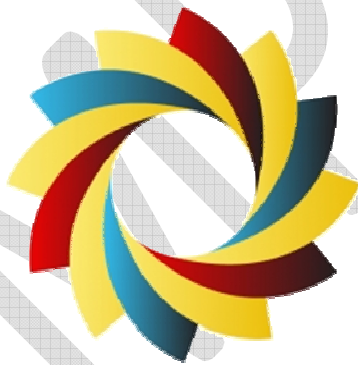


Network Vulnerability Report

4/6/09



DESIGN AGENCY
PROVIDING BEST SOLUTIONS



www.ddco.com



Jane Doe
Sample Design Company
4/6/09

ABOUT THIS REPORT:

Design Data Corporation provides the “Network Vulnerability Report” to help businesses better understand the current health of their I.T. environment. This report will pinpoint potential vulnerabilities that exist throughout your network as well as possible resolutions. Design Data highly recommends that before any work is done on your network that a more detailed analysis is performed.

Section 1 – System Snap Shot

A brief “Snap Shot” of the Key devices that are running throughout your business. This may include items such as Servers, Workstations, Routers, Backup Devices, Printers, and more. A DDC Technician will decide onsite which devices should be documented.

Section 2 – Network Vulnerabilities

A DDC Technician will provide a brief description of the various threats that were uncovered while onsite. This section is designed to help provide businesses with additional knowledge as to the overall threat of

Section 3 – Recommendation

Describes various “key” hardware devices located throughout the network. DDC will investigate the characteristics of the device to more accurately define the health of the network. The certified technician that performed the audit will provide a brief analysis of recommendations on way to improve the network stability.

Section 4 – Conclusion

A brief overview of what was uncovered during the Network Vulnerability Assessment. The technician that performed the audit will provide a brief summary of the findings to help provide better insight.

*For more information about Design Data Corporation please visit our website at www.DDCO.com. Or call us at (717) 295-9712.



Section 1 – System Snap Shot

The following information was gathered during our initial audit of your network infrastructure.

Server Info

Distributor:	Dell Power Edge SC-1420
Operating System:	Microsoft Windows Small Business Server
RAM:	1 GB
Disk Space:	C: 12 GB / 2 available D: 285 GB/ 248 available
Dell Warranty	Expires June 2010
Tape Drive Info:	DAT 72 Tape Drive
Nightly Backup Info:	37 GB backed up Nightly
Power Supply	APC Backup
Updates and Patches	SP2 – Out of Date
Anti-Virus	Symantec End Point v. 10

Workstation Info

Number of Workstations	6
Number of Laptops	2
Operating System:	Running a mix of Windows 200 and Windows XP
Anti-Virus	Each Workstation has their own anti-virus
Updates and Patches	Workstations get their own updates

Email Info

Email Hosted By	D&E Communications
Exchange Server	Is not being used
Using Outlook	All users are running Outlook Internally
Other Info	

Other Devices

Router Information	Cisco 587W
Wireless information	No Wireless
Printer Information	2 HP Network Printers
Software Application Info	No Special Software Applications being run at this time.



Section 2 – Network Vulnerabilities

The following information was gathered during our initial audit of your network infrastructure.

System Audit	Vulnerability Description:
Server Updates	<p>The 2003 Small Business Server is approximately 4 years behind in Microsoft System Updates. Microsoft updates are provided on a regular basis to help prevent a wide range of potential issues such as:</p> <ul style="list-style-type: none">• The latest security updates to protect against malware and other potentially unwanted software• Updates that improve reliability and performance• Upgrades to Windows features• Drivers from Microsoft partners
Data Backup Updates	<p>Symantec Backup Exec product is behind in software updates. Keeping your backup software up to date ensures the software is running at its full capacity. A lack of updates puts the software in jeopardy for a wide range of vulnerabilities.</p>
Data Backup Procedure	<p>After reviewing the backup configuration, DDC uncovered specific outlook.pst files as well as other business critical files are not being properly backed up. If files are not properly backed up on a regular basis, the risk of losing data increases significantly.</p>
Anti-Virus Protection	<p>The Symantec Anti-Virus on your server is currently no longer supported by the vendor. Your anti-virus software provider HIGHLY recommends keeping you anti-virus current to keep your network as secure as possible. Running older versions of anti-virus software greatly increases the opportunity for malicious activity.</p>
Disaster Recovery	<p>You currently have NO Disaster Recovery mechanism in place. In the event that a disaster would occur, you would experience a significant amount of downtime as the server gets rebuilt.</p>



Section 3 – Recommendation

The following information was gathered during our initial audit of your network infrastructure.

System Audit	DDC Recommendation
Server Updates	We highly recommend getting the Server up to date with Microsoft patches. Applying updates will greatly improve the efficiency of your server.
Data Backup Updates	Installing the Symantec Backup Exec updates will ensure that your software is current and running at its highest possible level.
Data Backup Procedure	A DDC technician will sit down with your staff to ensure the proper files are being backed up regularly. As your system grows, it is critical to review your backup plan on a regular basis.
Anti-Virus Protection	The latest version of Symantec anti-virus product, “Endpoint” is available from Symantec and would provide a greater level of security.
Disaster Recovery	DDC would create a disaster recovery plan which included a quarterly CD which is stored offsite. By creating a disaster recovery CD, you would greatly reduce the downtime experienced in the event a disaster would occur.



Section 4 – Conclusion

After reviewing your network, Design Data would highly recommend getting the proper updates and patches on your Microsoft Windows Server as a main priority. Doing this will improve the overall performance and health of your server. As noted above, Design Agency has NO disaster recovery plan in place to handle an emergency. DDC would suggest sitting down with one of our disaster recovery specialist to put together a plan which will ensure your data is safe and your downtime will be minimal in the event a disaster would occur.

Many of the other vulnerabilities outlined in the report deal with routine maintenance issues such as anti-virus updates to ensure your hardware investment is properly maintained.

If you have any questions regarding any information in this report please contact Design Data Corporation to learn more.

Thank you for your Time,

Design Data Technician

X _____

