

An Information Security Strategy for Networkable Devices

Networkable Windows-based operating systems devices present information security challenges to both vendors and users of such devices. This article highlights some of the threats that NWOS devices pose and offers measures to improve the link between a firm's business strategy, its operational activities, and its information security strategy.

ILAN OSHRI
Rotterdam
School of
Management

JULIA
KOTLARSKY
Warwick
Business
School

COREY HIRSCH
LeCroy
Corporation

In the approximately 60 years that digital general-purpose computers have been in use, many analog-based special-purpose machines have been redesigned in digital incarnations to exploit a myriad of inherent features, user interface benefits, and design reusability. Numerically controlled machine tools, cameras, televisions, and scientific equipment are a few examples. Because most of these devices use an embedded microprocessor, they require operating system and application software to convert them from general-purpose to special-purpose machines.

In recent years, many vendors have replaced traditional proprietary buses and operating systems with industry standards, and many have offered these devices as networkable Windows-based operating systems devices. NWOS devices require vendors to make smaller design investments in low value-added areas, such as writing hardware drivers and file-management systems. However, many vendors fail to grasp the corresponding requirement—that is, to become knowledgeable about information security and provide a comprehensive security regime to protect downstream organizations (that is, users).

Information security practitioners must defend against several routes of malware contagion.^{1,2} These include traditional “tunnels and bridges” that bypass the firewalled corporate perimeter, such as visitors' laptops, virtual private network (VPN) tunnels, and encrypted and zipped email attachments. However, NWOS devices and appliances have been mostly overlooked as potential security threats. Corporate networks that are otherwise highly secure often have some tens of nodes that aren't generally recognized as computers but that run NWOS. These devices range from smart phones to engineering micro-

scopes, and from oscilloscopes to print stations.³ They might have no single owner, and frequently generic or group user accounts are established on them.

We wrote this article with enterprise networks in mind, especially those with several hundred nodes. Today, myriad tools, including antispam, antivirus, anti-spyware, autopathing, encryption, firewalls, and intrusion detection and prevention, often protect these networks. Processes are also vital in locking down large networks, and many organizations have implemented policies regarding password strength, access control, and patching and virus definition updating, all of which rely on the “one machine, one owner” concept. These tools and processes probably won't encompass network nodes that were purchased, for example, by the facilities or engineering departments. For example, a shared microscope might offer a soft node in an otherwise hardened network, and serve as a platform from which to gain unauthorized access, conduct internal reconnaissance, and propagate damage. A hospital with several medical imagers on its network, a university physics lab with 20 oscilloscope stations, a business whose office staff keeps their PDAs in cradles, and a document copy/print station face the same potential threat.

Security vulnerability in NWOS devices

The professional media has disclosed several security vulnerabilities in popular NWOS devices. For example, on 3 March 2003, SecurityFocus, a community of security professionals, announced (www.securityfocus.com/bid/7004/discuss):

“It has been reported that some Siemens mobile phones are unable to sufficiently handle certain SMS message content. If a maliciously formed SMS message contains certain characters, the mobile phone firmware will behave in an unstable manner. Exploitation of this issue may result in a target phone no longer functioning.”

On the same day, SecurityFocus released the following announcement (www.securityfocus.com/bid/7001/info):

“It has been reported that Hewlett-Packard JetDirect printers leak the web JetAdmin device password under some circumstances. By sending an SNMP GET request to a vulnerable printer, the printer will return the hex-encoded device password to the requester. This could allow a remote user to access and change configuration of the printer.”

And, on 9 January 2004, the Common Vulnerability and Exposure Group (CVE) reported the following threat (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0103>):

“Format string vulnerability in Nokia 6210 handset allows remote attackers to cause a denial of service (crash, lockup, or restart) via a Multi-Part vCard with fields containing a large number of format string specifiers.”

This article deals with recognizing and mitigating vulnerabilities associated with Microsoft networking and Windows operating systems in embedded systems and devices. We provide vendors of such systems with precautionary measures, and users with checklists to help them to select secure products and vendors. Our empirical findings are based on research conducted at LeCroy, a New York-based vendor of digital oscilloscopes and general-purpose NWOS devices. Until 2003, LeCroy based its products on proprietary operating systems developed in-house. In early 2003, LeCroy introduced WaveMaster, a new product operating on Windows 2000. Since then, most LeCroy products have used the Windows operating system.

Risks of NWOS devices

Most vendors of off-the-shelf computing products either bundle an information security solution into the product or let users select a solution that fits their needs. This presents the market for NWOS devices with unique challenges because vendors of such devices must consider additional information-security risks:

- End-user departments often purchase the NWOS devices, so the security team might be unaware of them.

- The network might not recognize the devices as computers.
- NWOS devices might have multiple users and shared accounts, with no one person responsible for securing the device.
- Some NWOS devices run multiple operating systems (for example, multifunction devices such as combined printer/copier/fax machines), increasing the risk of attack.
- Some NWOS devices move in and out of the organization through a portal not widely considered: the loading dock.
- Vendor practices vary widely with regard to securing NWOS devices.

However, NWOS devices are in the same category as most Windows-based personal computers and servers. And, because of the large installed base of Windows-based platforms, they're subject to most hacker attacks. Consequently, the risk for NWOS devices has become acute and the challenges they present require new capabilities. For example, NWOS devices that are designed for a particular use (such as digital microscopes or digital storage oscilloscopes) impose interactions between the vendor and the client during demonstration and postsale activities. Consider product demonstration activities during which an NWOS device is connected to the potential client's local network to demonstrate its printing capabilities. In connecting this networkable device to the client's network, the vendor puts at risk both the client's network and the demonstration product by making possible the transfer of malicious software from the client's network to the NWOS device and vice versa. The risk can be even more acute if the salesperson uses the same device while visiting other clients, without protecting both the client's network and the demonstration device.

Although these information security risks seem technical and operational in nature, they put the firm's business strategy at risk. The firm must therefore tighten the links between information security strategy, operational processes, and business objectives.⁴ In addition to the di-

Although information security risks might seem technical and operational in nature, they can put a firm's business strategy at risk.

rect damage to business operations that an infected NWOS device might cause, consequences from a marketing and sales viewpoint could include alienated customers and a tarnished reputation.

Building a strategy

Information security measures occur in four stages of the product life cycle: design, production, sales, and postsale. Vendors should be aware of the risks in each of these stages and align operational activities with information security measures to reduce NWOS device vulnerability.

Clients should also be aware of NWOS device vulnerability and have tools that let them use the devices securely as well as assess and compare potential vendors according to their information security policies.

We've developed checklists of information security measures for vendors and users of NWOS devices. Vendors can use these checklists to improve their information security measures at different stages of the product life cycle. Clients can use the checklists to select vendors based on how they ensure information security at each stage.

Stage 1: Product design

Design choices as fundamental as motherboard, processor, and chipset will affect the resulting NWOS device's long-term security. Vendors might choose a line of commercial components, seeking the latest-revision processors, memories, busses, and peripherals in support of frequently improved banner spec claims. Alternatively, they might choose original equipment manufacturer lines in support of stable, more secure platforms over time. Software will often track hardware revision levels, so component choices made early in design will influence the vendor's *dwell time*—that is, the time the vendor stays with a particular version of application before upgrading—on a given operating system. Indeed, operating systems have a security “sweet spot” as they age: new releases have undiscovered vulnerabilities, while old operating systems are unsupported and without patches when vulnerabilities are found.

NWOS device vendors should therefore carefully consider their customer's security needs and be able to explain how their adoption practices optimize the trade-off between processor banner specs and overall system security. For example, hardware security features, such as the Intel disable bit architecture, can play a part in the vendor's chip and chipset selection, and the application software design can be compatible with future operating system patches.

LeCroy implementation. Indeed, design choices might reflect on the vendor's security culture. At LeCroy, for example, the security and design team examined several possible solutions at the design stage. These alternatives provoked questions in the context of LeCroy's product line:

- Is antivirus a standard accessory?
- Are other security options, such as dual factor authentication or a firewall, available?

- Are removable drives an option?
- Have we considered customers' diverse security requirements and preferences, such as a preference for one antivirus package over another?

Vendors should consider an operating system's security when licensing the software. A choice that limits the user's ability to operate a secure device introduces needless and severe security risks. The license, for example, might limit the device to two applications, in which case the device's application program would use at least one, eliminating the possibility of running both antivirus and a risk-management package. The operating system license might also impact allowed methodologies for automated operating system patching.

Client checklist. A client can ask certain questions to uncover key indicators of vendor maturity with regard to information security. These questions should include:

- What is your design-for-security strategy with regard to hardware and mechanical and operating systems?
- What product hardware and software options do you provide or support to reduce security risk?
- What end-user license agreements come with the product?
- What steps have you taken to ensure that the application program will be compatible with future security patches?
- Have you disabled any of the operating system's standard features?
- Does the application have any back doors or hard-coded passwords?
- Do you perform regression testing on new operating system and application updates?
- Are application updates digitally signed?
- What strength encryption, if any, does the device use?
- Does the antivirus come with performance specifications?
- Will running antivirus (or antispysware) real-time protection interfere with the application program?
- Does the application program perform user authentication; and if so, does it use secure methods?
- Does the device have potentially insecure access, such as a CD-ROM, that will accept a Windows recovery CD?

In some cases, the salesperson will have to refer the question to a security team member.

Stage 2: Production

Because the production environment can also be a source of malicious software, vendors should consider isolating it from other networks and educating the workforce not to bring portable memory devices into the production environment. To make clients aware of information security risks, vendors can place warning labels near

What to consider when choosing an antivirus package

In selecting an antivirus package, the vendor should pay attention to several aspects:

- The antivirus software product should be accepted among the target market segment for the embedded device.
- The chosen package should allow for a delay between the vendor's original purchase and the start of the license period (when the end user installs the software).
- The package should be fully licensed, as only this will actually protect users in the long term.

Some technical constraints could effect an antivirus package's selection. Antivirus packages can interact badly with other applications. For example, some security products, such as antispyware packages, have exhibited mutually destructive interaction with certain antivirus packages, with each application perceiving the other as malware. For this reason, the vendor must test antivirus

packages for compatibility with its own appliance application code as well as with applications that customers commonly run on the appliance.

Furthermore, because antivirus products consume resources (such as CPU cycles, disks, and memory), they can affect device performance. So, the vendor should provide an antivirus package but not install it. The vendor should provide key device specifications both with an antivirus package installed and active, and without it. Users can set antivirus packages to minimize performance degradation by, for example, scanning at night or throttling the CPU load.

Vendors should manage operating system security upgrades and updates on a weekly and monthly cycle. Microsoft, for example, publishes their patches every second Tuesday of each month, giving vendors a week to test them before deploying them internally. Vendors should also update customer instructions on their Web sites whenever new relevant information arises.

connectors. Indeed, most NWOS devices (such as PDAs, videogame appliances, and smart phones) are shipped to customers without such warnings. Finally, vendors should provide an antivirus package with each shipment.

LeCroy implementation. 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 where the security staff presented and discussed issues relating to the company's information security strategy. In addition, LeCroy designated a production network to eliminate the possibility of malicious software entering the production environment. To ensure that the production network was isolated, engineers were instructed not to connect external devices (such as memory sticks and laptops) or use CDs on this network.

LeCroy updated its production procedure to include a final virus check of the NWOS device before shipping it to a customer. Moreover, it included an information package and antivirus software in each product shipment. The information package advised clients to contact their IT department before connecting the NWOS device to their network and to install an antivirus software of their choosing (for guidelines on selecting an antivirus package, see the sidebar). To ensure that clients pay attention to the risk involved in connecting the NWOS device to the network, LeCroy placed a sticker on the Ethernet socket that said, "This is a Windows networkable device; visit the security Web site." Clients therefore had to consider the consequences of plugging the unit into the network without consulting their IT

department. Lastly, LeCroy offered a recovery disk in each product shipment so, if an NWOS device was infected by a virus, the client could restore the unit to its original settings.

Client checklist. Few clients will visit a vendor's plant to see what information security measures the vendor takes during production. However, a vendor should be willing to host such a visit if a client wishes (and it doesn't hurt to inquire). Even without traveling, a client should be able to learn a good deal by contacting the head of the vendor's security team. The client should ask the following questions:

- Do you manufacture the product in your own facilities, or those of a contract manufacturer? If you use a contract manufacturer, how do you ensure that their production line is secured?
- Are isolated networks in place for production (and later servicing) of the product?
- Do production or service networks contain out-of-support (old) nodes? Is the production equipment certified to be malware-free?
- Do you externally scan each box prior to shipment? With what tool? (Internal scanning tools introduce difficulties for customers who prefer a tool other than that which the vendor chooses to embed.)
- How often do you update master images to reflect the most recent patches?
- Do recovery CDs reflect recent images?

When asking these questions, buyers can also consider their own information security procedures and improve them according to the best-practices applied by their vendors.

Stage 3: Sales

For sales activities, vendors should consider developing a methodology to communicate important security information to clients. The sales force should also be

Clients should ask to see any training documents, brochures, or security materials that their salesperson has received within the year.

knowledgeable about security issues. Finally, vendors should provide technical support for remotely updating virus definitions

LeCroy implementation. LeCroy's objectives in educating its sales force about information security issues were twofold.

First, it taught the sales force to consider information security threats when performing product demonstrations at client sites. This training included several practices for the sales force to follow. For example, before product demonstrations requiring a local network connection, the salesperson should check the site's information security arrangements. In addition, the salesperson should perform a virus check after each product demonstration involving a network connection. A major challenge for the sales force in implementing these new practices was the difficulty of updating virus definitions while on the road. LeCroy solved this problem through a company-supported synchronization process that transferred the latest virus definitions and patches to the salesperson, who stored them on a memory stick and later uploaded them onto the NWOS device.

Next, LeCroy trained the sales force to educate clients about NWOS device information security risks. This training was particularly challenging because the sales force's main focus was on "getting the deal done" and less on technical matters. Nonetheless, LeCroy's management emphasized the importance of educating clients about information security risks as a long-term business strategy. The sales staff learned to walk clients through LeCroy's Web site to demonstrate how they can download security updates. Finally, the company provides an antivirus package in every box shipped.

Client checklist. By the time a salesperson visits a potential client, he or she has already taken the demo NWOS to several other locations. To ensure that the demo NWOS device doesn't present risks to the client's network, the client's IT department, security team, and application end users should check it. The client should further investigate

the vendor's information security capabilities by asking the salesperson the following questions:

- What precautions do you take prior to connecting the device to my network?
- What precautions do you take to ensure that your laptop PC has no malware contagion?
- How does your firm guard against spam, malware, and spyware on your networks in general, and on demonstration units and sales staff PCs in particular?

The client should also ask to see any training documents, brochures, or information security materials that the salesperson has received within the year.

Stage 4: Postsale activities

A vendor's postsale activities involve maintenance and upgrades. During this stage, vendors should consider how they can isolate the customer-service environment from other networks, and ensure that the application software is compatible with operating system updates and virus definitions

LeCroy implementation. LeCroy handles NWOS devices returned for repair or upgrade similarly to its handling of products during production. One key difference is its immediate check of returned NWOS devices for viruses using an independent CD. This ensures that the unit is clean before it's admitted to the service network. LeCroy regularly checks for Microsoft updates, which often result in antivirus software updates, testing each new update and informing clients about the update's compatibility through its Web site.

Client checklist. The client's postsale activities start at product delivery and deployment, and continue with maintenance and upgrades. A client should ask the following questions about vendor processes at this stage:

- What is your software support and version update process?
- Do you provide active (via email, for example) or passive (such as posting on your Web site) security updates, such as advice on service packs or patches?
- Do you scan products before connecting them to a network during repair?
- Is the repair network isolated?
- Do you scan products before returning them to clients?
- If you discover a security problem, will you contact us to offer a range of possible methods for dealing with it?
- How do you insure the privacy of data stored on the device during servicing?

To ensure security when the NWOS device is connected to the network, the client should involve the IT depart-

ment in the device's deployment. The client should also check the vendor's Web site for information about the warranty period, newly discovered operating system vulnerabilities, and the information security policy. Information about the policy can help the client assess whether the vendor took proper measures during maintenance activities, such as calibration and repair.

Information security and business strategy

Because our findings are based on one case study, they meet the transferability criteria to only a limited extent (that is, the extent to which we can replicate the findings across cases). We'll need additional research across multiple case studies to verify our findings. With this in mind, we can explore the approach to improve information security in NWOS devices by both vendors and users, recognizing that not all of LeCroy's practices are appropriate for other NWOS device vendors.

Indeed, following our suggestions will improve the links between a firm's information security policy, operational activities, and business strategy. Recent studies have recognized that senior and middle managers (such as the chief information officer and chief information security officer) must create an information security policy that aligns with the firm's business objectives (such as client retention).^{5,6} In devising such a policy, the chief information officer, with the chief executive officer and other senior managers (such as the director of sales and director of engineering), should list the firm's business objectives and the information security risks that might hamper their efforts,⁷ and clearly assign responsibilities to the functional teams involved in delivering security to clients.

Detecting and overcoming information security vulnerabilities in NWOS devices in each stage of the product life cycle requires cooperation among the engineering, production, sales, and security teams.

In the design stage, the security team should work closely with the engineering division to consider the long-term implications of selecting one design versus another, even a chip selection or an operating system patch update. The sales team's role is also critical in this stage because the client's preference for managing security issues after delivery is an important consideration.

In the production stage, the security team, along with the production team must secure the product network and educate the workforce to keep the production network isolated from other networks within the firm as well as from the Internet. The security team must also address the loopholes that might be discovered in some production areas.

Nonetheless, information security challenges could go beyond management control as more companies outsource their manufacturing activities. In this case, the information security team might need to combine business

objectives related to managing their supply network with those related to client relationships. We know little about the management of information security in the outsourcing relationship, a gap that calls for further study.

Similarly, in the sales and postsale stages, the security team must implement information security measures while working closely with the sales team. The most significant challenge here is training the sales force to consider information security risks as part of their daily activities. As we argued earlier, a salesperson is often concerned with completing the deal, paying 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, could alienate clients and ruin the firm's reputation.

We can't report on the cost/benefit ratio associated with implementing such information measures. However, managers at LeCroy report that since implementing the measures we've described, they've had no information security incidents in which a client's network was infected because of LeCroy's activities. In a way, avoiding bad publicity and upset customers is an achievement in itself. To improve the effectiveness of these information security procedures, companies should develop methods to assess their NWOS information security policy's impact on their business objectives. For example, a company could

- conduct customer surveys that link customer satisfaction and retention with the information security policy;
- continuously monitor the firm's performance against the industry's average rate of information security incidents; and
- monitor the number of customer visits to the security page of its Web site (a high number could indicate good customer security practices).

Nonetheless, we need further research before we can present a complete metric for the success of information security in NWOS devices.

What value do these information security measures add? They can differentiate one vendor's product from those of vendors who shift the responsibility for managing information security risks to clients. By offering support for information security risks, NWOS device vendors can position their product as superior to others and possibly command premium prices. In the long term, such practices might improve client retention and offer the vendor additional opportunities to promote new products. In addition, clients develop a degree of dependency on vendors through constant antivirus updates and upgrades, which can serve the vendors in future of-

ferings. Clients, on the other hand, might enjoy a vendor's continuous support of information security issues throughout the product life, a value-adding activity that also reduces their network's vulnerability. □

References

1. J.A. Hoffer and D.W. Straub, "The 9 to 5 Underground: Are You Policing Computer Crimes?" *Sloan Management Rev.*, vol. 30, no. 4, 1989, pp. 35–43.
2. S.D. Ryan and B. Bordoloi, "Evaluating Security Threats in Mainframe and Client/Server Environments," *Information & Management*, vol. 32, no. 3, 1997, pp. 137–146.
3. I. Arce, "The Rise of the Gadgets," *IEEE Security & Privacy*, vol. 1, no. 5, 2003, pp. 78–81.
4. D. Taylor and G. McGraw, "Adopting a Software Security Improvement Program," *IEEE Security & Privacy*, vol. 3, no. 3, 2005, pp. 88–91.
5. B. von Solms and R. von Solms, "From Information Security to Business Security," *Computers & Security*, vol. 24, no. 4, 2005, pp. 271–273.
6. A. McAdams, "Security and Risk Management: A Fundamental Business Issue," *Information Management J.*, vol. 38, July/Aug. 2004, pp. 36–44.
7. B. von Solms and R. von Solms, "The Ten Deadly Sins of Information Security management," *Computers & Security*, vol. 23, no. 5, 2004, pp. 371–376.

Ilan Oshri is an associate professor of strategy and technology management in the Rotterdam School of Management, the Netherlands. His main research interest is information systems and knowledge management. Oshri has a PhD in technological innovation from the Warwick Business School, UK. Contact him at ioshri@rsm.nl.

Julia Kotlarsky is lecturer in information systems, Warwick Business School. Her main research interests focus on the management of information systems and social and technical aspects involved in globally distributed teams. Kotlarsky has a PhD in management and information systems from the Rotterdam School of Management, the Netherlands. Contact her at Julia.kotlarsky@wbs.ac.uk.

Corey Hirsch is the chief information officer of the LeCroy Corporation, New York. He's also a visiting executive fellow at Henley Management College, UK, where he's subject leader in customer relationship management systems and competitor intelligence. His research interests are information security and enterprise risk management. Hirsch has a DBA from Henley Management College. He is a member of Information Systems Audit and Control Association's (ISACA), Albany, New York, chapter. Contact him at corey.hirsch@henleymc.ac.uk.