critical stages in the product lifecycle. LeCroy, a vendor of Digital Storage Oscilloscopes, have addressed these challenges by introducing various measures that attempted to reduce the vulnerability of its NWOS products to malicious software and improve the usage of the product by its clients over time. In doing so, this vendor focused on improving information security practices during production, sales and after-sales activities by building capabilities that aligned their operational activities with their business objectives.

It was not our intention to offer a generic model for managing information security risks in the NWOS devices market. Rather, this paper highlights the importance of understanding the nature of challenges that a vendor of NWOS devices may face and to offer an insight into the set of solutions provided by this particular vendor. We acknowledge that the challenges and solutions associated with NWOS devices are context-dependent thus requiring additional research into this emerging market.

From a business objectives perspective, pursuing an information security strategy by applying some of the proposed practices in Table 2 can be beneficial for both vendors and buyers in the short- and long-term.

In particular, it is imperative that senior managers create an information security policy that takes into consideration the business objectives of the firm (e.g. the retention of clients). In devising such information security policy, senior managers should list down the firm's business objectives and the information security risks that may hamper achieving

Table 2 – Challenges and solution in managing information security for NWOS devices

Stage	Challenges	Solutions
Production	<ul style="list-style-type: none"> • Produce virus-free products 	<ul style="list-style-type: none"> • Increase awareness of information security issues through newsletters, fairs, security exercises and conferences • Isolate production network from firm's network • Check products for viruses before shipment • Provide essential information security tools in product package
Sales	<ul style="list-style-type: none"> • Ensure virus-free demo devices • Educate buyers about information security risks 	<ul style="list-style-type: none"> • Train the sales force to check for virus after each demo • Provide the sales force with the support to download virus definitions and updates while on the road • Provide buyers with critical information about information security risks
After-Sales	<ul style="list-style-type: none"> • Support buyer's virus-free usage of the device 	<ul style="list-style-type: none"> • Provide support for Windows and anti-virus packages over the web (test and confirm compatibility) • Check returning devices for viruses before connecting them to your network

them. In addition, the risks in each stage in product lifecycle (i.e. production, sales and after-sales) should be examined from information security viewpoint. For the production stage, the challenges can go beyond the control of management as more companies engage in outsourcing their manufacturing activities. In this case, senior managers require combining business objectives related to managing their supply network with the objectives related to client relationships. Assisting the subcontractor to secure and isolate their production network may seem as a sunken investment from the buyer viewpoint; however, such investments may prove to be critical for the vendor in terms of maintaining their clients satisfied and ensuring high retention levels.

Similarly, the sales and after-sales stages require top management's attention. The challenges involved in aligning business objectives with information security measures concern the handling of demonstration and defect devices. In such cases, third party service provider can also be involved as some companies outsource maintenance activities. Nonetheless, the most significant challenge is to educate the sales force to consider information security risks as part of their daily activities. As argued before, a salesperson would mainly be concerned with "getting the deal done", which is a short term business objective, and may pay less attention to technical and operational aspects such as securing entry points to the demonstration device and the client's network. These technical and operational aspects are in fact long-term strategic goals that if not carefully implemented, may alienate clients and ruin the firm's reputation.

What value is added from these information security measures? Through such information security measures, vendors of NWOS devices may differentiate their product from vendors who prefer to shift the responsibility for managing information security risks to their clients. Vendors of NWOS devices may offer extra value in offering support with information security risks, thus positioning their product as superior to others and possibly commanding premium prices for their products. In the long-term, bonding clients and vendors through such practices may improve the retention of existing

clients and may offer the vendor additional opportunities to promote new product introductions. In addition, buyers develop a degree of dependency on vendors through constant updates and upgrades related to anti-virus packages, which can in return serve the vendors in future offerings. Buyers, on the other hand, may enjoy a continuous support relating to information security issues from the vendor during the product life, a value-adding activity that also reduces the vulnerability of their network.

REFERENCES

- Austin RD, Darby CAR. The myth of secure computing. *Harvard Business Review* 2003;June:120-6.
- Farahmand F, Navathe SB, et al., Managing vulnerabilities of information systems to security incidents. The 5th international conference on electronic commerce ICEC03 Pittsburgh, PA, USA; 2003.
- Joseph GW, Blanton JE. Computer infectors: prevention, detection, and recovery. *Information and Management* 1992;23: 205-16.
- Jung B, Han I, et al. Security threats to Internet: a Korean multi-industry investigation. *Information and Management* 2001;38: 487-98.
- Kotulic AG, Clark JG. Why there aren't more information security research studies. *Information and Management* 2004;41: 597-607.
- McAdams A. Security and risk management: a fundamental business issue. *Information Management Journal* 2004;38(4): 36-44.
- McGraw G. Software security. *IEEE Security & Privacy* 2004;2(2): 80-3.
- Taylor D, McGraw G. Adopting a software security improvement program. *IEEE Security & Privacy* 2005;3(3):88-91.
- von Solms B, von Solms R. The ten deadly sins of information security management. *Computers and Security* 2004;23:371-6.
- von Solms B, von Solms R. From information security to business security. *Computers and Security* 2005;24:271-3.
- von Solms R, van de Haar H, et al. A framework for information security evaluation. *Information and Management* 1994;26: 143-53.

Dr. Ilan Oshri is Assistant Professor of Strategic Management, Rotterdam School of Management Erasmus, The Netherlands. Ilan holds a PhD degree in technological innovation from Warwick Business School (UK). His main research interest lies in the area of knowledge management and innovation. Ilan has published widely his work in journals and books which include *IEEE Transactions on Engineering Management*, *Communications of the ACM*, *European Journal of Information Systems*, *Information Systems Journal*, *Management Learning*, and others.

Dr. Julia Kotlarsky is Assistant Professor of Information Systems, Warwick Business School, UK. She holds a PhD degree in Management and IS at Rotterdam School of Management Erasmus (The Netherlands). Her main research interests revolve around social and technical aspects involved in the management of globally distributed IS teams, and IT

outsourcing. Julia published her work in *Communications of the ACM*, *European Journal of Information Systems*, *Information Systems Journal*, *International Journal of Production Research*, and a number of book chapters.

Dr. Hirsch has served as Associate Faculty in Information Systems, and subject tutor and course author in Customer Relationship Management Systems at Henley Management College since January 2002, and recently as tutor in Information and Communications Technology. He completed his Doctorate degree in Business Administration, awarded by Brunel University, London, and his Masters in Business Administration from the University of Oregon. Recently he has earned a Certification in Information Security Management (CISM) from Information Systems Audit and Control Association (ISACA).