# Security Vulnerability Audit

## Assessing Your Organization's Security

### A White Paper for Management

The most effective team to determine your own vulnerabilities and then put a plan into place to close the vulnerabilities is ... *your own team*. This white paper includes the basic version of the **Infrastructure and Network Security Report Card,** a system for grading your own security vulnerabilities. This simple self-assessment tool is designed to provide a basis for further security planning.

**By James P. Cavanagh**
Global Telecom and Security Consultant
jpc@consultant-registry.com

**January 2002**

www.consultant-registry.com

**The Consultant Registry**
***Global Telecommunications & Security Consulting and Training Since 1994***

www.
consultant-
registry
.com

## *About The Consultant Registry*

**The Consultant Registry** is a consortium of some of the top telecom and security consultants in the industry. Each have their own consulting practices, but come together on larger, or more complex, projects. In this way each of our members maintain their autonomy, but our clients still benefit from our strength in numbers.

Many of us have been involved in various aspects of infrastructure and network security for many years. Some of us have helped private industry, the military/law enforcement or both. This free security white paper is our way of sharing the essence of our expertise in the security, anti-hacking and counter-terrorism areas with as many businesses as we possibly can, as cost effectively as possible.

**The Consultant Registry** also provides training classes, workshops, publications and consulting in the areas of telecommunications, and infrastructure and network security. Please visit our website, **www.consultant-registry.com** - for more details on the products and services we offer and, for current information on security as well as a variety of other areas.

(c) Copyright 2002 by James P. Cavanagh, jcavanagh@consultant-registry.com
ALL RIGHTS RESERVED UNDER US AND INTERNATIONAL COPYRIGHT LAW
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the author and The Consultant Registry. Reproduction prohibitions do not apply to the forms contained in this product when reproduced for non-commercial use. Reproduction prohibitions also do not apply to the use of excerpts or quotes for use in reviews or attributed quotes in other works of any type as allowed for in copyright law.

For additional information about this or other products or services of The Consultant Registry, please contact us:

The Consultant Registry
4405 Northside Parkway
Suite 2120
Atlanta, Georgia 30327
+1.404.760.0667
info@consultant-registry.com

# Table of Contents





© 2002 James P. Cavanagh, Global Telecom & Security Consultant


jcavanagh@consultant-registry.com / www.consultant-registry.com

© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

# Overview

## Vulnerability Audit: Assessing Your Organization's Security

*Security is a basic human need that predates civilization as we know it.*

Security is among the oldest human needs. While security has evolved through the ages the basics remain the same. The better an individual or organization understands their vulnerabilities and how to protect against exploitation of those vulnerabilities, the better the chance of survival.

*Early humans closed the vulnerability of individuals hunting by hunting in pairs or groups.*

In the earliest days humans realized, for instance, that hunting by themselves exposed them not only to the animals they hoped to kill and eat, but also to other, competing, humans vying for the same items for their family dinner. Security was enhanced by reducing the vulnerability of hunting alone by hunting in pairs and groups. Other aspects of the operation were also enhanced, but this is beyond the scope of this document.

*In the American West "circling the wagons" left less of the wagon exposed to attack and created a more effective defense.*

Early settlers in the American West understood that fighting the original inhabitants of the region from a single line of wagon trains strung in a single line across the open prairie made them more vulnerable to attack and exposed the two long sides of each wagon to attack. They learned that "circling the wagons" was an effective way to close the vulnerability and increase their chances of survival.

*City walls and fortifications are examples of solutions to known vulnerabilities..*

Inhabitants of what is now Europe and Asia discovered many hundreds of years ago that living in exposed sites made left them vulnerable to ad hoc attacks from bands of roving ruffians or armies. They closed the vulnerability by building fortifications, forts, kremlins, moats, walls and other similar structures around their cities to discourage ad hoc attacks.

*Security is an integral part of the overall operation of an organization, just like payroll or purchasing.*

To summarize, a large part of the function of security over the years has been to identify potential vulnerabilities, and to counter them or make them less attractive to potential attackers. Security threats and vulnerabilities to business, as well as the business benefits of good security and implementation of effective organizational security policy and technology are covered in other white papers in this series[1]. This specific white paper addresses auditing your own organization and highlighting its vulnerabilities.

*The vulnerability assessment process must, itself, be kept secure.*

It is vital to keep the information which is gathered as a part of the vulnerability audit process secret and secure as this information could provide a blue print for an attack on your organization.

[1] The entire **Security White Paper Series** from **The Consultant Registry** may be requested free of charge at www.consultant-registry.com. The white papers are written by leading security experts and are made available free of charge by **The Consultant Registry** as a public service to encourage discussion and understanding of key security topics of current interest to a wide variety of organizations globally.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

*This white paper will help an organization with the vulnerability audit.*

The object of this white paper is to help organizations begin the vulnerability assessment process as quickly and cost effectively as possible. In order to begin the planning process, to develop budgets, to deploy resources, implement training and assure stock holders, employees and customers about your organization's security situation before vulnerabilities must be assessed and their probability of being exploited must be examined.

## Take the First Steps

*All of these free white papers, taken together, can provide the basic steps needed for a comprehensive security program..*

If you are reading all of the white papers in this series in order you began with *Threats & Vulnerabilities*, which brought to light the broad threats to an organization due to improper security. The next step was *Network Security: The Business Value Proposition,* which stated that there are business values of network security as well as manageable risks that must be considered. Fundamentally, it shed a business light on a previously technical subject. You are now at the third step: auditing your own organization for security vulnerabilities.

*Vulnerability assessment is the first step to creating a comprehensive and effective organizational security program*

The **Infrastructure and Network Security Report Card**[2] is a useful tool designed to help create a document which will serve the needs of your organization as you develop and/or refine your security program.

[2] The Infrastructure and Network Security Report Card included with this white paper is a basic assessment tool with 20+ questions relating to organizational security policy, infrastructure and network security vulnerability assessment. An advanced Report Card is available for an additional fee at www.consultant-registry.com.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

*The vulnerability audit can be performed in a variety of different ways. Choose the best one for your organization, or create a hybrid.*

The vulnerability audit process must adhere to some reasonable business guidelines in order to be effective. First of all, it must receive complete support from management and, ideally, uppermost management will be active in overseeing the project. The next issue is the budget. This point should include both time and money as budget resource considerations. Organizations who clearly understand their security risks and liabilities will already have staff in place, as well as funds budgeted for a routine vulnerability audit. In fact, these security aware organizations probably do not need to perform a security audit now because they already have a current audit for reference purposes. The other organizations have a choice of three primary options, or a customized hybrid created for your own specific needs.

The three primary options are:

- The Gold Strategy
- The Silver Strategy
- The Bronze Strategy

*There are three primary strategies for the vulnerability audit, depending upon the time and money budget.*

The Gold Strategy is the most expensive in terms of money and time but produces a premium result which will result to with which to implement an actionable security plan. The Silver Strategy is less expensive in terms of money and time and produces a reasonable result for the investment. The Bronze Strategy requires the least time and money and is a very good first step to determine if the additional resources should be spent. We will now review each strategy briefly.

## The Gold Strategy

*The Gold Strategy is the most expensive in terms of money and time, but produces a premium result with which to implement an actionable security plan.*

The Gold Strategy uses both internal and external resources to achieve the audit as well as specialists and generalists, as shown in Figure 1. The best way to understand the Gold Strategy concept is in terms of a mini-case study. For our case study we will look at the fictional company Medium Pharmacies. Medium Pharmacies is a regional company with 28 pharmacies in neighborhood locations serving their local communities. Recent general news articles about computer fraud and hacking as well as articles in the pharmaceutical industry trade press and recent Health Information Privacy Act (HIPA) requirements have raised the awareness of Medium's management's attention to security issues. Medium's management has directed that "no expense be spared" to assure that the privacy and integrity of their patient information is maintained at the highest levels allowed by current technology. In this (ideal) case study Medium CEO Pat Patrick will personally manage the project.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

*The Medium Pharmacy Company plans for their project.*

Medium Pharmacy's security vulnerability audit team is staffed per the guidelines in Figure 1. Pat Patrick takes the position of "Project Leader" and assigns four team leaders: two internal and two external teams are named. The team leader for the Internal/ Generalist Team is the Human Resources Manager, and the Director of Security and Facilities leads the Internal/ Specialist Team. The External/ Generalist Team Lead is an accountant from an outside accounting firm, and the Specialist/ External team is headed up by a security consultant hired through good third party references with familiarity and experience in the pharmacy business in general and HIPA guidelines.

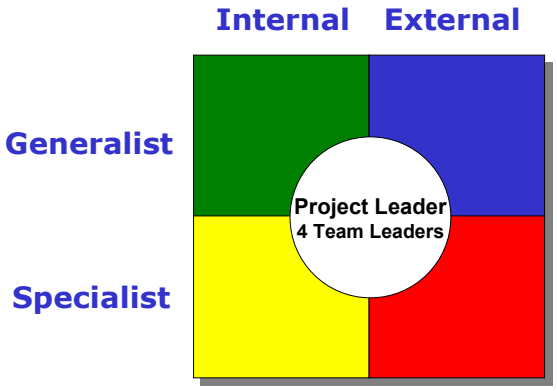


**Figure 1**
**Gold Strategy Project Member Table**

*Multiple parties complete the Report Card.*

Each team leader assembles their team and completes the **Infrastructure and Network Security Report Card** for their own areas of expertise.

### Internal Generalists

*Internal Generalists provide general knowledge from an internal perspective.*

Internal Generalists, for instance, are Medium employees from a variety of areas including accounting and human resources. They complete the report card as it regards security policy, cooperation with outside organizations and existing rules and regulations. Internal generalists have a general knowledge about Mediums present security operations.

### Internal Specialists

*Internal Specialists provide specific knowledge from an internal perspective*

Internal specialists are employees with highly specialized knowledge about Mediums operations and may only be called on to answer one or two of the questions on the Report Card. Examples of Internal Specialists in Medium's case are the shipping/receiving manager with specialized knowledge of drug shipping and controlled substances regulation, the internal LAN/WAN security specialist with knowledge of the network firewalls, the physical plant maintenance supervisor accountable for locks, alarms, surveillance cameras and the purchasing manager responsible for the relationship with the cleaning contractor.

***Continued on page 13.***


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

www.
consultant-
registry
.com

# The "Report Card"

## Report Card Overview

This white paper includes the basic version of The **Infrastructure and Network Security Report Card.** It is divided into three sections:

- Organizational Security Policy Audit
- Infrastructure and Physical Security Audit
- Network Security Audit

Each question in each of the three sections has a fixed point value. The points can be tallied and used to provide a general grade on overall security. A grading scale is provided at the end of the report card that should be sufficient to provide management with the general overall security of an organization. This simple grading system will allow the organization to prioritize the three areas covered by this "report card" and to determine the order in which these initiatives should be undertaken.

**DISCLAIMER:** There is no substitute for a proper security evaluation performed by a competent security consulting organization: the **Infrastructure and Network Security Report Card** is designed as a diagnostic tool to help an organization understand where to begin the process of developing their own customized network security program.

**SECURITY NOTICE:** After this document is filled in with organizational information it should be treated as:

**PROPRIETARY AND CONFIDENTIAL**

**Please note that the "Report Card" may easily be separated from the center of the printed white paper by loosening the staples and removing the center two pages. This will facilitate easy reproduction and use of the Report Card.**


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

## Organizational Security Policy Audit

**(1) Does the organization have a (current, written) Security Policy?**

The existence of a current, written infrastructure and network security policy is critical to an organization's security effectiveness. Security policy must be mandated from the top of the organization and have management's unwavering support in order to be effective. If the organization has an existing policy document then the existing policy document can be used as the foundation for the new policy after the vulnerability audit exercise. If not then one will have to be created from the start or a template will have to be procured to provide the basis of the new document.

*(Worth 5 points for a "YES" answer.)*

**(2) Does the organization periodically review the Security Policy?**

Security is not static. It is dynamic, ever changing as hackers, cyber-criminals, common criminals, industrial spies, malicious internal individuals and terrorists modify their approaches, refine their craft and respond and evolve based upon countermeasures and anti-hacking techniques they encounter in the course of their activities. The security-savvy organization must review their policy on a regular basis. The frequency of review will, of course, vary based upon the industry the organization is in as well as the number of successful and unsuccessful attacks that are detected.

*(Worth 5 points for a "YES" answer.)*

**(3) Does the organization have an internal Security Awareness Program?**

The three elements of good security are policy, technology and people. Management-directed policy provides an essential basis for an effective organizational security program and technology should be deployed in such a manner as to enforce the security policy. People, however, are the element that will make or break a security initiative and a good internal security awareness program is a cornerstone of the people part of good security.

*(Worth 5 points for a "YES" answer.)*

**(4) Does the organization know the value of what is being protected versus the cost of protection?**

Historically security has been "managed" by technologists outside the realm of the traditional business justification process. Increasingly, however, security is being brought into the business justification process and is being analyzed from a risk assessment standpoint, much the way any other potential business liability might be evaluated. In order to operate an effective security program the organization must be cognizant of the impact of any damage vs. the cost of reducing the impact or probability of loss. Actuarial tables and statistics are only now becoming available on a broad enough scope to allow intelligent, risk assessment-based decisions about security to be made.

*(Worth 5 points for a "YES" answer.)*


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

**(5) Does the organization check validity of identity and credentials of workers?**

Good business practice dictates that résumés, training requests, employment applications, identity documents, visa status, educational and training credentials and similar documents be checked for authenticity, accuracy and validity. When business is good, however, these formalities are often waived so as not to unduly prolong the hiring process or antagonize the applicant or prospective customer. When business is not good, however, these formalities are often waived due to the high cost, lack of personnel or time or other similar reasons. The net effect is that organizations rarely do their human resources "due diligence" unless forced to do so due to government or military regulations related to contracts or specific legal requirements.

By not meticulously checking the background of all applicants for employment as well as applicants for certain specialized training organizations may unknowingly be providing food and shelter and, possibly, specialized training to terrorists or others who have the intention to do harm to the organization or, possibly, to the nation. There are a number of examples of this situation associated with the terrorist attacks in the United States on September 11, 2001. Even "odd jobs" or temporary employment can allow spies, hackers, criminals and terrorists the time and money they need to wait to be activated, or can facilitate the training process in support of their future missions.

*(Worth 5 points for a "YES" answer.)*

**(6) Does the organization track compliance with the security policy?**

Most organizations are very informal when it comes to security policy compliance tracking. There are a few basics requirements of human behavior and even more basics of good human resources management that are satisfied with a formal policy of tracking compliance and non-compliance with security policy. The human behavior elements are, basically, that if a person knows their compliance or non-compliance with policy is being monitored, and their score in that area is tied to employment/non-employment or bonuses, they are more likely to know that management is serious about the policy. The employees are, therefore, more likely to adhere to the policy to the extent possible. Another element is that by tracking and logging non-compliance it is possible to see patterns as well as to go back after the fact, for forensics purposes. Any organization interested in using this historical information for purposes of prosecution should also assure that the quality, accuracy and non-repudiation aspects of the log files meet basic evidentiary requirements for the legal jurisdiction in which any potential case may be tried. Though this is an important audit point, changing a "no" answer to a "yes" answer is not always expensive. Many organizations use an existing human resources package that might have the option of tracking time clock violations or some other breach of personnel policy. Systems of this type often have a "ticketing" system with an employee acknowledgement function. This tracking not only provides a level of fairness it also provides a reporting system for management to see where compliance problems exist so they may be addressed.

*(Worth 5 points for a "YES" answer.)*


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

**(7) Does the organization cooperate on security initiatives with suppliers, contractors and/or clients?**

A formal security cooperation program between related companies is as important as a program between related countries and the issues are quite the same. Any organization has security objectives in common with closely related companies and the fates of those organizations are inextricably intertwined. Consider, for instance, if Company A provides raw materials to Company B. Any interruption of the supply chain or sabotaging or tampering with the raw materials of Company A has a direct effect on Company B. What alternatives does Company B have to protect its interests? One option, of course, may be to have several sources of raw material, possibly from different geographic areas in order to reduce the risk of not having raw materials. This is not always possible, depending upon the specific industry and "raw materials" we are discussing. Not only is it not always possible, but increasing the number of sources also increases the security risk as it spreads the focus of security over a broader group of related companies. The same types of issues exist when considering the relationship of the organization to clients. Materials and information must be shared, and this also increases the window of opportunity for sabotage, espionage, theft and other security issues.

*(Worth 5 points for a "YES" answer.)*

## Infrastructure and Physical Security Audit

**(8) Does the organization have back-up plans for basic services?**

It is unlikely that all but the largest, most visible organizations will be the direct target of terrorist or criminal activity affecting basic services such as water and electricity. It is possible, however, that an attack on municipal or state systems will have the indirect effect of depriving the organization of such services. For this reason each organization must understand the impact and have at least a minimal back-up plan. Consider back-up plans for water, electricity, HVAC, transportation systems and basic supplies and raw materials. In some cases simple stockpiling can solve a short outage and in other cases it is possible to get entire back-up systems, such as power generation equipment, which can run the business for an indefinite length of time.

*(Worth 5 points for a "YES" answer.*

**(9) Does the organization have a disaster recovery plan for network and IT services?**

The following section covers data backup and security and is usually the purview of the Information Technology (IT) department. This item covers availability of physical back-up computers and the implementation of a disaster recovery plan and often includes physical plant personnel and others who are not normally associated with the IT area. Items in this area can include the physical movement of data center or call center personnel to an alternate off-site location, physical off-site vaults or data storage for back-up information, physical location and management of mirror servers and similar related activities.

*(Worth 5 points for a "YES" answer.)*


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

**(10) Does the organization have a security plan for especially hazardous materials or processes?**

Each organization will understand exactly what this means in their own context, and should have a specific security plan to cover it. This question may mean nuclear material, it may mean caustic chemicals or it may mean protection from manufacturing processes which might pose a threat to the local community for a variety of contamination reasons.

*(Worth 5 points for a "YES" answer.)*

**(11) Does the organization use basic access control systems such as key cards, cameras linked to guards or keypads? Is access logged and are log files maintained for historical purposes?**

Organizations should be able to document the movement of employees, suppliers, clients, service personnel and other visitors (employee family members, fire inspection teams, food service workers, etc.) in and out of a facility. Use of key cards, cameras with remote admission systems and similar systems provide a big advantage over paper logs or no logging at all. Log files should be maintained for historical purposes in such a manner that their authenticity can be validated and that tampering is greatly reduced.

*(Worth 5 points for a "YES" answer.)*

**(12) Does the organization use advanced access control systems such as biometrics (fingerprints, facial recognition and/or voice recognition)?**

For many organizations the old paper logs provide a sufficient record of entrances and exits for low-traffic or less secure facilities. The next level of access logging and control is a system based upon key cards, key pads, remote cameras or similar devices as discussed in the prior question. Many organizations, however, utilize more expensive and more precise methods of access control, such as finger print readers or retina scanners. The organization is awarded extra points for the proper implementation and use of such systems as they take facilities security to the next level and further reduce the chances of unauthorized access when used properly. These types of systems also usually include indexing systems which are designed to perform rapid searches of the transaction logs to show specific events or patterns of events.

*(Worth 5 points for a "YES" answer.)*

**(13) Does the organization combine basic and advanced control systems such as voice recognition plus a Personal Identification Number (PIN)?**

Implementation and use of multiple access control systems provide additional benefits and make systems more difficult to compromise. Using voice recognition for access, as an example, is a good biometric check, but can be defeated with a tape recorder/player. Voice recognition plus a pass card or use of a keypad to enter a Personal Identification Number (PIN) strengthens the system.

*(Worth 5 points for a "YES" answer.)*


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

## Network Security Audit

### (14) Does the organization have any of the following:

- User assigned passwords?
- Direct dial-in telephone lines?
- Unsecured Telnet terminal access over the Internet or other IP network.
- Routers used in the role of security devices such as packet filters, 'firewalls', or intranet/Internet gateways, proxy servers or translation gateways?
- PCs, workstations or terminals without automatic, time-based, logoff?
- Non-secure physical access to any site or facility where computer or communications equipment is stored or used?
- Home users on VPNs sharing LANs or DSL connections with family members.

There are a plethora of convenience features in any network. Not only do they make the task of using or administering the network easier, they also facilitate the ease of hacking of the network. User assigned passwords, for instance, allow the user to create a password that is easy for the user to remember, but often creates a gaping whole in security as user-defined passwords are often based upon dictionary terms which are easily cracked. Dial-in modems without dial-back security features, for instance, facilitate ease of use from home or administration of systems at a distance. Telnet is the IP network version of 'dial in' and allow hacking of systems from all over the world. Each of the 'ease of use' or cost reduction items listed above, and a myriad others, constitute potential vulnerabilities in organization security which can be exploited by outsiders as well as malicious insiders.

*(Subtract 1 points for each "YES" answer above, but not more than 5 points.)*

### (15) Does the organization use a "firewall" or other similar "perimeter security" product or service? Does the organization manage the firewalls themselves or do they use a third party service?

While use of a firewall or similar type of system does not, in itself, assure the security of a network or networked system(s) it is a very useful tool. In addition to the basic question about the existence of a firewall are questions about how the firewall is implemented and managed. For instance, is the firewall a part of a managed Virtual Private Network (VPN) system or service, or is it managed in isolation? Are all firewalls managed from a central authority and from a central rules base, or are different firewalls managed from different areas within the organization? Is it possible that one firewall might admit network traffic that another one prohibits, and vice versa? When considering the firewall's capabilities other areas of interest are if the firewall supports stateful inspection, logging, proxy services and a wide variety of key features. Another common approach to firewalls is to implement firewalls in a back-to-back "DMZ" configuration, thereby reducing the effectiveness of an assault on a single firewall and requires a coordinated breach of both firewalls for the attackers to be successful in compromising organizational security. An additional bit of fine tuning to a DMZ configuration is the use of two different firewall products to further increase the complexity of any attack.

*(Worth 5 points for each "YES" answer. A possible 10 points total.)*


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

**(16) Does the organization use an Intrusion Detection System (IDS)? Does the organization utilize a third party intrusion monitoring service?**

Formal Intrusion Detection Systems (IDSs) monitor access requests and requests for files and other resources and coordinate those requests with log files and other records of past network and system activity. Very advanced systems used in governmental and military applications can also cross-check and coordinate physical site access logs with network logs. Intrusion Detection Systems also alert network managers when a possible intrusion is detected. Intrusions can be handled in a variety of ways, either from a pre-determined script, or as determined at the time an intrusion is detected. Intrusions may be stopped completely, isolated or allowed to continue and be monitored and logged. The maintenance of an Intrusion Detection System requires a lot of manually intensive updating and customization as new intrusion signatures (the series of steps or processes indicating an intrusion has occurred) are discovered and updated. An extra five points are awarded in this audit for use of an outside, third party, intrusion monitoring service.

*(Worth 5 points for each "YES" answer. A possible total of 10 points.)*

**(17) Does the organization use a Virtual Private Network for external access? Are special security procedures in place at the remote locations to avoid exploitation of the VPN connection?**

A Virtual Private Network (VPN) can be a very effective tool for secure communications, especially if the organization wishes to increase geographic coverage and reduce operating costs by using the public Internet for some or all of the network transport. On the other hand, use of a VPN can also lead to a false sense of security. Through the use of secure, often encrypted/systematically scrambled connections known as tunnels, the VPN effectively extends the secure entry points into the network out to the remote location. Breaking into the intermediate connections, the tunnels, corrupting or otherwise compromising the information is extremely difficult. On the other hand, simply going to the user-end of the tunnel and 'hair pinning' back into the secure connection is an easy exploit which can be accomplished in a variety of ways and is relatively simple to execute. Simply using VPN services is not enough to gain the points that are possible from this audit point. The organization must use VPNs in conjunction with special procedures at remote locations designed to avoid unauthorized access to the VPN. One such technique that can be used is called Air Gap Technology (AGT). AGT means that the VPN-connected computers share no connection with the other computers or networks.

*(Worth 5 points for a "YES" answer to both questions.)*

**18) Does the organization implement network security in a manner which is non-obtrusive and which has a minimum impact on productivity?**

Security is mandatory in any situation, but must be evaluated in terms of its impact on productivity and system ease of use. Often a more expensive security solution is justified if it minimizes negative impact on productivity and system or user effectiveness.

*(Worth 5 points for a "YES" answer.)*


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

**(19) Does the organization have policies and procedures in place to manage a situation where *their systems* are used to launch an attack on other systems?**

A very common type of hacking attack uses the organizations' network-connected computers to elicit a return attack (or hack back) from another organization. By the time the smoke clears the hacker is long gone and the damage has been done. For example, the hacker's target is Company A. The hacker compromises one or more computers or servers of Company A and installs an attack program. The attack program is executed and launches an attack on Company (or even government or military) B. Company B sees the attack (a denial of service attack, for instance, in which hundreds of thousands of incoming requests tie up computing and server resources) coming from Company A and retaliates. Company A is unaware that the hacker had started the attack from their platform and suffers from the attack until they can get Company B to stop. Getting Company B to stop can be very difficult if time zones, cultural and language differences are involved. It can be even more difficult if Company A and Company B are historical adversaries. It is noteworthy that current case law is such that Company A also bears a legal liability if the cannot show they have sufficiently protected their systems form being exploited.

*(Worth 5 points for a "YES" answer)*

**(20) Does the organization have security policies and technologies for dealing with wireless communications?**

Wireless systems, both voice and data, are becoming more and more pervasive each day for communications between mobile individuals as well as in the guise of wireless Local Area Networks (LANs) and Wireless Local Loops (WLLs) to replace the traditional copper wire for network access. This question deals with secure systems put in place to avoid problems with wireless security.

*(Worth 5 points for a "YES" answer)*

| **SCORING:** | |
|---|---|
| **90-100+ Points** | Excellent awareness of security issues, vulnerabilities and scenarios. Apparently needs no help, but is probably not answering honestly. |
| **80-89 Points** | Overall scores are good. Security efforts should focus on the particular areas that are not at 100% as indicated by questions not answered yes on the survey. |
| **70-79 Points** | Needs some help. Would recommend that they read, and implement the suggestions from, *Secrets & Lies*, by Bruce Schneier and *Inside Internet Security (What Hackers Don't WantYou to Know)*, by Jeff Crume. |
| **69 Points** | Recommend that key management attend formal network security training and that an outside organization be engaged to assist with a more formal audit and identification of potential solutions. |
| **68 and lower** | Recommend a full consultation and security audit by an accredited and recognized outside security consulting firm. |


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

***Continued from page 4.***

### External Generalists

*External Generalists provide general knowledge from an external, independent perspective.*

External Generalists mirror the functions of the internal generalists, but have no specific knowledge of Medium's operations. They complete the report card in terms of what is normal for companies with distributed pharmacy operations, in general. This information is used as a benchmark against which Medium's internal information is compared.

### External Specialists

*External Specialists provide specialized knowledge from an impartial external perspective.*

The External Specialists fill a similar role to the External Generalists in that they provide specific information on what similar companies are doing in specific areas: physical facility security, records security and retention, network security, firewalls, computer virus protection, etc.

### Team Leaders

*Team Leaders coordinate the activities of each team and provide a liaison to the Project Leader.*

Team Leaders provide a liaison between their teams and the other three teams as well as with The Project Leader.

### The Project Leader

*The Project Leader coordinates and compiles the common information from all four teams.*

The Project Leader coordinates the entire project and manages the compilation of all of the findings. The actual analysis is discussed in this white paper in a following section.

## The Silver Strategy

*The Silver Strategy is less expensive in terms of money and time and produces a reasonable result for the investment.*

The Silver Strategy is less expensive than the Gold Strategy, but can also produce quite acceptable results. The Silver Strategy is the Gold Strategy without the external benchmarks for comparison. The Silver Strategy is truly an internal self-assessment and can be performed in a shorter time frame and for less money because no outside resources are engaged.

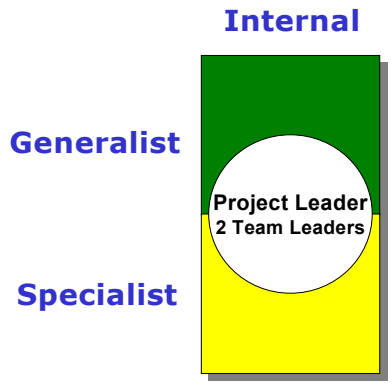


**Figure 2**
**Silver Strategy Staffing**

*The Silver Strategy might be a strategic first step.*

The Silver Strategy is often a good, cost effective, first step in determining how to proceed with an organizational security strategy.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

## The Bronze Strategy

*The Bronze Strategy requires the least time and money and is a very good first step to determine if the additional resources should be spent..*

The Bronze Strategy is the quickest and least expensive internal vulnerability assessment of all. The primary tools are the pen and the telephone. The "Project Leader" of the Bronze Project is usually the CEO, CIO, CFO, CSO or similar C-Level executive who completes the Report Card on their own. When they reach an unfamiliar area a call is placed to the internal specialist and get the answers they need.

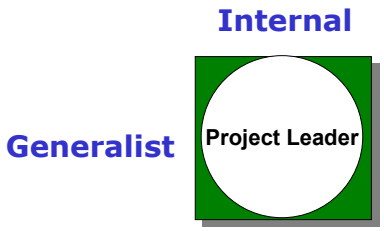


**Figure 3**
**Bronze Strategy "Staffing"**

*The Bronze Strategy is ideal for the executive who is not clear as to the security vulnerabilities of their organization.*

Once completed, The Report Card provides the C-Level executive with a clear picture of the security vulnerabilities and exposures of their organization, and a reasonably clear idea of what areas need the highest initial prioritization and attention.

## Variations on the Theme

*Each industry and company should take their own approach.*

It is possible to combine various aspects of these three basic strategies. For instance, a plan can be put into place that looks fundamentally like the Gold Strategy, but does not use External Generalists. Published research or survey results may be available for a specific industry, eliminating the need for the External Generalist. It may also be possible to allow your Internal Specialists to provide general industry knowledge gained from user group meetings or other sources, thereby saving the cost and time of using External Specialists on the project. Whatever combination of experts and other personnel and resources are needed, or in what order the steps are taken, this is the general set of guidelines to assure success with an internal vulnerability audit.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

# Putting the Report Card to Work

*Modify the Report Card to your own needs and proceed.*

The best way to put the Report Card to work is to begin by understanding the audit strategies as outlined above and then making changes to the Report Card for your own, specific situation. You may obtain a non-copy protected, editable, Microsoft Word version of the **Basic Infrastructure and Network Security Report Card** as provided in the center of this white paper free of charge by sending your request to info@consultant-registry.com. If you received this white paper by email, the Zip Archive you received should have had two documents. One is this white paper you are reading and the other is the MS Word version of the Report Card.

The advanced version of the Report Card, containing approximately 200 questions (as opposed to the 20 questions in the Basic Report Card) is also available for purchase on the www.consultant-registry.com web site.

## Report Card Philosophy and Structure

*The Report Card is organized into three primary areas.*

The Report Card is organized into three primary areas. It is possible to modify the editable version of the report so that the appropriate section of the report card can be printed or emailed to the necessary parties to be completed before being recombined in the final report. Depending upon the distribution of the final report, the narrative text included with the blank report card template may be removed, edited, or simply left in place as explanatory text for the reader. The three primary divisions of the Report Card are:

- Organizational Security Policy Audit
- Infrastructure and Physical Security Audit
- Network Security Audit

We will review each section briefly here.

### Organizational Security Policy Audit

*Organizational policy, human resources, vendor and client security relationships.*

The Organizational Security Policy Audit section covers all aspects of corporate security. This section is the domain of corporate security, if the organization is large enough to have a separate corporate security division, and/or human resources. Other parts of the company involved in this are upper management and possible one or more C-Level executives responsible for the various areas.

### Infrastructure and Physical Security Audit

*Infrastructure and physical security covers capital assets, physical plant and related areas.*

The Infrastructure and Physical Security Audit section basically covers security of anything you can physically touch, with the exception of data and voice networking components, though the physical security (actual locks and keys) of these devices *is* covered in this area.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

### Network Security Audit

*Network security includes computers and connected devices such as servers, firewalls and related systems.*

The Network Security Audit section covers all interconnected networking devices and systems for data, telephony and multimedia networking. If the organization has a web site, it is covered here. Telephone systems and/or call centers, are covered in this section as well. Laptop computers used by mobile employees to access data at the corporate headquarters are also addressed. It is also possible that there will be some overlap of network security with infrastructure where the physical item performing the computer processing and the processing itself overlap. This is normal and cooperation between the different groups is expected.

*The Report Card does not contain all the questions.*

As previously mentioned, the Report Card does not contain all possible questions for all possible areas, but rather it contains a base set of questions to be used as a starting point. The Advanced Report Card is far more comprehensive, with almost 250 questions, but it is envisioned that the basic Report Card should be enough to get any project started.

*The Report Card, once completed, should be marked CONFIDENTIAL.*

It is important to stress once again that after the organizational information has been entered into the Report Card that the document should be marked Proprietary and Confidential and treated as such.

## Analysis, Strategic and Tactical Planning

*Analysis is organization and industry specific.*

Once the Report Card is filled in with the information gathered during the vulnerability assessment audit the paths taken by different organizations will take divergent paths. While security concepts remain constant, their interpretation and importance will change by industry. A library, for instance, does not need to protect its contents from being taken from the building by authorized persons, but should protect their assets from being modified. Complete information privacy, on the other hand, has regulatory mandates in certain industries.

*Strategic and Tactical Planning is an upper management function.*

Once the vulnerability audit has been completed and a general idea of the risks and liabilities has been developed it is time for upper management to draft a plan to close vulnerabilities, or at least to make the vulnerabilities unattractive to those who would exploit them. Each management team must look at their own, unique organization as well as their industry and nation and determine for themselves their own modern version of hunting in groups, circling the wagons and moving their corporate societies into fortified towns.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

# Conclusion

*This is not the end, but rather it is just the beginning.*

Security is not a project as much as a process. The information contained in this white paper represents only a single element of the process. The following sections briefly describe other free white papers in The Consultant Registry's Security White Paper series. You may request any of these white papers from our website at **www.consultant-registry.com**.

## Threats & Vulnerabilities: Security and Your Business

*A clear understanding of the Threats and Vulnerabilities any organization faces is the first step in developing a sound security program.*

Recent surveys have proven three facts:

1) Management is concerned about security.
2) Management does not clearly understand security threats, vulnerabilities, risks and liabilities.
3) Management does not know what to do first in dealing with security problems.

The **Threats and Vulnerabilities** White Paper addresses all three areas and is recommended for all levels of management.

## Network Security: The Business Value Proposition

*Network security is an important part of a business's operations. It should be driven by business needs, not by technology..*

Network security is an important part of any business. All too often network security is driven by the operations and technology people, not by the business needs. Network security can, and should, be put to the same tests for cost effectiveness and return on investment (ROI) as any other investment. This white paper explains many of the underlying fundamentals of understanding the business value of network security.

The **Business Value Proposition** white paper is recommended for all levels of management.

## Four Steps to Improved Security

*There really are more than four steps, but this white paper covers the four major steps.*

The four steps to improved security are prevention, detection, forensics and response. Prevention is obviously the superior strategy as it discourages any would-be attacker from applying their craft in the first place. If prevention is not effective a security breach or compromise must be detected, and reported. Next forensics come into play to assure the breach can be proven and appropriate steps, such as closing the vulnerability and/or prosecuting the perpetrator can be taken. At that point an effective response can be mounted in a timely fashion.

The **Four Steps to Improved Security** white paper is especially recommended for operations personnel.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

## Defenses & Countermeasures

The goal of the **Threats and Vulnerabilities** white paper is to enlighten management about the threats, vulnerabilities and liabilities associated with organizational security. Due to space considerations, however, no actual solutions or answers are offered. The Defenses and Countermeasures white paper proposes, at a high level, solutions to the threats and vulnerabilities mentioned in the current white paper.

*The companion white paper to Threats and Vulnerabilities.*

The **Defenses and Countermeasures** white paper is recommended for all levels of management, for operational personnel and for purchasing agents who will be involved in the procurement of security systems, products and services.

## How Can The Consultant Registry Help You?

*A proper balance of internal and external resources can allow you to respond quickly and cost effectively to security needs..*

The Consultant Registry is a group of two dozen of the top industry professionals with a wide range of skills and expertise ranging from technology to business and that wide chasm in between. The best use of The Consultant Registry's resources is to supplement your team and to help them be the best they can be.

*The Consultant Registry focuses on transferring our knowledge and expertise to our client's team.*

One of our biggest areas of focus, and where we feel the client gets the most benefit is in knowledge transfer. We are best utilized as consultants, advisors, coaches, trainers and focused subject matter experts. Ideally we are not doing the work for you, or on your behalf, but rather as a part of your team, working in partnership to get your work done *and* to transfer knowledge and expertise to your team so that you are self-sufficient.

*www.consultant-registry.com is your resource for all telecom and security training and consulting.*

Consider our web site, **www.consultant-registry.com**, as your staffing catalog for all of your critical security and networking projects.

## Your Mission

*Your mission is to go out and assess the security vulnerabilities of your organization and use the assessment as the foundation to putting an organizational security plan in place.*

Your mission is to use the basic version of the **Infrastructure and Network Security Report Card** included in this white paper to begin the process of assessing the security vulnerabilities of your organization. Once the vulnerabilities are assessed you can begin the process of architecting and implementing a comprehensive and effective organizational security program. Security is a process, not an event. The assessment tool provided in this white paper will enable you to begin the process of assuring security for your organization and everyone who depends on it.


© 2002 James P. Cavanagh, Global Telecom & Security Consultant
jcavanagh@consultant-registry.com / www.consultant-registry.com

# About The Author

## James P. Cavanagh

Global Telecom & Security Consultant

**James P. Cavanagh** has worked closely with five of the predominant communications technologies of our time very early in their life cycles. He has been intimately involved with the engineering, sales support, marketing, design, installation and training for ATM, Frame Relay, IP, optical networking and xDSL since their early commercialization. Mr. Cavanagh has also been intimately involved in network security, disaster recovery planning and infrastructure security since the early 1980s. Jim is able to combine his experience with creativity and a long, varied career to develop exceptionally effective solutions for his consulting clients as well as having a rich background for his teaching and writing. Jim is a former member of the ATM forum.

Mr. Cavanagh's consulting practice is built around three primary areas: traditional consulting, writing and training. In the area of traditional consulting Mr. Cavanagh boasts a long list of recognizable clients in the areas of network and infrastructure security, IP, ATM, Frame Relay, DSL and optical networking as well as traditional telephony areas. The client list includes manufacturers, carriers, service providers and end-user organizations whom he has helped with everything from product specification to network procurement, design, integration, installation, engineering, marketing, business planning and tactical and strategic planning. Mr. Cavanagh's clients are quick to point out that Jim brings major projects in consistently on-time and on budget.

Jim is an internationally recognized expert on infrastructure and network security, anti-hacking, counter-cyberterrorism and business and corporate security. He recently completed a very well attended five city Canadian tour as a part of the TELUS Expert Series which received good press coverage and attendance in light of the events of September 11 and is continuing his heavy involvement in consulting, writing and training in the security area. For additional security related information, please see The Consultant Registry **Focus on Security** Page.

Mr. Cavanagh is the editor of books on multimedia networking and network security as well as author of *Frame Relay Applications: Business and Technology Case Studies*. He is presently writing a book on network and infrastructure security aimed at the corporate and business market, and is starting a new website covering domestic US and International telecom regulatory and legal issues. Mr. Cavanagh is also the author of several popular computer based training (CBT) programs covering Frame Relay, emerging broadband technologies, fiber optic communications basics and advanced fiber optic network design in addition to over three dozen articles for trade publications and journals.

Mr. Cavanagh is also a frequent guest on panels at industry conferences, has been an instructor for the International Communications Association's (ICA) Summer Program at the University of Colorado at Boulder from 1992 until 1997 and is the recipient of the ICA's Citation of Merit Award for "outstanding contributions to global telecommunications". Mr. Cavanagh provides training on ATM, Frame Relay, Emerging Technologies, LAN and TCP/IP Integration, Telecom and Datacom Fundamentals and a variety of other subjects to over 2,500 telecommunications professionals each year. Mr. Cavanagh is very active with the Atlanta Telecom Professionals (ATP), an organization for telecommunications professionals in Atlanta. The Consultant Registry is a Gold Sponsor of ATP.

www.
consultant-
registry
.com

# The Consultant Registry Security Skills Training Series

## SECURITY SKILLS TRAINING SERIES

**A comprehensive series of 3 technical training courses on security topics.**

In addition to management, organizational policy, security awareness and related security consulting and training **The Consultant Registry** offers a full range of technical consulting services and training. **The Security Skills Training Series** is comprised of three courses: an introductory class, and intermediate class and an advanced class, designed to be taken as a series or independently. Additional information on these and other courses is available on the web at www.consultant-registry.com.

**Infrastructure and Network Security™Theory & Practice™,** 2 Day Class. *The Infrastructure and Network Security Theory and Practice*™ course is an introductory level course covering a wide range of areas related to the security of network and operational infrastructure. This is an ideal course to use as a stepping stone to other, more advanced topics, or as a general introduction for organizational security or law enforcement personnel. This course is designed for everyone from the network administrator of a small to large corporation, non-profit organization or academic institution to local, state and federal law enforcement personnel involved in network and infrastructure security, anti-hacking and counter-terrorism. It does not matter if the risks to your network or assets are competitors, industrial spys or international terrorists, this course has a rich, broad content applicable to a wide variety of security needs.

**Network Security Theory & Practice™,** 2 Day Class. This course is an intermediate level course. This is an overview course with a lot of breadth and is designed for the telecommunications networking professional. We refer to this one as a "smorgasbord course" because it offers a little of everything. This course will be of particular interest to individuals wishing to build a base of knowledge that will allow them to go on to our more advanced courses. A lot of emphasis is placed on encryption, hacker techniques, and overall security policy, technology and implementation. This course is ideal for the individual who has just been told by management that they must develop and implement a security program within their organization. This course includes the comprehensive "Network and Infrastructure Report Card" assessment tool as well as a comprehensive security review covering all seven layers of the OSI model.

**Network Services Security™Theory & Practice™**, 2 Day Class. A two day class designed for organizations providing network services and Virtual Private Networks (VPNs), such as Internet Service Providers (ISPs), Network/Backbone Service Providers (N/BSPs), carriers and large organizations managing their own intranets and private IP networks. This class has been very well received by nationally recognized IP service organizations in the US and Canada and is typically attended by network engineers, security professionals and technical managers.

To better understand how **The Consultant Registry** can help your organization contact us at 404.760.0667 or via email at info@consultant-registry.com.


**The Consultant Registry**

**Telecommunications & Security Consulting and Training Since 1994**

**4405 Northside Parkway, Suite 2120 Atlanta, Georgia 30327 USA**

**+1.404.760.0667 - www.consultant-registry.com**