

I D C E X E C U T I V E B R I E F

Creating Corporate Policies to Protect IT Infrastructure

January 2009

Adapted from *Counterfeit Products: Protecting IT Infrastructure Integrity* by Joseph Pucciarelli,
IDC #ICUS20839107

Sponsored by Cisco

Introduction

The relentlessly evolving nature of IT technology, new process-enabling applications, and changing suppliers has conspired to create a new, unexpected problem for IT managers — the issue of uncertified IT equipment being installed within the corporate IT infrastructure. Uncertified IT equipment, defined as "new" or used equipment not sourced, or recertified, through the OEM-authorized reseller channels, includes counterfeit, stolen, third-party refurbished, and other unknown heritage products. Once installed, uncertified IT equipment can increase risks associated with business continuity, security, legal and regulatory, and financial issues.

Uncertified equipment can find its way into the IT supply chain through a variety of avenues. It may be offered as "new" equipment from a nonmanufacturer-certified reseller, through a broker seeking to move "extra" equipment, or via a "surplus" lot of new equipment on a semianonymous auction Web site. And, the price will be right — often 30% to 40% below that of certified sellers. Uncertified used equipment — that is, used equipment not returned to the manufacturer for testing, recalibration, and updating to the latest software release — is available from even more sources, including companies selling excess gear, leasing companies or banks selling returned or repossessed equipment, or liquidators and brokers. By some estimates, nearly 10% of certain kinds of IT components in the IT supply chain are counterfeit.

IT managers, who are already working with tight budgets and who are further taxed by challenging economic conditions, may be tempted to opt for the least expensive IT equipment available from nonmanufacturer-authorized reseller channels. This paper explains the inherent dangers posed by uncertified IT equipment, outlines why organizations need to create or update their corporate policy for IT equipment, and provides guidance as to how organizations can best get started.

Risks of Uncertified IT Equipment

Uncertified IT equipment is generally introduced into corporate systems inadvertently. Buyers looking for discontinued products to maintain the existing infrastructure, an emergency replacement for a failed unit, or better pricing on new products to fit into constrained a IT budget are just a few of the possible scenarios that could introduce the uncertified equipment. Uncertified IT equipment poses four types of risk: business continuity, security, legal and regulatory, and financial.

Business continuity risks arise when the system is not able to provide the required IT service levels to its internal and external customers. This is manifested in the form of system performance degradation, network instability, loss of scalability, and frequent system downtime due to functionally inferior and, in some cases, unsafe equipment. For example, counterfeit equipment may fail prematurely due to the use of inferior components. Third-party refurbished equipment may be improperly refurbished, lack critical hardware upgrades, or use components that don't meet OEM standards. Further exacerbating this situation is that uncertified equipment is not supported by the manufacturer and may, depending on specific provider terms and conditions, invalidate support for an entire system.

Uncertified IT equipment may introduce new or magnify existing system security vulnerabilities that result in loss of network control and compromised access to private data. Counterfeit hardware may contain malicious software that creates system backdoors or exploits existing vulnerabilities. Other uncertified equipment may contain outdated operating software, lack required critical software patches, or be functionally obsolete from a system protection perspective.

The introduction and usage of counterfeit, stolen, and improperly licensed equipment may put the business at legal risk with law enforcement agencies. Other uncertified equipment may not be compliant with such environmental regulations as Restriction of Hazardous Substances (RoHS) and may have been imported into the country of use illegally. It may not meet UL, FCC, EMI/EMC, and other product, safety, and health standards and corporate regulations.

Beyond the regulatory and compliance risks uncertified IT equipment poses, the additional performance risk it introduces into an organization's IT infrastructure may be its most significant attribute. Lost sales may result from an IT infrastructure that is unable to support business and revenue generation operations. Theft of intellectual property due to security breaches impacts future revenue generation. Lawsuits may arise from external customers whose own businesses are adversely impacted or from customers whose private data has been compromised. Other financial costs may be incurred, including the purchase of replacement units, software licensing fees, and software upgrades to compliant versions. The business may also be subject to legal and criminal fines arising from the possession of stolen, counterfeit equipment and unentitled access to support services.

Corporate Policies Protect Network Integrity

For most IT departments, the idea of establishing a corporate policy for things such as software applications and even PC use is common. After all, software use is governed by licensing agreements that, when violated, can lead to penalties and regulatory compliance problems. The security issues related to the inadvertent or deliberate misuse of PCs — both desktops and laptops — are also well-understood by IT departments, and hence corporate policies are in place to address them.

Similarly, a corporate policy for IT equipment procurement is needed to mitigate the risks associated with uncertified IT equipment. By taking a systematic and formal approach — in the form of either a new corporate policy specific to IT components and equipment or an amended corporate policy — IT managers can proactively safeguard against having uncertified IT equipment and components in their infrastructures.

Building a Corporate Policy for IT Equipment

An effective corporate policy consists of three elements: guiding principles, components, and processes.

Key Policy Principles

The following key principles can help guide any company as it starts to create its own corporate policy for IT equipment:

- The company is committed to maintaining and operating an IT infrastructure compliant with all security, privacy, trademark, intellectual property, and environmental laws of each country in which it operates.
- The company chooses to acquire new and refurbished IT equipment and components from OEM-certified channels. The equipment must come with manufacturer warranties and be certified for sale in the country in which it will be domiciled.
- When new and refurbished IT equipment is not available from OEM-certified channels, the company requires that third-party refurbished and used IT equipment cannot be installed within the IT infrastructure until it has been recertified as compliant with industry, government, and any specified manufacturer compliance standards (e.g., FCC, UL, CE, SA, RoHS), unless the OEM is no longer in business. All products must be provided with the valid OEM licenses and must contain the latest OEM software releases. When possible, the company may request that the product suppliers provide an unbroken, traceable, and documented heritage leading back to the OEM and be supportable through manufacturer product support channels.

- Supplier process certifications and documentation (e.g., ISO) must not be substituted for compliance with any OEM license, governmental, or international regulation or OEM certification.
- The company is committed to maintaining the IT infrastructure in a manner such that the license terms and conditions for equipment, components, and software remain compliant with manufacturer and corporate policies.

Key Policy Components

The specifics of any corporate policy will vary based on the organization, yet any corporate policy governing IT equipment should essentially include the following components:

- A mission statement outlining that the objective of the policy is to provide information regarding processes designed to guide the acquisition of new and used IT equipment
- A definitive list of procurement or IT personnel (including company contractors and agents, if applicable) who are authorized to purchase specific IT equipment
- A requirement that equipment, software, and services be acquired from vendors or resellers certified by the manufacturer to deliver products or perform services
- A definitive compilation of the IT technology covered by the policy, including equipment components, subassemblies, replacement parts, software, and services
- A list of the major requirements to be complied with — corporate, regulatory, health/safety, environmental, and so on
- A clear and concise summary of the potential security/legal/performance issues that may result when uncertified IT components and equipment are used, such as security vulnerabilities, software licensing risks, regulatory compliance issues, and so on

Key Policy Processes

Once the baseline components of the policy are established, the next step is to put in place processes that ensure that the policy stays current. To create the most comprehensive corporate policy, personnel from IT, procurement, legal, and finance should be involved in establishing and maintaining the following processes:

- Requesting and receiving new and refurbished IT equipment
- Qualifying and/or vetting resellers/channel partners
- Handling exceptional situations, such as when a certified vendor/reseller does not have the needed IT equipment

- Auditing and verifying compliance, including conducting reasonable tests as are deemed necessary to verify compliance with the policy
- Maintaining the list of authorized personnel within the organization
- Systematically certifying vendors or resellers through a comprehensive independent process, ensuring it is kept current and tightening policies to ensure minimum purchase thresholds do not create avenues for uncertified equipment
- Identifying a procedure for systematically auditing, removing, and reporting suspect uncertified equipment
- Reviewing and updating the policy on a periodic (annual) and exception basis such as a merger or an acquisition, when a major technology is replaced or discontinued, "emergency" situations when equipment is needed on a rush basis, or other unusual circumstances

Conclusion

The current economic volatility will bring increased competition, higher levels of used equipment from discontinued operations, and more nefarious behavior — all increasing the amount of uncertified, and potentially fraudulent, IT products circulating within global markets. As a result, IT departments must revisit their procurement policies. Now is the time to update and/or revise corporate IT procurement policies to include a clear and formal directive prohibiting the acquisition of uncertified IT equipment — that is, equipment that has not been certified by a bona fide servicing agent to be at the most current software release and performing at factory specification. Proactively addressing the issue of uncertified IT products now through a clear corporate policy will offset the likelihood of spending time with the corporate legal department later.

By establishing a clear and concise policy, and communicating both its existence and its purpose to the appropriate personnel, the IT department can safeguard the organization from the business continuity, security, legal and regulatory, and financial concerns that are associated with using uncertified IT equipment.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2009 IDC. Reproduction is forbidden unless authorized.