Sneaker Systems, Inc.

Security Assessment Report

Assessment of Security using the ISO-17799 Standard
@
World Wide Tools, Inc.
(WWT)

December 16, 2005

Table of Contents

World Wide Tools Security Assessment

Executive Summary

This document will be used to discuss the detailed security assessment being developed by Sneaker Systems, Inc. for World Wide Tools, Inc. (WWT). WWT has recently considered installation of a new ordering system for their company. This new system will vastly change the dynamics of their systems. We have successfully completed our pre-assessment and on-site assessment, and data gathered from these analyses have allowed us to deliver several recommendations for improving security in the areas covered by the ISO 17799.

We have identified several areas in which WWT is doing quite well, but there are some areas that could be changed without a dramatic impact on WWT's security budget. For example, WWT's General Computing Policies/Acceptable Use Policy addresses everything expected of an employee and clearly states what will occur if violations are detected. The company has also done an excellent job in defining the responsibilities of the Information Security Officer, Administrator, and Auditor. It has also ensured accountability by making all on-line or batch actions auditable to the individual for both users and programmers. WWT has increased the likelihood of confidentiality, integrity, and availability by using access controls, system surveillance, and encryption on the AS/400s. WWT is also on the right track with separation of duties: programming and operating functions are not performed by the same individual, and the company encourages cross training of operations staff.

Our team generated a list of vulnerabilities and assessed risk impact on three levels: high, medium, and low, and estimated risk probabilities as a percentage. Our assessment identified six high impact, high probability items that require the most attention. Four of these items are related

to the rollout of laptops for salesmen using the Perfect Orders System. The document shredding vulnerability concerns confidentiality and possibly compliance, and the vulnerability involving employee access after termination concerns operational security. Detailed descriptions of all vulnerabilities are listed in the remainder of this document. The scale for Effective Risk measure is from 0 (lowest) to 3 (highest).

Table 1: High Level Risks

Effective Risk	High Level Items: Risk Description
2.7	Policies for software installation on laptops are not in place.
2.7	Inadequate employee termination policy
2.4	No formal procedure in place for lost or stolen laptops
2.4	No policy or guidelines on wireless security and usage
2.4	No security measures in place for data contained in laptops.
2.1	Document shredding is not specified for a majority of documents at WWT

The next category of vulnerabilities consists of mainly medium impact items with medium to high risk probabilities.

Table 2: Medium-High Level Risks.

Effective Risk	Medium-High Level Items: Risk Description
1.6	No asset management system in place
1.6	No documentation for how software change management will work
1.5	Lack of emergency change management policies and procedures
1.5	Inadequate media handling policies enforcement at distribution centers could cause loss of confidential data
1.5	Password guidelines and enforcement for Perfect Orders have not been defined
1.4	Lack of laptop usage guidelines in the security policy
1.4	Lack of access control on unattended devices could lead to potential loss or damaged of equipment (primary laptops)
1.4	Data security requirements on contracts with outsourced or third-party companies
1.4	Introduction of laptops increases workload of monitoring which is not addressed

1.4	Security testing is not incorporated as part of the PO System
1.2	Too much of a dependency placed on email vendor regarding PO system for email

WWT should also be concerned about the next vulnerability level consisting of mostly medium impact, low probability items. These vulnerabilities should be addressed, but are not the main focus of the recommendations.

Table 3: Low-Medium Level Risks.

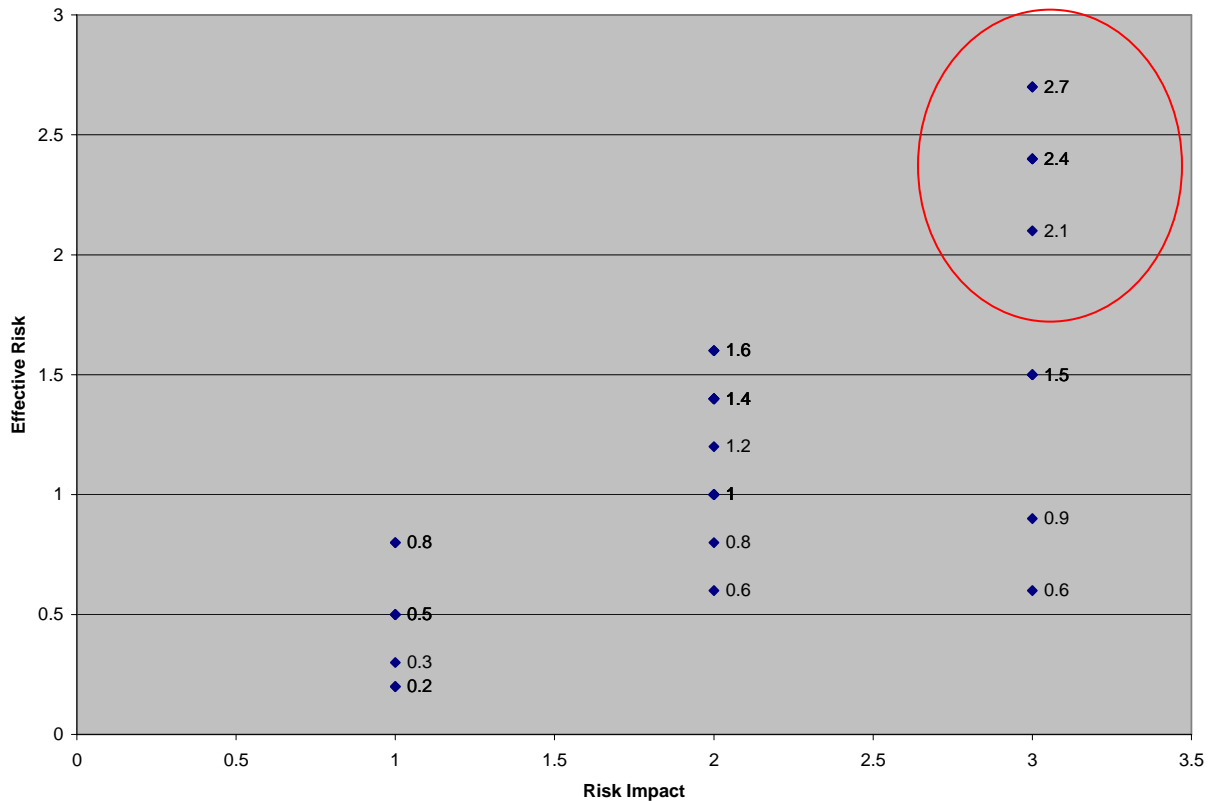| Effective Risk	Low-Medium Level Items: Risk Description
1	Lack of formal information classification training and security awareness training
1	No defined and enforced security responsibility
1	Security configuration management on laptops has not been adequately addressed
1	Email- usage has not been planned properly. It's more critical to business process without accompanying policies and procedures.
1	No formal and defined change management responsibilities
1	No defined workflow procedures when critical issues on laptops occur and stop working completely
0.9	No hard drive disposal policies in place might lead to leaks of confidential data
0.8	Expected increase in workload of technical support because of Perfect Orders is less than current staff capacity
0.8	Media labeling is defective; could lead to misplacement, disclosure, or loss of data
0.8	Lack of privileged access logs reviewing – auditing system
0.6	Lack of Business Continuity Plan should Perfect Orders fail
0.6	Lack of defined user responsibilities in the PO system

The next section includes low impact, low probability items

Table 4: Low Level Risks.

Effective Risk	Low Level Items: Risk Description
0.5	No policy on how salesman should handle PO system downtime when out in the field

0.5	No storing policies and responsibility for what can be placed on computers.
0.3	Lack of an SLA from the e-mail service provider could jeopardize reliability and availability of system
0.2	Possibility of data storage vendor mixing data with other client's information.
0.2	No procedure for facility lock out could prevent emergency access

Figure 1: Effective Risk Chart

Introduction

WWT is a well known international tool company with markets through the world. With a distribution network of seven locations worldwide and sixteen manufacturing facilities throughout the United States, Europe, Asia, South America, and Australia, WWT is in need of upgrading their ordering system to better server their customer.

While World Wide Tools is primarily focused on AS/400 systems as their primary means for delivering the new ordering system, several other key systems need to be reviewed and addresses. WWT also utilized several Windows NT domains, a Windows Exchange e-mail server, along with the introduction of company laptops for their sales force with this new ordering system, Prefect Orders.

With Perfect Orders, WWT has reviewed their previous three hundred successful installations and is confident this system will meet their needs. They are looking to Sneaker Systems to help them address security concerns for this new ordering system.

Throughout this assessment, Sneaker Systems has meet with key WWT personnel to help in understanding the existing security presence. In addition, Sneaker Systems has conducted an exhaustive review of WWT's security policy at the headquarters level, met with key management at a sampling of local distribution and manufacturing facilities, along with a discussion about third-party vendors that WWT uses for portions of their business operations. Further discussion of the specifics will be addressed in the next section of this document.

Systems, Policies & Procedures Being Evaluated

As mentioned previously, WWT has provided Sneaker Systems with their entire security policy, an opportunity to speak with key personnel for this assessment, along with discussion of any procedures already in place.

After the first few meetings with WWT and reviewing the structure of WWT, we came to the conclusion that the ISO-17799 would do the best job in representing the security best practices for WWT. Since this is an international security standard, it is well accepted in the business community through the world and this will help WWT in understanding and meeting key security objectives for their company. Details on the ISO-17799 can be found by reviewing our previous document on the recommended standard –

Sneaker_Sys_Recommended_Standard_for_WWT.doc. This provides a brief history on the ISO-17799 and why it is recommended for WWT.

In addition to making the ISO recommendation for a standard, we also reviewed in detail the WWT security policies and procedures document. In the next section we will provide our findings / recommendations we are making from the security policy, on-site observation, interviews, and general working meetings with key WWT personnel. When providing our recommendations, we will first provide a listing of the recommendations. After each recommendation, we will list the subsection within the ISO-17799 as to why we made this recommendation. Just as a reminder, here are the ten key areas discussed under the ISO-17799:

- Security Policy – Requires a written security policy and continual review and evaluation of the policy.

- Organizational Security – Handles information security infrastructures, security given for third-party access and outsourcing.

- <u>Asset Classification and Control</u> – Deals with proper classification of assets.

- <u>Personnel Security</u> – This area covers personnel training, security as part of an employee's job, and how personnel should respond to a security incident.

- <u>Physical & Environmental Security</u> – Securing various areas and equipment within an organization, along with general security controls.

- <u>Communications and Operations Management</u> – Operational procedures, system planning, handling malicious activities, backup process, network management, and communication with external organizations.

- <u>Access Control</u> – Covers which business areas need access to what, user responsibilities for access control, application access, network access controls, mobile access, and monitoring access.

- <u>System Development and Maintenance</u> – Security in applications, development, file systems, and encryption processes.

- <u>Business Continuity Management</u> – Deals with the ways a business can avoid disruption in general business, critical business processes, and understanding the ways to recover from potential disasters.

- <u>Compliance</u> - Deals with placing the technical requirements with the legal, regulatory and business context.

Vulnerabilities Report

By Effective Risk

Vulnerability #1

Policies for software installation on laptops are not in place.

> **ISO-17799 Section:** Communications and Operations Management
>
> **Impact:** High
>
> **Probability:** 0.9
>
> **Effective Risk:** 2.7
>
> **Description:**
>
> Perfect Orders program might not work properly if other programs are installed in the laptop. Since mobile users have administrator privileges, they can install and uninstall software with no restrictions. If any application installed by the user causes a conflict with Perfect Orders and makes it un-operable, the availability of that service is compromised and the disruption of the operations could be one consequence.
>
> **Fix:**
>
> Polices regarding installations of any software on laptops need to be created. Mobile users must know that even though they are capable of installing their own software, every installation has to be addressed and/or coordinated with IT department.
>
> Education users will be the primary mean to get this goal. Enforcement of these policies is critical for the company. Constant control on mobile equipments should be planned.
>
> **Additional information:**
>
> For more information on software installation procedures, please refer to the following links:
>
> An approach for secure software installation
> http://scholar.google.com/scholar?hl=en&lr=&client=firefox-a&q=software+installation+policies&btnG=Search
>
> Delegation of tasks and rights

http://www.loria.fr/~festor/DSOM2001/proceedings/S9-4.pdf

Vulnerability #2

Inadequate employee termination policy

ISO-17799 Section: Security Policy

Impact: Medium

Probability: 0.9

Effective Risk: 2.7

Description:

Company does not have a formal policy on how to handle employee termination.

Fix:

WWT should improve and formalize the employee termination policy, since little was found for this in the security policy. There is a need to formalize a policy specifying who is responsible for what when an employee is terminated. The issue of the Employee terminations process must be documented between the Human Resources and the Information Technology departments.

Additional information:
For more information on this subject, review
http://www.wetfeet.com/employer/articles/article.asp?aid=389&atype=retain

Vulnerability #3

No formal procedure in place for lost or stolen laptops.

ISO-17799 Section: Business Continuity Management

Impact: High

Probability: 0.8

Effective Risk: 2.4

Description:

How long should it take to replace laptops that are out of service or simply stolen? In such cases, the salesmen can not do their job effectively without their laptop. One, salesman less means declining sales for WWT and also less income (commission) for salesman.

Fix:
In order to keep a constant work flow, WWT should develop a business continuity plan. There should be backup laptops available which should be preconfigured and ready to go. Remote support should also be available in case of a system failure.
If laptop can not be repaired remotely, a working laptop should be delivered to the salesman.

Vulnerability #4

No policy on wireless security and wireless usage guidelines

ISO-17799 Section: Security Policy

Impact: High

Probability: 0.8

Effective Risk: 2.7

Description:
Company does not have a formal policy on ensuring employees uses protected wireless access to exchange company information.

Fix:
WWT should update their security policy for use of wireless access and ensuring proper security infrastructure is turned on and is in place.

Additional information:
For more information on this subject, review the following links:

Wireless Security - NIST
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

Ken Bent—White paper, A long, quick guide to the auditor, 2005

http://64.233.187.104/search?q=cache:w1RLzoSWNUkJ:www.governmentsecurity.org/forum/index.php%3Fact%3DAttach%26type%3Dpost%26id%3D3375+gkismet+dump+file&hl=en

Vulnerability #5

No security measures in place for data contained in the laptops.

ISO-17799 Section: Physical and Environmental Security

Impact: High

Probability: 0.8

Effective Risk: 2.4

Description:

Mobile equipments such as laptops might be left unattended at times. Currently, WWT has no way to protect data if someone can bypass other access controls.

Fix:

There are different security measures regarding this aspect. One of the most widely used is laptops locking cables. The use of these cables should be mandatory for all mobile users. In addition, certain security policies and procedures regarding this topic should be part of the entire security policy worldwide. We also recommend WWT use disk level encryption on the laptops and desktops. If any USB sticks are used, encrypt them too. Also, significant testing should be completed using a separate image of each machine type before rolling-out the whole disk encryption and the USB encryption.

Additional information:

For more information on protecting laptops, please refer to the following links:

Laptop security: A guide to protect your laptop
http://www.giac.org/certified_professionals/practicals/gsec/2641.php

Security in mobile devices
http://www.sec-consult.com/fileadmin/Newsletters/newsletter092004.pdf

Vulnerability #6

Document shredding is not specified for a majority of documents at WWT

ISO-17799 Section: Organizational Security

Impact: High

Probability: 0.7

Effective Risk: 2.1

Description:

Currently, WWT does not specify anything regarding document shredding outside of system dumps.

Fix:
More specifics should be given regarding document shredding. Policy should be updated to include what information should be shredded (e.g. anything classified as sensitive), when it should be shredded and any other process of when it will be removed from a given facility.

Additional information:
For additional information, please refer to the following link:

http://www.naidonline.org/news/pdf/05-19-2003_1.pdf

Vulnerability #7

No separation of duties regarding local system administrators

   ISO-17799 Section: Organizational Security

   Impact: Medium

   Probability: 0.8

   Effective Risk: 1.6

   Description:

   Company does not have a formal policy on how system administrators should have divided responsibility on the systems they manage.

   Fix:

   In the security policy, mention is made on having an overall local administrator responsible for physical security. This should be changed to have more separation of duties.

   Additional information:

For more information, visit
http://it.ojp.gov/documents/asp/disciplines/section1-4.htm

Vulnerability #8

No asset management system in place

ISO-17799 Section: Asset Classification and Control

Impact: Medium

Probability: 0.8

Effective Risk: 1.6

Description:

WWT does not have a formal asset management plan for IT inventory. Control of IT
assets is critical for the company since it will allow having a complete inventory of the
equipment and avoiding information disclosure contained in certain equipments.

Fix:

A formal asset management plan should be established at WWT. Since mobile
equipments will be incorporated into the IT inventory, the control of these items becomes
even harder and the lack of control of them could cause a leak of confidential
information. Asset management software will greatly assist IT staff with this task.

Additional information:

For more information on asset management solutions, importance and cases please refer
to the following links:

The use of **asset management** companies in the resolution of banking crises: cross-
country experience
http://scholar.google.com/scholar?hs=Ycq&hl=en&lr=&client=firefox-
a&rls=org.mozilla:en-
US:official_s&q=asset%20management&btnG=Search&sa=N&tab=ws

Why industry needs asset management tools
http://irc.nrc-cnrc.gc.ca/fulltext/nrcc44702/nrcc44702.pdf

Vulnerability #9

No documentation for how software change management will work

> **ISO-17799 Section:** Communications and Operations Management
>
> **Impact:** Medium
>
> **Probability:** 0.8
>
> **Effective Risk:** 1.6
>
> **Description:**
>
> Change management processes for the new ordering system, Perfect Orders, may cause security vulnerabilities in mobile workstations and hence the whole system in AS/400. Allowing Perfect Orders Company to perform software changes in the application opens a security control flaw in WWT entire infrastructure. Those software changes are not being coordinated fully by the Change management Team at WWT.
>
> **Fix:**
>
> If the proprietary Company takes care of change management processes on Perfect Order system, then World Wide Tools must watch these changes and coordinate the job with the application company very closely. It is recommended that WWT change management team address any change on this system carefully since this application will be the heart of the business operations for WWT. It would be better if WWT change management team has the total control and decision regarding any change on this system. No changes on this software should be permitted without the approval of the change management team at WWT.
>
> **Additional information:**
>
> For more information on software change management, please refer to the following links:
>
> Quality Software Management: Vol. 4: Anticipating Change
> http://www.dorsethouse.com/books/qsm4.html

Vulnerability #10

Lack of emergency change management policies and procedures

ISO-17799 Section: Communications and Operations Management

Impact: High

Probability: 0.5

Effective Risk: 1.5

Description:

WWT does not have a formal emergency change procedure for any of their systems. In an emergency, IT staff performs the require changes on the system and then document what they did. Even though the problem was resolved in good timing, the probability of opening some vulnerabilities and leave the system unstable is high.

Fix:

A formal procedure must be documented and published so that it is available for IT staff, 24x7 and using different access ways (Web, Documentation Database, Print outs, etc). Documenting this procedure and enforcing it so that it is followed by all employees in any emergencies is an important step for establishing a secure environment at the company.

Special care should be paid to Perfect Orders systems since emergency changes in the server could affect mobile users on laptops, PDA, etc. The same way, if any module of this program is modified, make sure to replicate the change to all mobile users.

Eventually, this procedure should be part of Business continuity plan and recovery plan.

Additional information:

For more information on emergency change management, please refer to the following links:

Emergency Change Management
http://itmanagement.earthweb.com/service/article.php/3529051

IT Change management policy example
http://72.14.203.104/search?q=cache:iHrMNI4WSqYJ:www.auditnet.org/docs/ChangeManagement.pdf+change%2Bmanagement%2Bemergencies&hl=en&client=firefox-a

Emergency Problem Solving
http://www.chacocanyon.com/pointlookout/050112.shtml

An Improvisational Model of Change Management,
http://www.ida.liu.se/~TDEI36/documents/CCSWP191.html

Vulnerability #11

Inadequate media handling policies enforcement at distribution centers could cause loss of confidential data

ISO-17799 Section: Communications and Operations Management

Impact: High

Probability: 0.5

Effective Risk: 1.5

Description:

Media handling at distribution centers is managed locally and low control from headquarters is in place.

Fix:

Enforcement of media handling policies at the remote places needs to be stronger and constantly monitored by local management as well as headquarters. WWT headquarters should implement a policy control plan which allows them to effectively check if media handling processes are being performed properly.

Additional information:

For more information on Median handling policies and creation of policies, please refer to the following links:

A checklist of responsible Information-Handling Practices
http://www.privacyrights.org/fs/fs12-ih2.htm

Electronic and paper-based media handling
http://www.ffiec.gov/ffiecinfobase/booklets/information_security/04g_electronic_paper_media_handling.htm

Vulnerability #12

Password guidelines and enforcement for Perfect Orders have not been defined

ISO-17799 Section: Access Control

Impact: High

Probability: 0.5

Effective Risk: 1.5

Description:

Password guidelines and enforcement for Perfect Orders are not defined; therefore, the probability of having weak password is high.

Fix:

Taking into account that the system will be accessed from mobile equipments, the need of emphasizing the security measures on access control is a must. Even though basic security measures on password control are handled by AS/400, WWT should consider in implementing a strong password system control for this specific application. Since Perfect Orders will be loaded in and accessed from mobile equipments, the need of strong passwords is crucial. In addition, it would be recommended that WWT implement a double layer password system.

Educate personnel who will access the system is also a valid recommendation. Showing the real risks that the company faces when passwords are disclosed could be one approach. Security policies regarding this topic also need to be reinforced. We recommend that network login passwords should be changed every week for the salesmen in order gain access into the network for inventory updates, etc.

Additional information:

For more information on strong password enforcement, please refer to the following links:

Password Enable PKI
http://www.cs.dartmouth.edu/~pki02/Sandhu/paper.pdf

Password Management Software Evolution
http://kamatoz.com/passwords-management-software.htm

User Key Management
http://www2.imm.dtu.dk/courses/02232/Cache/sfs.pdf

COSuser – Identity management and user provisioning for Unix, Linux and Microsoft Windows®
http://www.cosuser.com/

Vulnerability #13

Lack of laptop usage guidelines in the security policy

ISO-17799 Section: Security Policy

Impact: Medium

Probability: 0.7

Effective Risk: 1.4

Description:

Mobility of these laptops are creating a whole new set of security requirements

Fix:

Updating the current security policy, with new access control rules, and user responsibility for the mobile users is one recommended solution for this threat.

Additional Information

For more information, please visit the following links:
http://www.uab.edu/fsenate/computer.htm

Vulnerability #14

Lack of access control on unattended devices could lead to potential loss or damaged of equipment (primary laptops)

ISO-17799 Section: Access Control

Severity: Medium

Probability: 0.7

Effective Risk: 1.4

Description:

Mobile equipments such as laptops are can be left unattended. The company does not have a formal procedure to go beyond user id/password to protect access to company data on laptops and desktops.

Fix:

There are different security measures regarding this aspect. One of the most widely used is the screen saver with password. Other option is the implementation of PKI cards. This system requires new hardware installation on the laptops (PCMCIA) which allow users to insert their company ID card to log on to the station. When they leave users just take out the ID card and the laptop automatically locks the workstation. Password timeouts can also be used. We also recommend that all laptops should use system timeouts, automatic controls which close an active connection after a certain amount of time without inactivity since login. Regarding the physical security of the laptop, the use of lock cables should be mandatory for all employees.

Additional information:

For more information on security on unattended devices, please refer to the following links:

PKI cards deployment – Schlumberger Case Study
http://www.smart.gov/information/schlumberger_case_stdy_full.pdf

Security in mobile devices
http://www.sec-consult.com/fileadmin/Newsletters/newsletter092004.pdf

Who has the key to the vault? Protecting secrets on laptops
http://www.securesystems.com.au/pages/04_news/whitepaper_pdf/helen_armstrong_paper.pdf

Vulnerability #15

Data security requirements on contracts with outsourced or third-party companies

ISO-17799 Section: Organizational Security

Impact: Medium

Probability: 0.7

Effective Risk: 1.4

Description:

WWT does not have policies pertaining to data protection on systems that are outsourced or developed by third-parties. For instance, if mobile users will be using the email and exchanging information with Perfect Orders, they might send confidential information through this system and create new data security vulnerabilities.

Fix:

WWT needs to ensure that organizational data is being secured while it is processed, in transit or stored on their third-party systems. In order to this, WWT needs to write their contracts forcing the third parties to use security measures on their systems such as encryption, double layer access controls, etc.

Additional information:

For more information on security data facts (email system at WWT), please refer to the following links:

Securing data in transit
http://www.windowsecurity.com/articles/Securing_Data_in_Transit_with_IPSec.html

Protect your data in transit
http://www.dartmouth.edu/comp/support/library/safecomputing/defenses/network/transit/

Vulnerability #16

Introduction of laptops increases workload of systems monitoring which is not addressed

ISO-17799 Section: Physical and Environmental Security

Impact: Medium

Probability: 0.7

Effective Risk: 1.4

Description:

Because of the mobility of these laptops, they are more vulnerable to theft hackers, theft, damage, etc.

Fix:

We suggest that there should be at least one network administrator in charge for the laptop division. Network Activity Monitoring should be watched constantly because password changes are going to be performed more frequently, connectivity problems are going to occur more frequent than desktops, and access control must be monitored. Laptops can be controlled and maintained by creating different groups in a domain - laptop users and PC users - and group policies. Active Directory can be to manage all Microsoft based tasks. The company can also push application or other patches out to the clients using applications such as Altiris or Landesk. To handle the initial setup of the Perfect Orders software, it should be included in a basic image that can be copied onto other machines.

Additional Information

Network and Network Monitoring Software
http://www.alw.nih.gov/Security/prog-network.html

Altiris
http://www.altiris.com/products/clientmgmt/index.asp#doc

Landesk Management Suite
http://www.landesk.com/Products/LDMS/index.aspx

Vulnerability #17

Security testing is not incorporated as part of the Perfect Order system.

ISO-17799 Section: System Development and Maintenance

Impact: Medium

Probability: 0.7

Effective Risk: 1.4

Description:

Company does not have a formal procedure to test new PO system against threats.

Fix:

WWT should ensure they have formal procedure to test all changes to the new PO system, along with incorporating PO system changes into formal change management process. We recommend penetration testing as part of the process, and if PO needs to be customized, penetration testing should be done after customization as well.

Additional information:
For more information please visit the following links:

Problems with leaving open security holes (possible when not testing an installation).
http://www.benedelman.org/news/111804-1.html

Vulnerability #18

Too much of a dependency placed on email vendor regarding PO system for email portion.

ISO-17799 Section: Organizational Security

Impact: Medium

Probability: 0.6

Effective Risk: 1.2

Description:

Currently, there is a limited involvement with WWT's email vendor.

Fix:
We recommend that especially since the new ordering system will rely heavily on email, that you make regular visits to your email vendor's data center and other facilities.

Additional information:
For more information, visit http://www.cunaopsscouncil.org/news/323.html

Additional information:
For more information, please visit http://www.llrx.com/features/disasterIT.htm

Vulnerability #19
Vendor / Contractor access is not well defined within the security policy

ISO-17799 Section: Organizational Security

Impact: Medium

Probability: 0.5

Effective Risk: 1

Description:

Currently, WWT is rather vague on what contractors / vendors can do while in a WWT facility, along with monitoring them.

Fix:

A more detailed process needs to be given / defined for contractor / vendor access to facilities and how to monitor them once they are on-site; make this change in the security policy.

Additional information:

For more information, please visit
http://www.llrx.com/features/disasterIT.htm

Vulnerability #20

Lack of formal information classification training and security awareness training

ISO-17799 Section: Personnel Security Management

Severity: Medium

Probability: 0.5

Effective Risk: 1.0

Description:

Implementation is handled at each location by the facility manager (their primary responsibility is the business of making tools, not conducting information assurance classes for their employees). There is a need to formalize standards and responsibility for this kind of activity.

Fix:

Teach employees about your security requirements. Teach employees about their legal responsibilities. Teach employees about your business controls. Take this function out of the hands of the facility managers and put it under the control & responsibility of either the IS Officer or IS Administrator. Our recommendation is that is be put under the responsibility of the IS Administrator with the IS Officer implementing the policy. Develop a process to discipline people who violate your security procedures.

Vulnerability #21

No defined and enforced security responsibility

> **ISO-17799 Section:** Physical and Environmental Security
>
> **Impact:** Medium
>
> **Probability:** 0.5
>
> **Effective Risk:** 1
>
> **Description:**
>
> Currently, WWT has limited mention of a local facility manager's security responsibility.
>
> **Fix:**
>
> We suggest that under the section of the security policy entitled "General Computing Policies", WWT needs to add more details discussing how each local facility manager needs to handle physical security for that area.
>
> **Additional information:**
>
> For more information, please visit the following link:
> http://www.windowsecurity.com/articles/Defining_a_Security_Policy.html

Vulnerability #22

Security configuration management on laptops have not been defined

> **ISO-17799 Section:** Communications and Operations Management
>
> **Impact:** Low
>
> **Probability:** 0.5

Effective Risk: 1

Description:
Salesmen will be accessing the Perfect Orders System from remote locations, sometimes from hotel rooms. Depending on the location they are connecting from, firewalls might block out certain ports, thus blocking the connection to Perfect Orders.

Fix:
We suggest configuration management for laptops – firewalls should be configured to allow incoming and outgoing traffic for Perfect Orders.

Additional information:
SecureWorks: Firewall Management Service
http://www.secureworks.com/servicesProducts/managedFW.html

Vulnerability #23

Email- usage has not been planned properly. It's more critical to business process without accompanying policies and procedures.

ISO-17799 Section: Communications and Operations Management

Severity: Medium

Probability: 0.5

Effective Risk: 1.0

Description:

We must recommend to WWT that they formalize their usage of email. We must spend time addressing the outsourcing email issue. Currently, WWT's email is not encrypted. ERP access requests sometimes goes through email. Customer information sometimes goes through email. In the interview, WWT did not know exactly what they were using email for. The following sections of the ISO 17799 should assist the client in creating a viable email usage policy.

Fix:

Make sure that external contractors protect your information. Make sure that contracts define controls that contractors must use. Make sure that contracts specify business continuity requirements. Acceptable use policy for email – may enhance current policy. Establish controls to make email less vulnerable to tampering. Establish controls to make email less vulnerable to unauthorized access. Establish controls to increase the reliability of your email service. Ensure that policy explains how email attacks should be handled.

Ensure that policy explains how email viruses should be handled. Ensure that policy explains how email attachments should be handled. Ensure that policy explains when cryptographic techniques must be used. Ensure that policy explains when email should not be used. Specifies what is and is not acceptable use in regards to email. Establish procedures to control voice communications. Establish procedures to control mobile phone communications. Establish procedures to control answering machine messages. Establish procedures to control dial-in voice-mail systems. Establish procedures to control video communications. Establish procedures to control fax communications. Technical means related to email – the very definition of email is changing so by including these items in the client's email policy, they will be ahead of the curve.

Vulnerability #24

No formal and defined change management responsibilities

ISO-17799 Section: Communications and Operations Management

Impact: Medium

Probability: 0.5

Effective Risk: 1

Description:

Change management is handled mainly by IT stuff and no specific person is formally assigned as the responsible of the whole process. IT security manager controls the change processes however, other areas that might be affected by the system change may not be involved in certain occasions.

Fix:

It is recommended that companies have a change management team in place. This team will be the entity responsible of any change, either emergency or normal, on any system pertaining to the company. There must be a designated person or group who can initiate the change process; at the same time, the list of people and roles authorized to initiate the change must be established. This team must take care of documenting procedures and enforce them.

Additional information:

For more information on change management team creation, please refer to the following links:

Integrated Disaster Management

http://pecolab.colorado.edu/augnet/papers/MeissnerDesChal.pdf

An Improvisational Model of Change Management
http://www.ida.liu.se/~TDEI36/documents/CCSWP191.html

Change Management: A guide to effective implementation (book)
http://print.google.com/print?id=vJZ9GUlCdCkC&oi=fnd&pg=PA2&sig=_q1sfzsrV2iG
vGgX6yKZAe7k99I

Vulnerability #25

No defined workflow procedures when critical issues on laptops occur and stop working
completely

ISO-17799 Section: Business Continuity Management

Impact: Medium

Probability: 0.5

Effective Risk: 1

Description:

No formal policy to handle replacement or restore of damaged laptops.

Fix:
WWT should develop a business continuity plan for when laptops become
decommissioned, thus ensuring salesman and others using laptops can continue to do
their job.

Additional information:

For more information, visit
http://networkingsmallbusiness.com/net.worker/columnists/2005/0606gittlen.html.

Vulnerability #26

No hard drive disposal policies in place might lead to leaks of confidential data.

ISO-17799 Section: Communications and Operations Management

Impact: High

Probability: 0.3

Effective Risk: 0.9

Description:

Media disposal is not performed and monitored properly. There is a need to address the issue with just formatting drive for "bad drives". This does not remove the data.   Hard drives in workstations sent to disposal are only formatted once. Information in hard drives can be recovered easily after the hard drive has been formatted once or more.

Fix:

WWT has to implement a disposal procedure for hard drives. There are free applications that could be used to wipe the disk. According to sanitizing procedures, it is recommended to re-write the whole disk with 0 or 1. This is performed by wiping tools. Other standards recommend formatting the hard drive more than 5 times (7 – German Sanitizing standard).

Additional information:

For more information on hard drives disposal vulnerabilities, solutions for either paper-based media or electronic media, please refer to the following links:

Hard drive disposal: The overlooked Confidentiality Exposure
http://www-03.ibm.com/financing/pdf/us/recovery/igf4-a032.pdf

Hard drive secure information removal and destruction guidelines
http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/g2-003_e.pdf

Electronic and paper-based media handling
http://www.ffiec.gov/ffiecinfobase/booklets/information_security/04g_electronic_paper_media_handling.htm

Cleaning bad drives
http://www.ugr.com/nl0504.html

Vulnerability #27

Expected increase in workload of technical support because of Perfect Orders is less than current staff capacity

ISO-17799 Section: Communications and Operations Management

Impact: Low

Probability: 0.7

Effective Risk: 1.4

Description:

Since the implementation of Perfect Orders will require more training and support until employees become accustomed to it. The lack of this support could cause a threat to the availability of the service.

Fix:

We suggest increasing the size of the technical support team to make sure salesmen are able to use the system as efficiently as possible.

Additional information:
-   NOTHING FOUND –

Vulnerability #28

Media labeling is defective; could lead to misplacement, disclosure, or loss of data

ISO-17799 Section: Communications and Operations Management

Impact: Medium

Probability: 0.4

Effective Risk: 0.8

Description:

Media labeling is not being performed properly at WWT. Neither format nor template is applied to the labels of the media. This lack of labeling could affect the three security aspects of data: Confidentiality, availability and integrity. If no label is on the media, this media could be reused and therefore the information in it could be lost. At the same time, the restoring process would be poor if no proper label is on media; this could cause a delay in recovering data and hence affecting the availability of data. Finally, if no format is used, misunderstandings at the moment of appending data on those media could cause a loss of integrity of data.

Fix:

WWT needs to establish a media labeling plan that manages media format or template, media naming, media tracking and documentation regarding these aspects.

Additional information:

Please refer to this example of media handling:

Example of media labeling
http://www.mpi.nl/corpus/a4guides/tapelabeling.pdf

Vulnerability #29

Privileged access logs reviewing – auditing system

ISO-17799 Section: Access Control

Severity: Low

Probability: 0.8

Effective Risk: 0.8

Description:

Privilege access is not being monitor at WWT. Auditing these actions performed by system administrators are important for providing a secure environment at all levels.

Fix:

The control of the use of privileges account such as administrators, roots, etc must be established at WWT. The use of sensitive accounts needs to be logged and then audited by external people.

Additional information:

For more information on privileged access logging and auditing, please refer to the following links:

A management perspective on privileged access to computer systems
http://www.usenix.org/publications/login/1999-4/mgmt_persp.html

Log Analysis and FFIEC compliance
http://www.rescomp.com/ffiec.htm

Vulnerability #30

Lack of Business Continuity Plan should Perfect Orders fail

ISO-17799 Section: Business Continuity Management

Severity: High

Probability: 0.2

Effective Risk: 0.6

Description:
Since Perfect Orders is mission critical, WWT should have a backup plan in the event that Perfect Orders is deemed unsuitable for use.

Fix:
A formal Business Continuity Plan should be created that includes the following:
1. Review and assessment of existing contingency arrangements
2. Map of data, process, and system dependencies for each resource
3. Recommendations on improvements on the existing plan
4. An appropriate framework for continuity and recovery

Additional Information:
Developing a business-continuity plan
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci883578,00.html

Vulnerability #31

Lack of definition of user responsibilities in the PO system

ISO-17799 Section: Security Policy

Severity: Medium

Probability: 0.3

Effective Risk: 0.6

Description:

User roles and responsibilities for the PO system need to be clearly defined so that the application owner can easily determine the level of access to grant and which levels to remove.

Fix:

Updating the current security policy, with new access control rules, and user responsibility for the Perfect Orders Users. To keep client and sales data confidential, the technical support role should have full functionality, but only "dummy" data. When altering the policy to include roles for PO, keep in mind that in the future, there might be a need for an external user to access

Vulnerability #32

Security policy is too narrow. Only American (U.S.) laws published in the policy

ISO-17799 Section: Security Policy

Severity: Low

Probability: 0.5

Effective Risk: 0.5

Description:

WWT's security policy is very specific in regards to laws in the United States. Still, little is said of laws in other locations where WWT has operations.

Fix:

We see that you make mention of several U.S. government regulations (US Dept of Homeland Security alerts, HIPAA, GLB, etc). You should remove this and add in information about reviewing procedures that cover laws specific to each locality where the facility is located, since WWT is an international company.

Additional information:

For more information, please refer to the following link:
http://www.eda.admin.ch/content/eda/e/home/foreign/secpe/intsec.html

Vulnerability #33

No policy on how salesman should handle PO system downtime when out in the field

ISO-17799 Section: Organizational Security

Severity: Low

Probability: 0.5

Effective Risk: 0.5

Description:
No formal policy discusses that salesman should revert to the paper system and how to store this information when the PO system is down or laptop is inoperable.

Fix:

If customers are going to get their order invoice via email (most of them – those who have access and not handled other ways), a procedure should define what the sales force should do when the email system is down (even for 15 minutes).

Additional information:

For more information, please refer to the following link:
http://www.ocio.usda.gov/directives/files/dm/DM3570-001.htm

Vulnerability #34

No storing policies and responsibility for what can be placed on computers.

ISO-17799 Section: Organizational Security

Severity: Low

Probability: 0.5

Effective Risk: 0.5

Description:

Currently, there is limited mention of what can be placed on computers. Mobile users could compromise the equipment but saving critical information on local drives. Also, responsibility if focused on local facility mangers.

Fix:

WWT should update policy to reflect exactly what can be stored on the local desktops and laptops for employees. Also, shift responsibility from local manger to individual employees.

Additional information:

For more information, please refer to the following link:
http://www.uab.edu/fsenate/computer.htm

Vulnerability #35

Lack of an SLA from the e-mail service provider could jeopardize reliability and availability of system

ISO-17799 Section: Communications and Operations Management

Severity: Low

Probability: 0.3

Effective Risk: 0.3

Description:

There are indications that the e-mail system might be used for more tasks after the implementation of Perfect Orders. Salesmen might be e-mailing order confirmations to clients, which serves as a backup to data entered into the main system.

Fix:

We suggest asking the European e-mail service manager to provide you with a detailed Service Level Agreement that tells you the level of guaranteed uptime and their policies regarding backups of data. If they do not already have an SLA written up, they should be willing to make one available for you. If you find that e-mail usage has become mission-critical, you might want to think about taking back control of the e-mail system.

Additional information:

Vulnerability #36

Possibility of data storage vendor mixing data with other client's information could cause a confidentiality and availability threat.

> **ISO-17799 Section:** Organizational Security
>
> **Impact:** Low
>
> **Probability:** 0.2
>
> **Effective Risk:** 0.2
>
> **Description:**
>
> Currently, no mention is made as to how WWT will handle any mix up in data between WWT information and other clients of the third-party vendor.
>
> **Fix:**
>
> Procedures should be developed to mention that if tapes are somehow mixed with other client data, what are the ramifications to the vendor. This should also be discussed in the vendor SLA and other contracts with the data storage (Iron Mountain) vendor.

Vulnerability #37

No procedure for facility lock out could prevent emergency access

> **ISO-17799 Section:** Communications and Operations Management
>
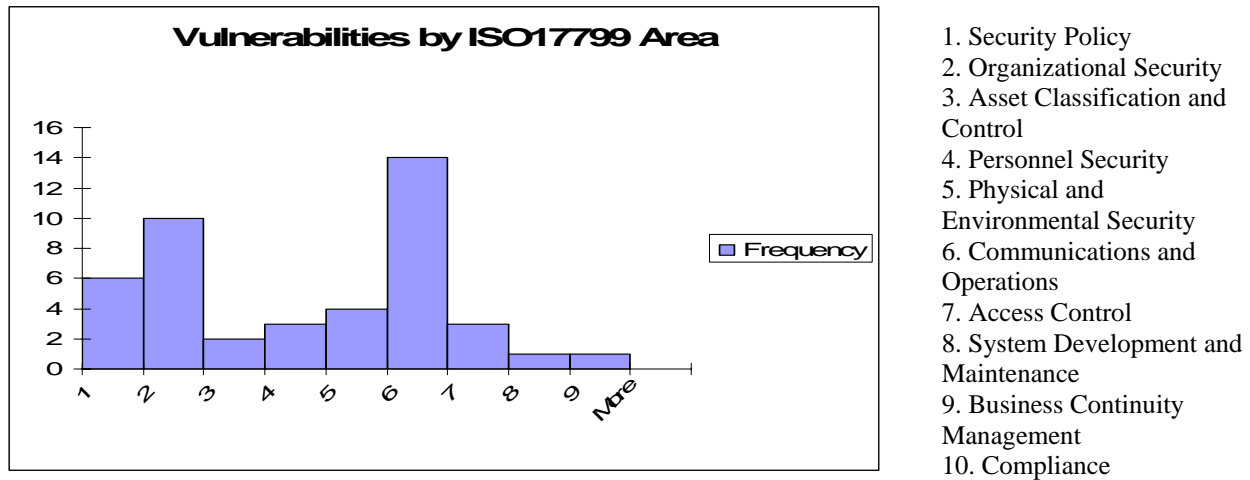> **Impact:** Low
>
> **Probability:** 0.2
>
> **Effective Risk:** 0.2
>
> **Description:**
>
> Company lacks procedure to inform employee on what to do when locked out of a facility for any length of time.
>
> **Fix:**
>
> A procedure should be developed discussing what to do under the scenario that a facility is locked out (who has keys, who to call, what to do if they need to break-in, etc.)

Figure 2: Chart of Vulnerabilities by ISO17799

Vulnerabilities by ISO17799 Area

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations
7. Access Control
8. System Development and Maintenance
9. Business Continuity Management
10. Compliance

Conclusion

Overall, WWT has taken the right steps in putting a security policy in place and working to spread the idea of security throughout the company. We hope that this assessment has provided you with adequate guidance for developing security strategies that are in line with your budget and goals for the Perfect Orders system. Providing the employees with initial security training and sign-off for their job is an important first step. Please take the recommendations given as an independent approach to reviewing security at WWT. Hopefully, this assessment has served to add value to security awareness within WWT and we look forward to the opportunity in assisting with the next stage – Evaluation. If you have further questions about the vulnerabilities and recommendations mentioned in this report, please contact Sneaker Systems via e-mail at Assessments@sneakersystems.com.

Sincerely,

Sneakers System, Inc.

Security Assessment – Customer Acknowledgement

This document will serve to acknowledge the receipt of the final security assessment report from Sneakers Systems, Inc. for World Wide Tools, Inc (WWT). Any further questions the customer may have regarding the final report can be directed to the e-mail address provided in the conclusion of the report. Thank you for allowing us to take part in this assessment for WWT.

I certify that I have reviewed the Information Security Assessment Report for WWT that was dated December 13, 2005. I further acknowledge that I accept the finding of this report. In your acknowledgement below, please print and then sign your name.

_____   _____
World Wide Tools, Inc. - Chief Information Security Officer   Date

_____   _____
World Wide Tools, Inc. – CEO   Date