How Secure is Secure Enough for Your Network?

Why Should your Business be Preventative with Your Network?

If your business has any network or cybersecurity concerns, this assessment will make sure that your security needs are met. Even if your organization does not have any compliance standards out of the ordinary, this is still highly recommended. What if you could decrease downtime and emergency maintenance costs? This assessment will be able to guide your organization to the best solutions for your network and to keep viruses, disgruntled employees, and hackers out of your network!

Having a security assessment done can find weak spots on your network. If there are any vulnerabilities within the network, they will be found so that the discussion for an effective solution can begin. Doing these assessments on an annual basis helps to decrease the chances of a data breach. For any company needing to meet compliance standards, such as handling private personal data, credit card data, or other sensitive data, this is a highly recommended proactive step to take.

$200

Software Scan

(this price does not include labor)

262.522.8560
sales@ontech.com

Ontech systems, inc.

Ontech Systems, Inc.
N85W16186 Appleton Ave., Suite A
Menomonee Falls, WI 53051

What is Found in a Security Assessment?

Network Security Management Plan: This report will help prioritize issues based on the issue's risk score. A listing of all security related risks is provided along with recommended actions.

External Vulnerabilities Scan Detail Report: A comprehensive output including security holes, warnings, and informational items that can help you make better network security decisions. This is an essential item for many standard security compliance reports.

Outbound Security Report: Highlights website access from internal computers for ease of comparison with your existing web access policies. It also lists available wireless networks as part of a wireless security survey.

Physical Security: Ontech will review the physical environment for your IT assets, and make recommendations for improvements that can increase the security of your network infrastructure.

Failed Login History by Computer Report: Same data as User Behavior but inverted to show you by computer. Quite useful, in particular, for looking at commonly accessed machines (file server, domain controller, etc.) – or a particularly sensitive machine for failed login attempts.

Login Failures by Computer Report: Report identifies users who have failed in logging into a computer. Great for auditing/logging purposes to know of all attempts.

This security analysis is not all encompassing. However, the results of this analysis may prompt additional recommendations that are more focused on specific aspects of your environment.
EX: PCI & HIPAA audits, in-depth anti-virus testing, firewall/router audit, etc.