Threats & Vulnerabilities

Security and Your Business

A White Paper for Management

Recent surveys have proven three facts:

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

This white paper addresses all three areas.

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

December 2001

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 loose constellation 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

OVERVIEW 1

SECURITY THREATS AND VULNERABILITIES 1
THE NEW BUSINESS LANDSCAPE - UNCERTAINTY REPLACES TRUST 1
TAKE THE FIRST STEPS 2

THREATS & VULNERABILITIES 3

WHO 3
Threat Source Matrix 3
External Threat 3
Internal Threat 4
Crossover Threat 4
Competition 4
Espionage / Cybercriminal 4
Terrorist 4
Hacktivist 5
Unknown 5
WHAT 5
Threats Ranking Checklist 5
Threats to Infrastructure 7
Threats to Network and Communication Systems 7
Threats to Personnel 7
Threats to Product / Service 7
Threats to Brand / Reputation 7
Exploitation / Reallocation of Assets 7
Unintentional Assistance to Hackers / Terrorists 8
Threats to National Defense 8
WHY 8
Competitors 8
Spies / Cybercriminals 8
Terrorists 9
Hacktivists 9
Unknown 9
WHEN 9
Holidays 9
Layoffs 9
Times of Higher Visibility 10
Increased Competitor Activity 10
Highs or Lows in the Marketplace 10
Unusual Patterns 10
Times of Lower Security Vigilance 10
What is Common in Your Industry? 10

WHERE 10
HOW 11
Infrastructure 11
Network and Communication Systems 11
Personnel 12
Product / Service / Brand / Reputation 12
SUMMARY 12

CONCLUSION 13

NETWORK SECURITY: THE BUSINESS VALUE PROPOSITION 13
SECURITY VULNERABILITY AUDIT 13
THREE STEPS TO IMPROVED SECURITY 13
DEFENSES & COUNTERMEASURES 14
HOW CAN THE CONSULTANT REGISTRY HELP YOU? 14
YOUR MISSION 14

Overview

Security Threats and Vulnerabilities

Personalize the story by asking "What is the impact on my organization."

This is a story about security threats and vulnerabilities. This is a story about your business. You will benefit a lot more from this story if you would pause from time to time and ask the questions *"What does this mean to me personally?"* and *"How can I take action on this in my own business?"*

We will answer the Who?, What?, Why?, When?, Where? and How? of organizational security.

Like any story we have specific points we must cover. We must answer the Who? What? Why, When, Where and How of organizational security. And though the specifics will vary from organization to organization there are some similarities across most businesses. By the end of the story you will have a much better idea of:

- **WHO** might wish to compromise your information, do harm to you or your employees or exploit your products or assets to attack other organizations or compromise our national defense.
- **WHAT** these attackers might do, and what they have done to other organizations.
- **WHY** the security situation is as it is today, the attackers do what they do and might select you as a target for their attacks.
- **WHEN** the attackers are most likely to strike.
- **WHERE** their attacks are most likely to focus and ...
- **HOW** they do their jobs.

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 the thinking process, to stimulate discussion and debate and kick-start the process of organizational security awareness and planning.

The New Business Landscape - Uncertainty Replaces Trust

One major non-human casualty of recent events is trust.

The landscape for all businesses large and small has changed both dramatically and subtly since September 11th. For the most part we have gotten over the shock of the events. Now the difficulty lies in understanding and managing the impact of these incidents on our lives and routines. If there is one major non-human casualty of recent events it is trust: trust in our relationships, trust in our future, trust in our business and banking transactions, trust in our mail. Whatever we do in the area of security we must build on the trust that still exists.

This is easier said than done, however. Trust takes years to build and only seconds to destroy. It is fragile, but it is the lifeblood of business and the very foundation upon which business has been built for centuries and must continue to be.

Security is that important chore which cannot be put off any longer. It has been on the 'to do' list long enough and is now crying out for attention.

What has filled the void left by trust? Uncertainty. The time is now to take some action, to combat security issues big and small, local and global, in your organization and on a national scale. We are in an unprecedented time of anxiety, uncertainty, mistrust and confusion, but the experts tell us, and anecdotal evidence supports the assertion that the best way to combat these feelings and get back into a productive regime is to take action. So, let's look at security as that project that must be tackled and take the first steps.

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 are, of course, only the first steps. Once an organization is aware of its own vulnerabilities, it must put a program in place to defend against or avoid situations that can be foreseen, and respond quickly and effectively to those which can not be forecasted. By having a clearer understanding of these key points, and devoting time to consider the possible impact on your business, you will be better prepared to mount an intelligent, cost-effective, well-considered campaign of defenses and counter-measures, and suitable responses to the unknown.

Who

Do not underestimate any source of attack. Rank them in order of likelihood and plan accordingly.

There are several possible types of organizations and individuals who may pose a threat to you. It is not prudent to discount any of these potential adversaries, but rather to rank the likelihood that they will cause problems and plan accordingly. The following Threat Source Matrix will allow you to assign a relative threat value to each. This will help the thought process as we continue on and look at the other facets of threats to your organization.

Complete the Threat Source Matrix. Assign a value from 1 to 100, with 100 meaning 100% likely this is a source of possible attack on our organization.

The Threat Source Matrix will help you understand the source of threats to your organization. Virtually all organizations will be subject to threats from all sources to some degree. The problem of security is also compounded by the fact that these sources will not stand in line to attack you one at a time, but rather may attack in parallel in a coordinated or uncoordinated fashion.

Threat	Competition	Espionage/ Cybercriminal	Terrorist	Hacktivist	Unknown
External					
Crossover					
Internal					

Table 1
Threat Source Matrix

Any type of threat can come from an External Source, Internal Source or someone in the gray area between Internal and External.

Threat Source Matrix

The Threat Source Matrix is organized to show the possible sources of threats across the top and their positioning on the side. Any type of threat can come from any position. You could, for instance, be attacked by a spy who is an employee. The attacker could be a competitor with no ties to your organization, or a teenager who works for a courier service, or a contractor working on your company's web site.

External sources are those not connected with your organization

External Threat

Threats can come from **External** sources. This includes attacks from afar, such as across the Internet or through the mail. This category includes attackers who use an indirect approach, such as spreading misinformation about your organization through press "leaks" or malicious Internet postings, or even those who might use your computers to coordinate attacks on other targets. The external threat can come from anywhere on the globe in a variety of guises.

Internal Threat

Internal assistance is cited by the FBI in over 70% of corporate security breaches.

Threats can also be **Internal**. They can come from individuals inside your organization: disgruntled employees, malcontents and internal troublemakers. The internal threat is by far the biggest source, estimated by the FBI to exceed 70% of security problems. The internal threat can have the biggest negative impact on organizational efficiency and productivity because employees are unsure who they can and cannot trust within the organization. The normal response is to trust no one and this undermines organizational effectiveness.

Crossover Threat

Crossovers are neither the distant external threat nor are they as intimate with the target organization as the internal employee - they are somewhere in between the two.

The crossover threat can not be clearly defined as internal or external. The **Crossover** category includes contractors, travel agents, delivery personnel, visitors and others who have access to your information, facilities and personnel as a part of the normal course of their work. A lot of information about your organization can be gained by visitors who check over your visitor logs when they sign in, or by couriers or delivery personnel with a knowledge of the source and quantity ofmaterials delivered or shipped. A contractor or temp employee may have the same access to material and information as an employee, but often without the same background check.

Competition

Competitors are a traditional adversary.

The organization wishing to breach your security might be 'the competition' or a group or individual engaged by your competition. Competitive intelligence takes many forms, but surveillance, information gathering and penetration by competitors are a long-standing source of security problems. Competitors have always gathered confidential information in the attempt to sabotage each other for. Tools such as the Internet only improve their success ratios.

Espionage / Cybercriminal

Espionage is not just the realm of fictional spy novels. It can affect a variety of organizations.

While we are inclined to think about 'espionage' as the subject of spy novels, many organizations have processes or knowledge that is of great use to organizations other than direct business competitors. This category also includes cybercriminals - those who would gain financially from their spying or theft of information or resources. Cybercrime such as theft of information, credit card fraud, identification theft and similar crimes represent a multi-billion dollar per year problem globally.

Terrorist

Estimates of the number of terrorists who have gone through the al Queda training camps range from 50,000 to 500,000. Terrorists are active in over 65 countries.

Terrorists pose a potential security problem to organizations of any size. The biggest threat to most organizations from terrorists is indirect, attacking an organization's assets. This can range from a terrorist commandeering your aircraft to a terrorist receiving a small salary sufficient to live in the country long enough to participate in a planned action.

Hacktivist

Hacktivism can attack any organization at any time and is often a cover up for more serious security breaches. Hacktivists range from high school 'script kiddies' to the most professional hackers.

The hacker/activist, or **Hactivist**, is also a serious security threat to most organizations. The hacktivist ranges in skill level from the less knowledgeable junior hackers, often called 'script kiddies', to the most skilled hackers. Hacktivism can range from simple threats like email that clogs up servers to sophisticated denial of service attacks that bring down a system by making millions of requests very quickly. Hacktivists range from high school kids to true professionals.

Unknown

Attackers are often put into the unknown category because the can not be sorted into the other categories.

Unfortunately, **Unknown** is the category into which most threats fall. Due to the high cost in time, money and potential bad press, most security breaches go unreported and as a result are not prosecuted. Unknown in most cases is a grab bag of individuals from other categories. Attackers are often put into the unknown category because not enough is known about their identity or motivations.

What

Threats Ranking Checklist

Asking the proper security questions for your organization is an important first step in vulnerability assessment.

In the last half of 2001 we have seen the worst that can be done from a security standpoint. The real insight into the security dilemma is asking the right questions relative to your organization. For example, if the question is "What is the likelihood that one of our airplanes will be flown into a major target?" and your business is heavy equipment rental, but does not include airplanes, the answer would be 'not a possibility'. If, on the other hand, you asked, "How might our equipment be exploited to attack a key target?" you may tighten license checks and begin photocopying the identity documents of people renting heavy machinery. If you ask "What is the likelihood that we will encounter a letter contaminated with anthrax?", you may miss the point entirely. On the other hand, if the question you asked is "How might a terrorist exploit our processes or tamper with our products?" you might begin storing your chemicals in a more secure area or reviewing the security procedures of your suppliers of raw materials.

Use the checklist to help assess your own vulnerabilties.

In order to begin the process of assessing your own vulnerabilities, you may use the following **Threats Ranking Checklist**. Check the threats that may apply, even remotely, to your situation and ignore those that do not. As you review the possible attacks listed below please be sure to word the question as appropriately as possible for your situation. If for instance, you don't have a product per se, but rather a service simply insert the word service to get the proper meaning.

Check	Probability	Threat
		Threats to Infrastructure
	%	Sabotage/interruption of water service
	%	Sabotage/interruption of electricity
	%	Sabotage/interruption of Heating Ventilation and Air Conditioning (HVAC)
	%	Sabotage/interruption of traffic/vehicular movement
	%	Sabotage/interruption of movement of deliveries, goods and supplies
		Threats to Network and Communication Systems
	%	Interruption or denial of service for voice, data and/or video services
	%	Exploitation or theft of telecom services (voice, data, video or fax)
	%	Unauthorized disclosure or modification of data
	%	Unauthorized access to electronic transmissions (voice/including wireless, data, video or fax)
	%	**Threats to Personnel**
	%	Unauthorized facility access
	%	Personnel safety off site/in travel status
	%	Contamination / cross contamination of facilities/buildings/offices/plant
	%	Stoppage of work or production facilities
	%	Threats to personnel families, contractors and others
		Threats to Product / Service
	%	Sabotage / tampering with raw materials
	%	Product tampering
		Threats to Brand / Reputation
	%	Product tampering
	%	Unauthorized information compromise or disclosure
	%	Other malicious modification of internal or external information, web site, press releases or other information sources
	%	Misinformation / incorrect news stories
	%	Internet chat room or email based sabotage
		Exploitation of Assets
	%	Theft or reallocation of company assets
	%	Modification of systems or materials for offensive purposes
	%	Exploitation of company expertise or experts for terrorism or criminal gain
		Unintentional Assistance to Hackers / Terrorists
	%	Providing employment, training, housing or cover to terrorists
	%	Providing access to materials or supplies which may be used in terrorism
	%	Providing access to communications systems, the Internet, wireless communications or other resources to coordinate terrorism
		Threats to National Defense
	%	*see Unintentional assistance to hackers/terrorists*
	%	*see Exploitation of assets*
	%	*see Product tampering*

Table 2
Threats Ranking Checklist

The Table above is divided into multiple categories to allow you to identify and rank the most likely targets of criminals and terrorists. We will describe each briefly here.

Threats to Infrastructure

This area incorporates any threats to the basic systems that are required for an organization to operate and include all basic services and transportation. For most corporations these systems will not be subject to direct terrorist attack, but will be the byproduct of attacks on government or utility company systems. For instance, if you run a small manufacturing facility the likelihood that a group of terrorists will specifically target your operation is infinitesimally small. However, you should consider a contingency plan (such as a backup power generation system) in the event that the municipal power system is attacked.

Threats to Network and Communication Systems

The threats in this area are many and range from hackers rendering the voice, data, video and/or fax systems inoperative to using these systems to coordinate terrorist activities. This area is, in itself, an entire industry.

There are a wide variety of threats to any organization. Many organizations have additional specialized threat categories based upon their unique industry.

Threats to Personnel

Threats to personnel are among the most serious because your employees, and their unique knowledge and capabilities are the true foundation of your company. Human assets must be carefully assessed in terms of their value to terrorists: either for their direct capabilities or for their value in leveraging other resources (i.e. a hostage situation).

Threats to Product / Service

Threats to the basic products or services of an organization are often the intention of competitors. Sabotage, blocking of access to raw materials and destruction of finished goods have all been documented over the years, as has product tampering. Their are a variety of motivations for these actions, but the results are the same.

Threats to Brand / Reputation

Because a company's brand and reputation are both valuable and fragile threats to a brand or reputation are the most difficult to guard against. Unfortunately these are also among the easiest attacks to perpetrate. A company can find their stock value rise or fall overnight based upon artificial news on the Internet or misreported via regular news outlets.

Exploitation / Reallocation of Assets

How can criminals, attackers or terrorists use the assets of your organization? Can your network servers be used to store and forward hackers' or terrorists' messages? Can they use your airplanes, heavy equipment or other assets? Your judgement in this area is critical. Consult your internal experts on this important matter.

Unintentional Assistance to Hackers / Terrorists

Does your organization provide jobs, visas, assignments or other resources that aid terrorists in their activities? This is an area of great concern both for companies and the national defense.

Threats to National Defense

Each organization is a link in a chain of national defense. Each organization must do their part to assure that the chain is unbroken. Employee awareness is one of the most important tools in this area.

Why

In order to understand the "Why" part of organizational security, let's return to the "Who". The threats to your security come from five predominant groups or individuals:

Each adversarial group or individual has their own motivation. Understanding their motives is a key to preventing their success.

- Competitors
- Spies / Cybercriminals
- Terrorists
- Hacktivists
- Unknown

Each group or individual has their own motivation. We will examine each briefly.

Competitors

Competitors want to hurt your business prospects.

Competitors want to improve their chances in business, hurt your chances, or both. Competitors might be trying to improve their time-to-market by obtaining your intellectual property without having to do the research and development themselves. They may also attempt to get your customer lists or other market data, or try to damage your reputation, brand or market standing. Competitive Intelligence, dirty tricks and sabotage have existed long before the Internet, but the Internet era has ushered in substantial information gathering and sabotage opportunities against the unsuspecting company.

Spies / Cybercriminals

Spies want to steal your information.

Spies want your information. Often they are agents of foreign governments or industries. Spies differ from competitors (or competitive spying) in that they may not seek to compete with you in the marketplace, but simply need your information or resources for some other requirements. Spies can gain valuable information from a variety of sources. Like competitors, they are not above actually obtaining employment in your organization to help them in their mission.

In addition to compromising your information the cybercriminal also wants to gain financially.

In addition to wishing to compromise your information for the variety of reasons a spy might, cyber criminals also hope to profit from their spying. They may sell your information to a competitor, black mail you, or use you or your clients' credit card information.

Terrorists want to upset operations in a highly visible way to publicize their political or religious agenda.

Terrorists

Terrorists want to create highly visible, press-worthy events on a grand scale. Their objective is not only to terrorize their targets, but also to impress their own people with their mighty capabilities.

Hacktivists use the World Wide Web to publicize their agendas or otherwise gain fame or notoriety.

Hacktivists

Hacktivists are seeking attention. They deface web sites, shut down large companies and generally disrupt network operations through malicious email, viruses, Trojan horses and worm attacks. Hacktivists range from teenage 'script kiddies' wishing to impress their peers with power and prowess to those that would deface web sites or create other mischief to publicize their views. The line between terrorists and hacktivists can be a thin one if hacktivists use the network to shut down power grids, disrupt phone service, modify flight operations or other terrorist acts.

Unknown belongs to one of the other categories, but we don't know which one.

Unknown

Unknown is most likely an individual or organization fitting into one of the other categories, we just lack sufficient information about them to put them into one of the other categories.

When

The timing of an attack is one of the hardest things to predict, if you are even aware that an attack is likely.

While there is no absolute way to predetermine when a breach of security will be attempted, there are some historical patterns that may be observed. The suggestions provided here will probably vary widely from what may be expected in your situation or industry, but it will at least provide some insights into the types of patterns of which we are speaking.

During holiday times security is often more lax. This can be exploited.

Holidays

Holidays are a time when people are naturally less vigilant about security matters. Some major military operations have exploited holidays. The Tet Offensive began on the Vietnamese Lunar New Year, Pearl Harbor happened as military personnel were more relaxed during the Thanksgiving-Christmas holiday season, to name just two. Unfortunately, holidays should be a time of heightened security alert and diligence.

Layoffs or other times create greater hostility toward an organization and are often a time of greater risk.

Layoffs

In our present financial situation layoffs, often involving thousands of people at one time, are a fact of life. Layoffs are also a substantial vulnerability in terms of organizational security. Not only are soon-to-be former employees more likely to make some bad decisions regarding how they should behave relative to the company, but they are also far more open to being approached by competitors and spies. If the job interview is a great source of competitive intelligence, the job interview immediately following a layoff is an absolute gold mine!

Times of Higher Visibility

Any time a person or organization is more in the public eye their risk is increased.

Any time an organization or individual's visibility is increased for any reason the chances of security challenges increases. If a company has increased paid advertising, for instance, they are reaching a broader audience. This may increase the likelihood of an attack by those who do not share the same beliefs, competitors, or a variety of other sources. If a company or individual is in the news, for good or bad reasons, they may increase their risk of attack. For example, a company alleged to have done damage to wildlife, water or air may become the target of hacktivists, even if the allegations are untrue.

Increased Competitor Activity

Increased competitive activity may be a time to be more diligent.

Increases or changes in competitor activity, such as product line changes or shifts in market focus are often accompanied by increased security risks. Other "red flags" in this area are major changes in the composition of senior management, the board of directors, or change in ownership.

Highs or Lows in the Marketplace

Market highs and/or lows are often times of increased activity and security risk.

Market changes, either up or down, are often indicators of increased security risks. Companies riding the wave of an up market are often emboldened by a feeling of invincibility to attempt things they may not otherwise. On the other end of the spectrum are companies who might make certain moves or take certain risks out of desperation.

Unusual Patterns

Any unusual patterns may indicate a heightened security risk.

Any unusual patterns such as changes in visitor traffic, requests for information, employee absences, unusual orders or shipments, strange web activity, and a myriad other items can signal possible changes in the security climate. Be aware of what is normal, be diligent and look for any changes, regardless of how trivial they may seem.

Times of Lower Security Vigilance

When a company 'lets its guard down' it is more likely to be subject to attack.

Some times of lower security vigilance, such as holidays, have already been noted. Others include vacation, when changing security companies, or moving to new facilities. Other instances include times of emergency, such as disasters or fire drills, when some of the usual security rules are ignored in the interest of safety. Company picnics, heavy visitation by clients, prospects or employees from distant offices may also be accompanied by lower security vigilance.

What is Common in Your Industry?

What has been reported in your industry? What have you observed?

Certain industries have periodic cycles. Be aware of what is common in your industry and plan accordingly.

Where

At your most vulnerable spot, of course.

You will most likely be attacked at your point of greatest vulnerability. Seek to understand what an attacker might think and plan accordingly.

How

There are many approaches, but we will cover some of the more common ones here.

To understand the how of organizational threats and vulnerabilities we will return to the actual threats and revisit them in terms of how a terrorist, cybercriminal or hacker might apply their craft. There are as many techniques and methods of operation as there are hackers, terrorists, and criminals. The variations of the criminal mind are an amazing thing to behold. In this section we will attempt to catalog some of the more common methods used to overcome organizational security.

Infrastructure

Infrastructure threats can be as serious as any other kind of security threat.

Threats to infrastructure can cover a wide range, depending upon the specific objectives of the attackers. On the one end of the spectrum is complete destruction of the infrastructure, or access to it, and on the other end are denial of service type attacks or sabotage. In the case of an access road or driveway, for instance, it is possible to completely destroy the road. It is also possible to block a perfectly good road. The effect is the same, but the time and effort, and legal penalties, are vastly different. In fact, the complete demolition of the road could be accomplished using dynamite - a clear criminal act. On the other hand, the road could be blocked effectively with a worker's strike. The results are the same but the strike option is not clearly a criminal act and might have as a side benefit bad press for the target company.

Network and Communication Systems

Because elements of network and communication systems can also have physical manifestations, the first things to consider are the types of damage that can be done to the infrastructure. After that, there are a wide variety of 'how' elements in network and communication systems:

Network and communications systems offer a wide range of vulnerabilities that might be exploited.

- Eavesdropping and compromise/disclosure of information
- Theft and compromise/disclosure of information
- Denial of service / access to voice/data/fax/video services
- Modification of information
- Use of network servers and services for criminal activity
- Launching of network attacks from a target company's systems exposing them to legal liabilities and counter attack.
- Destruction of software and information

It is also a common ploy for a professional hacker to cover their attacks by luring unsuspecting low level hackers know as script kiddies into attacking a target from many angles while the seasoned pro is attempting to breach a target. This is a useful tactic and measurably lowers the likelihood that the professional will be detected and stopped. Increasingly capable hackers are stretching the limits of corporate security to detect and stop them. The list of activities grows with each passing day.

Personnel

Personnel can be subjected to a variety of security situations. Without proper awareness training the outcome can be less than satisfactory. Personnel can be compromised and their unique skills and knowledge stolen through approaches such as kidnapping or threats to themselves or family members. Payments, bribes, attractive job offer, invitations to write articles or present papers at symposia are some other methods used to extract proprietary information from unsuspecting personnel. Two of the most successful tools of the professional hacker are social engineering and reverse social engineering. Social engineering exploits an individual's inherent trust by simply contacting them and getting them to provide information or other assistance. Social engineers convince the target that the target can help - no money exchanges hands. Reverse social engineering is similar, but the target is tricked into calling the hacker or criminal. These are very effective approaches and can be used to circumvent even the most stringent security systems.

Personnel can be subjected to everything from a great job offer to threats to their own safety.

Product / Service / Brand / Reputation

Product tampering, rumors of product tampering, indirect tampering by modifying/sabotaging raw materials, introduction of misinformation on web sites, in fictional press releases and a variety of other amazingly simple and effective approaches can be used to positively and negatively influence the reputation of a product, service or brand.

Fewer threats have a faster or more permanent impact than attacks on brand and product reputation, reliability, safety or quality.

Very simple approaches are possible, such as emailing misinformation in an attempt to get it forwarded so many times that the origin is impossible to trace. Very sophisticated approaches are also possible such a creating fictional press releases, web pages or even entire cloned web sites. Imagine how difficult it would be to deny a rumor or the accuracy of certain information if it is available on your web site, or on a highly regarded site such as Yahoo!, or CNN. It would be almost impossible to refute at that point.

It is, of course, possible to actually tamper with a product, but the criminal penalties are more severe and these cases are easier to prosecute because of the presence of physical evidence. It does not keep actual tampering cases from coming up from time to time, however.

Summary

You should now have a better understanding of the Who, What, Why, When, Where and How of organizational security. What to do next?

At this point you should have a much better understanding of security threats and vulnerabilities and their associated risks and liabilities. The question is "What should I do now?" We will answer this question in the following section.

Conclusion

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

This is not really the end of the story, but rather only a chapter in a much larger story about your organization and network security. 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**.

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 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.

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 were 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 IP networks, emerging technologies, wireless and optical networking to security planning, Intrusion Detection Systems, firewalls, IPSec, PKI, anti-hacking and counter-cyberterrorism. 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.

In order to be truly effective, a security program must be directed and managed from the top. You may be at the helm of the organization, or you may be charged with the task of implementing effective security measures. In either case you are a key figure in this unfolding story. Good luck on your quest.

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

Select Training Offerings of The Consultant Registry

Threats & Vulnerabilities: Security and Your Business™, 1/2 Day Seminar. As a business person you are in an unprecedented situation. Your business is at risk now like it never has been before. And, in addition to that, your business's vulnerabilities might provide the weak link in the national defense that can be exploited by hackers and terrorists. This half day seminar, conducted by internationally recognized security expert James P. Cavanagh, is designed to inform the business person about the risks to their business and allow them to be better prepared and make more informed decisions about their security situation.

C-Level Security Policy Seminars™, 1 Day Organizational Security Policy Workshops. The C-Level Security Policy Seminar is the first day of the two day program described below.

C-Level Security Policy Workshops™, 2 Day Organizational Security Policy Workshops. Every organization needs a written document stating the organization's policy on infrastructure and network security. The document must be written in a comprehensive but understandable manner and must be read, understood and acknowledge - often in writing - by each and every employee and often contractors and sometimes even customers. Many organizations already have such a policy: maybe its time for a review. But, many organizations do not have a policy and the time is now to draft one. A comprehensive, well-written Organizational Security Policy from a reputable, experienced consulting firm could cost a small to medium size organization anywhere from $5,000 to $50,000. By having an outside consultant prepare the document, not only are dollar costs high, the process robs the organization from participating directly in the document's creation, thereby leaving the organization with a document which is not fully customized to their needs. And, if they want to participate more fully, that participation drives the cost up even further. This is where the C-Level Security Policy Workshops™ provide the biggest benefit to attendees: *the attendee leaves the second day of the workshop with a draft Organization Security Policy which they created themselves and which is highly customized to their own needs*.

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 spies or international terrorists, this course has a rich, broad content applicable to a wide variety of security needs.

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