Network Security

The Business Value Proposition

A White Paper for Management

Network security has long been the domain of the technologist, spy and hacker. Increasingly, however, management is realizing that **network security has its own unique value within the business framework** and that **a successful security program is subject to the same evaluations and criteria as any other operational part of their business**.
This white paper looks at the **key elements of the security value proposition** common to most organizations.

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.

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

Network Security: The Business Value Proposition

Network interconnections that bring the benefits and convenience of Internet email, the World Wide Web and ecommerce are also fraught with risk.

The interconnection of a variety of organizations with their clients and suppliers on a local, regional, nationwide and global scale has never been more critical than it is today. A certain amount of risk goes with the convenience of remote access, the opportunities of new global markets and the cost reductions associated with networks based upon the protocols and concepts of the Internet. . No longer is it necessary for a spy to steam open your paper mail, an intruder to enter your physical premises or a saboteur to do damage to your brick and mortar property. Electronic intruders can do all that and more, remotely, using the same tools that bring cost savings, opportunities and convenience to the business world.

Network security has long been part of a separate cyber-world that did not overlap the world of business.

For as long as most people can remember network security, anti-hacking, cyber-snooping, anti-cyber terrorism and similar disciplines have been the quasi-fictional realm of the "white hat hackers", "black hat hackers", CIA, FBI, KGB, RCMP, MI5 and similar organizations. If the topic was discussed in the boardroom or management meetings, it was likely to comment on a news story or gossip about a leaked security event reported in the news, rather than address current issues within the organization. All that is changing.

Cyber-security has become increasingly important to business.

Only recently has management needed to begin to deal directly with the issues associated with network security[1]:

- Impact from hacking 'exploits' affecting company operations, stock price or brand value.
- Additional budgets for security equipment, software training and employee awareness programs.
- Electronic espionage, intelligence gathering and sabotage.
- Additional cost for 'business continuation', 'system availability' and similar insurance policies.
- Public Relations contingency plans in the case of publication of a security 'event'.
- Liabilities from company computers and servers being used as launching pads for computer vandalism and terrorism.
- And many, many more issues, depending upon the business or industry.

In many cases management lacks the experience and expertise to deal with the myriad security issues facing their organization.

[1] These issues are described more fully in the free white paper: *Threats & Vulnerabilities: Security and Your Business* by James P. Cavanagh, available from **The Consultant Registry** at http://www.consultant-registry.com.

Urgency and potential damage only make the security task more daunting for management.

Compounding the problem is the potentially devastating impact a single security breach can have, coupled with the urgency of dealing with security on an organization-wide basis. This is a daunting task for any manager.

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

All of this having been said, the fact that often goes unnoticed is that security is a regular part of business. Security policy must undergo the same scrutiny and rigorous testing as payroll, accounting, personnel, sales and marketing, and any other crucial business process. Does this mean security has a business justification? Yes. Can well-known business processes such as Return-On-Investment (ROI) be applied to security? Yes. Can security be planned? Yes, to an extent.

Our intent is to kick-start the process of organizational security awareness and planning.

In these few pages we are not, of course, able to provide a full range of information on all of these topics, nor is that our intent. Our intent is to help you begin planning, stimulate discussion and debate to kick-start the process of organizational security planning.

We will illuminate the business value proposition of security.

The object of this white paper to shed light on security in the setting of modern business, and help organizations to begin to recognize the value proposition inherent in a good security program.

Take the First Steps

Vulnerability assessment is the first step on creating a comprehensive and effective organizational security program.

The topics covered in this White Paper areonly the first steps. Once an organization understands the role that good network security plays in the overall operation of their business they will better be able to evaluate different approaches, for their own security. A clear understanding of these key points, and devoting time to consider the possible impact on your business, will better prepare you to mount an intelligent, cost-effective, of defenses and counter-measures,. You will understand bottom line as well as the strategic and tactical impact of security.

Securing the Business: A Change in Focus

The stakes are high and getting higher - organizations have no choice but to be prepared for an attack.

The changes in the nature of threats and damage, and the publicity often accompanying hacker 'exploits', network-assisted terrorism or cyber-crime activity, have changed the security stakes considerably. Offensive and defensive tactics employed by organizations have changed in response. In this section we will begin by discussing the shifting security models, network user's security objectives, variations by industry, and then discuss assessing and managing risks.

The Citadel vs Insurance Models of Security

The classic 'citadel' model of security says 'keep the bad guys out and the good guys in'. The newer 'insurance' model says that business security is largely a risk assessment exercise.

As the network security job moves from a part-time job for someone in IT to a full-time focus for management, the security models are also changing. The classic 'citadel' model was to simply keep the 'bad guys' out and let the 'good guys' in. The Citadel Model states if we fortify our castles properly, making them strong and sturdy, outsiders will not be able to penetrate our thick walls and reach the treasures hidden inside. Security was really never this simple and, therefore, the newer model that is emerging is the 'insurance' model of security. It states that security is more a risk analysis exercise than a clear-cut 'good guy/bad guy' scenario. The Insurance Model states that business is not about absolutes, but rather is about managed risk. This model tells us if we insure our businesses against network security problems, much as we would against fire, floods or work stoppage that we are managing the risks in a businesslike manner and that we will be compensated for unforeseeable damage.

The citadel model is fairly straightforward while the nuances of the insurance model can be far more subtle.

The citadel model is fairly binary - the person desiring access is either 'us' or 'them'. There is no gray area, and therefore anyone presenting themselves at the gate may be easily judged. That isif they actually present themselves for inspection at the front gate. That, of course, is exactly what the wily hacker or experienced cyber-criminal works so strenuously to avoid. The insurance model, however, involves budgetary trade-offs and works with the probability of specific problems vs. the cost of protection. The insurance model requires input from security subject matter experts, but is in fact more the expertise of the actuary, and becomes increasingly so as insurance companies gather more and more summary data and statistics about security breaches and hacker exploits. In many cases the "insurance" model of security concludes with an organization purchasing a policy against the risks they assess to be the most likely to occur.

Neither the citadel model nor the insurance model applies completely for any organization. A balance must be struck between the two.

While both models have merit it is easy to see that neither model completely applies to any given situation. What we must find is a proper balance between the two approaches. In the Citadel Model some of those "outsiders" to which we referred are actually clients, employees, suppliers and other valid users. In the Insurance Model we can replace buildings and desks, but it would be very difficult to insure ourselves against the loss of the most important parts of our business, such as our brand, reputation, stock value and client trust. For any given organization, however, such as a government agency, large financial services firm, e-business giant, health care firm, telecommunications company, small law firm, local pharmacy for example, there exists a reasonable balance between the two models. The value of convenience, simplicity and reasonable costs relative to risk must also be figured into the overall network security equation.

Network User Objectives

Generally most users' expectations are similar.

We will now look at the network user's objectives for network security and their general impact on any type of organization, followed by a closer look at vulnerabilities and risks for several major industries.

Confidentiality / Privacy

The organization who owns information would like to maintain control of the information's distribution and modification.

One of the first applications of information security in general, and network security, is to keep information confidential and assure privacy. Since before the time of the pyramids humans have used secret codes to protect information and assure that everything from religious rites and incantations to pottery glazing formulas remained the knowledge of a select group. One key aspect of the need for confidentiality and privacy is that some sort of damage or loss would occur as a result of the disclosure of the protected information. We see this same phenomenon today when information is disclosed, often out of context, impacting decisions such as buying or selling stocks or choosing the services of a specific company.

The first business value of network security:

The first business value of network security is to keep confidential information confidential and within the control of the owning organization.

Information Integrity

Information integrity controls modification of information.

As important as confidentiality and privacy of information are, those attributes of information are often confused with another of equal importance, information integrity. Confidentiality and privacy assure that information is not improperly disclosed. Information integrity assures that regardless of the final disposition, the information has not been altered in an unauthorized way since its origin. Information integrity ideally also includes an audit log showing the origin of information and what changes have been applied, when and by whom.

Imagine the problems that could occur if key transactions relied on financial information to make important decisions but the source information had been tampered with, or if historical records were falsified and became the basis for important legal decisions. Consider changes made by hackers to a pharmaceutical database resulting in death or serious health problems. The ramifications of information integrity are extreme, and the resulting liabilities and damages are only hinted at here. The difference between confidentiality/privacy and information integrity is subtle , but important.

Information integrity is often assumed, but is not necessarily an inherent trait of information.

.The second business value of network security:

The second business value of security is to assure the integrity of data so that it may be relied upon as the basis of decisions and transactions.

Document / Transaction Non-Repudiation

Another key objective of network security is to assure that the origin of a document may be realistically established such that the document's creator or a signatory to the document may not deny their part in its origination. This objective, called document non-repudiation, is as important in the electronic world as it is in the paper world for all manner of documents from purchase orders to house plans to electronic invoices to contracts of all types.

Non-repudiation means the parties to a transaction can not later disavow their participation.

The document non-repudiation aspect of network security is the technical basis of all electronic signature legislation and ecommerce. Though a ripe area for hacking, network-based document non-repudiation schemes generally have the same parameters and assurances as physical signatures. Electronic signatures for instance may be forged, and this is a valid defense if it can be proven. In General however, network transactions of all sizes are routinely carried out, in a variety of world occurrences each day as a result of document/transaction non-repudiation.

Non-repudiation, and the trust system which underlies it, are the basis of all electronic commerce.

The third business value of network security:

The third business value of network security is to assure that all parties involved in an electronic transaction may be realistically proven to have participated even though they may be physically distant from each other during the transaction.

Accountability

Various documents, records, files, emails, magazine articles, scientific papers, research results, statistics and many other pieces of information collectively create our body of knowledge on a certain topic and subsequently affect the actions we will take. In addition to the content of the raw information, humans attribute other values to information, such as the degree to which the information can be trusted and its likely biases. These further attributes are often assigned based upon the source of the information and form a very critical third dimension to the data. These additional elements of the information dramatically effect the perception of usability and reliability of the base information.

Accountability for information ties the document to its source and anyone who may have modified it from its original form.

When the source and/or parties who modified, or could have modified information are known the information may be seen in a different light.

This is when accountability comes into play. For example, in a very broad sense, we might trust an item from ***The Wall Street Journal*** to a much greater degree than something overheard on the street. In a very narrow business sense we might trust a detail in a personnel record, such as a salary figure, far more if we knew it had been entered by the Human Resources department at 14:32:04 on 29-August-2001, rather than by the employee themselves. Accountability is the capability to establish the source of information and by whom, when and what other actions had been taken on that information since its creation. Accountability allows us to examine the raw information regarding the creation, handling and evolution of information and, thereby, to make our own decisions as to its suitability.

The fourth business value of network security:

The fourth business value of network security is to provide an element of accountability to information so that the suitability of information for certain uses may be established.

System Availability

System availability is at the heart of most security programs, regardless of industry.

Virtually all organizations, from lumbering operations to agricultural concerns to online financial services, rely to some extent on access to network-based computing and information resources. Even though the highest profile issues are with systems such as air traffic control, stock markets and the military, every organization experiences some loss as a result of systems not being available when needed. System availability, therefore, is another key objective of network security.

Disruption of system availability is surprisingly easy to do with little technical skill.

Sadly, system availability is one of the simplest areas to attack and is often the target of 'script kiddies' who lack the technical abilities to shut-down or deny access to systems, but who can use 'canned' routines created by others. The question has been raised more than once about the suitability of a technology that can be compromised by teenagers sitting at home trying to impress friends. System availability is the object and denial of service attacks are the frequent exploit, or approach, to disrupting system availability.

System availability may appear to be obvious, but there are many subtleties that need to be appreciated.

While the impact of lack of system availability appears obvious, there are many subtleties that must be considered. The insurance approach would insure against availability problems by multiplying the hourly rate of the employees by the number of hours of a likely outage, by the number of hours per year, and insuring for that amount. Many would say this would not account for lost revenues.. Multiply the average revenue per hour by the average number of hours per year of outage. Add the second figure to the first, and insure for that amount. This hardly compensates for loss of reputation, client impressions of lack of reliability or the strengthening of competitors' position when the business intended for their site goes to the competition. All of these possible damages and penalties are avoided or reduced by the system availability aspect of network security.

The fifth business value of network security:

The fifth and final key business value of network security is to assure that network resources, such as file servers, web pages, email services and similar items are available when needed by employees, prospects or customers.

Network security programs and systems based upon prevention are the best, but rarely get the organizational visibility they deserve because they don't have the same strong emotional impact of sirens going off and dogs barking.

One of the biggest problems facing network security professionals is that network security is one of those odd services where the real objective is for the system to remain diligent and on standby, but not actually be called to action. Think about the shrill sound of a fire siren piercing the night. Only then are we really aware that the system is working and we are seeing a return on our investment. However, we understand, intellectually, but not emotionally, that the better fire system is one of prevention. We should reward our firefighters for prevention campaigns, inspections and awareness programs that reduce fires. The fact is only when we hear the siren are we emotionally satisfied. We must assure that reasonable measurements are built into our network security systems. It must be part of the program and part of the compensation.

The Security Business Value Proposition: A Review

	Description
1	**Confidentiality / Privacy** To keep confidential information confidential and private, and within the control of the owning organization.
2	**Information Integrity** To assure the integrity of information so that it may be relied upon as the basis of decisions and transactions.
3	**Document / Transaction Non-Repudiation** To assure that all parties to an electronic transaction may be realistically proven to have been a part of the transaction even though the parties may be physically distant from each other during the transaction.
4	**Accountability** To provide an element of accountability to information so that the suitability of information for certain uses may be established.
5	**System Availability** To assure that network resources, such as file servers, web pages, email services and similar items are available when needed by employees, prospects or customers.

Table 1
Security Value to Business

Each industry sees varying degrees of value in each of the security aspects.

Now that the business value of network security has been clearly identified we will further investigate the relative value, and changes in value of each of the above items by industry

Security Vulnerabilities by Industry

It is impossible to generalize, but this table represents a fair cross section of security value.

While it is impossible to pinpoint the vulnerabilities of an organization precisely, there are some generalizations that can be made to assist the executive or manager to begin to understand the scope of possible vulnerabilities, and allow them to begin to ask the proper questions to seek the right solutions. Security vulnerability generalizations are summarized in the following table and discussed further in the next section. Industries represented here by no means form a comprehensive list, but are representative cross-section.

Industry	Confidentiality/ Privacy	Information Integrity	Document Non-Repudiation	Accountability	System Availability
Finance	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Government* *except military	★★★★★	★★★★★	★★★★★	★★★★★	★★★☆☆
e-Business & Information Technology	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Health Care	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Insurance	★★★★★	★★★★★	★★★★★	★★★★★	★★☆☆☆
Education* *except administration	★☆☆☆☆	★★★★★	★★★☆☆	★★★★★	★★⯪☆☆
International Trade/Broker	★★★☆☆	★★★★★	★★★☆☆	★★★★★	★★★★★
Your Business?	?	?	?	?	?

Table 2
Security Vulnerabilities by Industry

These values may not be universally accepted, but are, at the very least, a starting point for discussion.

The network security issues shown in the table about have been previously discussed in a general framework. We will now discuss them as they relate to the specific industries listed above and to specific security values to business. Individuals in each industry may disagree with our specific assessments, but at the very least, this table forms a starting point for meaningful dialogue about the issues.

Finance

Finance has very stringent security requirements. Security is high because this is 'where the money is'.

Finance has been given five stars across all categories. The basis of finance is trust in all information and transactions, confidentiality, and the ability to perform any transaction at any time. The potential loss to a company in the financial industry can cost justify, and in fact mandates, the highest possible level of network and systems security. Loss of reputation can be fatal for a financial services company whose reputation/name is really the only factor distinguishing them from competing organizations in their industry capable of handling the same transactions.

e-Business and Information Technology

eBusiness and IT also have stringent requirements: they provide the platform for financial transactions.

The e-business and Information Technology (IT) areas must live up to the same rigorous standards as the finance industry because e-business and IT often provide the delivery platforms for the financial industry and have similarly high risk profiles.

Health Care

HealthCare's security issues deal with tampering and timeliness of information.

Information provided within the health care industry must be of provable quality and must not be disclosed or tampered with. Health care information delivery must not only be accurate, but timely as well because often a life hangs in the balance. In health care there may be needless suffering and death followed by severe financial losses. Health care networks are held to the highest possible standards of quality.

Insurance

Accuracy and non-repudiation are critical in the Insurance Industry.

The insurance industry has the same need for accuracy and non-repudiation of the billions of dollars worth of claims filed annually as any other financial transaction. Even though outages may be inconvenient, the insurance industry is dealing with historic events. Availability issuesare critical when it comes to client and care provider network access. In this case the availability requirements are as high as any other industry where the reputation of the insurer rides on customer perceptions of quality. Comparisons to competitors' quality are also important in this case.

Education

Unauthorized access to educational information is not an issue, but tampering and vandalism are important.

With the exception of the administrative area educational networking and computing runs much more like a library. The accuracy and origin of information is of the greatest importance, but protecting it from unauthorized access is not as important, as the key is to have the information shared by many students with various needs.

International Trade/Brokerage

The trade/broker networks exist based upon trust and long-standing relationships

International trade and brokerage generally have fewer requirements for absolute secrecy than for speed and accuracy. Non-repudiation requirements are often less than in other areas, , because in many cases the parties to the transaction are known to each other and work on a system of trust which predates electronic systems.

Government

Information integrity requirements are high in government security.

Like the financial industry, government has a need to provide consistent information of the highest possible integrity. However, with the exception of the military, most aspects of the government do not have the fast response nor uptime requirements of the financial industry. In many cases attacks which make government systems temporarily unavailable or slow systems down rarely cause lasting problems as the systems under attack often have suitable manual back-ups.

What are the requirements for your specific business?

Your Business

With the foregoing discussion in mind, it might be a good time to take a few moments out and consider the specific needs of your organization.

Citadel and Insurance Models Revisited

Let's revisit the two prior security models and add some details.

Let's revisit the Citadel and Insurance models of security discussed earlier and investigate how we might strike that proper balance between the two in light of our new knowledge of network security. For this purpose we will take a look at the following diagram, "Network Security Model Applicability".

Figure 1 clusters the 5 key elements on the security continuum from citadel to insurance model.

There are several noteworthy aspects to this diagram. The first is that information integrity, accountability and document non-repudiation are clustered together as they all are associated with tracking objects, most commonly files, and their various interactions with other things, such as application programs and users, authorized or unauthorized. The next aspect is that system availability is the objective to which the Citadel model most applies, as it has to do with access control: we could almost picture the security checkpoints at our electronic castle. Confidentiality and Privacy are also better served by the Citadel Model in many cases because they most often have to do with documents or information that is stored, or is in transit between where it is stored and where it is needed.

The Insurance Model is more applicable to information integrity, accountability and document non-repudiation because the ability to control these aspects using technical tools is lower, and the issues of the impact are more in the human realm than the technical.

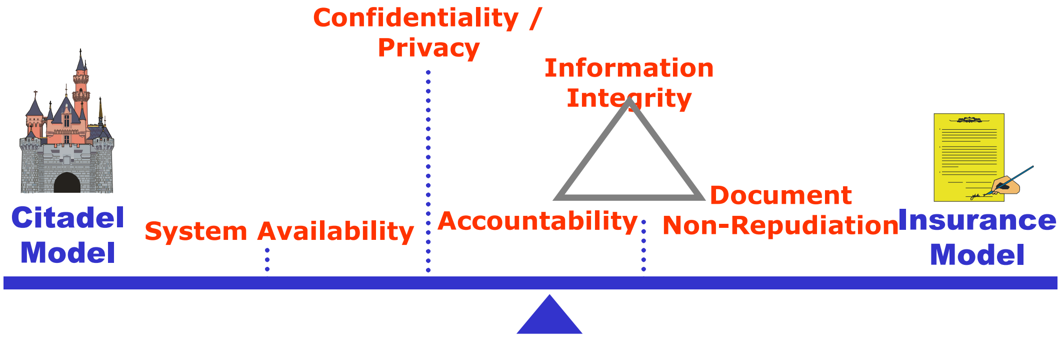

Figure 1
Network Security Model Applicability

Where does your industry or organization fall on this continuum?

Which model works best for your organization? There is no clear answer, but some reflection on your own needs as well as discussion with internal and external subject matter experts should begin to clarify where the initial emphasis can be placed, and how you can best focus the specific business benefits of network security.

Assessing and Managing Risk

Business is, and always has been, about managing risk. Business security is another element in the risk categories.

Once an organization's owners and managers have admitted that risk is an inevitable part of doing business, especially in a networked environment, they must realistically assess risk and manage it accordingly. **The Consultant Registry's** experience in network security consulting leads us to conclude that as important a point as this is risk is rarely assessed properly. In most cases risks are either grossly over-exaggerated, leading a customer to over-emphasize and over-budget for security, or greatly under-estimated leading to big gaping holes in the customer's network security mechanisms.

Assessing Risk

Each organization must assess their own risks before undertaking any activity.

Risks must be assessed for each organization independently. Only the organization can get an idea of what risks exist and the possible impact to their operation as to their ability to perform the functions of their business. Each organization must execute its own internal assessment. A starting place might be to engage an outside organization to perform a security audit and provide an initial report card identifying areas of possible risk and perhaps facilitate the internal discussion. An organization should also gather information about security risks and vulnerabilities of similar businesses.

Managing Risk

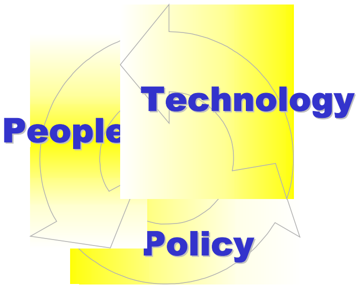

Figure 1
The Three Elements of Good Security

The three elements of good security take Policy, Technology and People into account.

Once the risks have been initially identified it is imperative to put definitive policies and procedures in place. To do so successfully responsible areas within the organization must assist in implementing an overall plan that addresses the three elements of good security: policy, technology and people. Policy drives the technology choices, technology implementation uniformly enforces policy and people are the final element that will either make or break a security system.

The Three Elements of Good Security

People

The first element of good security is people. People can make or break any security program.

From a people standpoint appointing a director or executive vice president of corporate security, or even better, a Chief Security Office (CSO) would be a good place to start. This person would possess a keen knowledge of your organization and industry, a sharp analytical capability and eye for details. These are more important in such a position than a strong security background. The security skills and technical capabilities can be hired: what are most needed is vision and an insider view of your company.

Policy

The second element of good security is policy. Policy is an organizations set of security rules and guidelines.

A strong policy statement that makes clear the acceptable and unacceptable networking practices and their ramifications, as well as penalties, is also critical. As a part of this program an internal security awareness training program and signed statements by employees stating their understanding of security policy are key.

Technology

Technology should be the vehicle for implementing the policy and monitoring the people.

The technology piece, while important, is only one of the three elements, and is the easiest to acquire from outside sources. Even though technical security vulnerabilities are most often reported in the press, and far and away more interesting, it is actually people and policy issues which allow technology-based exploits to be successful. The malicious "I Love You" software did not run on its own, its success required people (in this case millions of people globally) to start it running. Hackers don't guess everyone's password; they often find it on scraps of paper in the trash. Formidable mathematical scrambling programs, known as encryption, don't lay down and die when hackers show up, but rather, the hackers exploit vulnerabilities in the underlying math or even steal the information from a person's computer before it is scrambled or after it is unscrambled.

A Comprehensive Program for Good Security

A comprehensive program for good security will balance all three elements.

A comprehensive program taking all three elements into account must be customized and put in place. It must receive management scrutiny and support at the highest levels and be an ongoing effort. Good security is not a one-time event, but rather an continuous process requiring focus, discipline, budget, regular review and the overview of a talented and qualified outside organization with "in the trenches" experience and current network intelligence.

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.

Security Vulnerability Audit

Those who triumph,
Compute at their headquarters
A great number of factors
Prior to a challenge
Sun Tzu Art of War.

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 simple system for grading your own security vulnerabilities. This simple self-assessment tool is designed to provide a basis for further security planning.

The **Security Vulnerability Audit** white paper is recommended for operations management and personnel.

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.

Defenses & Countermeasures

The companion white paper to Threats and Vulnerabilities.

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 **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 provide a secure, productive and cost effective environment in which trust can thrive and your organization can maximize its business potential.

Security has been shrouded in mystery and secrecy for a very long time. In many cases it still is. That does not mean, however, that security expenditures do not have to undergo the same scrutiny as any other expenses and that security projects do not have to have a return on investment. Somewhere on that continuum between the simplistic citadel model and the risk-based insurance model lies the ideal security posture, philosophy and product set for your organization. Find that set of technologies which meets your needs, be sure to consider the business justifications and the three elements of good security - policy, technology and people - and develop a cost effective, high impact security program for your own organization.

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 Consulting Service

POLICY   TECHNOLOGY   PEOPLE

INDEPENDENT SECURITY AUDIT

The Security "Second Opinion"

An independent security audit of your policy, technology and people can provide the basis for a custom corporate security program or act as an important "second opinion" on security programs presently being implemented.

The single biggest obstacle to a comprehensive security plan for most organizations is the absence of clear, accurate information about threats, risks, vulnerabilities, and liabilities as it relates specifically to their organization. The Consultant Registry can solve this problem with an independent security audit. The independent security audit can provide the basis for an organizational security program or can be a critical 'second opinion' for organizations who presently have a security program or are in the process of implementing one. **The Consultant Registry** Independent Security Audit can focus on any combination of the elements of security: Policy, Technology & People.

Policy
We can review your existing infrastructure *and* network security policies to determine if they provide a sound, current foundation for a comprehensive organizational security program. We can offer recommendations for improvement or create a new policy from the beginning. Working with your management team we can assure that security policy is consistent with human resources guidelines and that security compliance does not negatively impact performance, efficiency and productivity.

Technology
Security technology has historically dictated policy. An Independent Security Audit can help assure that the reverse is true. Security policy will be implemented and supported by technology. The chosen technology will provide a provable return on investment (ROI) and meet other key guidelines of any other business activity. This is one of the key areas where **The Consultant Registry** distinguishes itself: we are technologists with a sharp focus on business needs, goals and objectives.

People
Even though addressed last, people are the most important element of any successful security program. Employees, contractors, customers, suppliers, or other people within the scope of your business can be the biggest liabilities as well as your first line of defense. An Independent Security Audit will help you assess the risks as well as understanding how to increase the security effectiveness of the people who affect your business.

To better understand how **The Consultant Registry** can help your organization contact us at the address, phone number or email below.

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