Four Steps to Improved Security

Prevention, Detection, Forensics and Response

A White Paper for Management

The four steps to improved security are prevention, detection, forensics and response. Prevention is 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.

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

February 2002

www.consultant-registry.com

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

Sincere thanks to the author of *Secrets and Lies* and *Applied Cryptography,* inventor of the *Blowfish* and *Twofish* encryption algorithms, CTO and founder of Counterpane Internet Security, Inc., general crypto pundit and occasional crypto curmudgeon Bruce Schneier for his input and recommendations on this white paper.

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

Overview

A Business Motivation for Taking the Four Steps

Security was once considered overhead but savvy organizations are re-evaluating the role of security.

Security was once thought of as a cost - an undesirable overhead item on the corporate balance sheet. Increasingly, however, security is being viewed as an important measure of a current, or prospective, business partner. Often, security is even considered as a positive market differentiator for products and/or services. Savvy managers realize that in order to be good business partners they must not only be secure, they must demand security from their suppliers and customers.

For network security to be effective the interconnected networks of all the participating companies must be secure.

Consider a company who uses the Internet or similar network, such as a Virtual Private Network (VPN), in the course of commerce. It is conceivable that they have a web site and sell products directly to the general public in a b2c, or business-to-consumer, ecommerce model. More likely, however, their ecommerce is strictly b2b, or business-to-business, and they use the Internet or VPN to purchase their raw materials or subassemblies and to sell their product to other businesses. In either case their networked environment is only as secure as the networks of their partners.

A security breach of one interconnected network is, effectively, a breach of all of the interconnected networks.

Company A has a very secure network. Company B security has adequate security. Company A will have to strongly consider the security of Company B's network before making them a full working partner. The sales department of Company B may need to view certain confidential and proprietary product information of Company A across a network directly from their own laptops. If, however, the salespeople of Company B often work at home on non-secure DSL or cable modem connections, Company A cannot reasonably be expected to grant access to Company B. Therefore, Company B can not represent or sell Company A's product as well, thereby making them a less desirable business partner. Confidential information could be provided on paper or CD so that network security issues are alleviated, but paper and CD have a variety of disclosure and disposal concerns of their own. The bottom line is that the difference in security levels makes one partner less desirable and reduces the potential positive impact of working closely together, or possibly, working together at all.

There are three areas of security: network security is only one.

While the first example is a very good example of network security, comprehensive organizational security goes well beyond just the network. The two other areas of security are infrastructure security and homeland security. Infrastructure security covers all things physical and homeland covers our mutual national defense. We will take a look at two other examples that cover these additional important areas.

Infrastructure security protects physical things, like office buildings and manufacturing plants.

As an example of infrastructure security consider two downtown buildings connected by a skywalk. Two companies who are business partners own the two buildings. Each building has its own security system, operated by the company that owns the respective building. To operate together as efficiently as possible there are no security checks on the skywalk connecting the buildings. The mutual security objective is to protect the shared perimeter. In order to accomplish the common objective both individual security systems must be equivalent. If there is a difference in security levels the weaker must be brought up to the level of the stronger, or the owner of the stronger system must insist that a security checkpoint be implemented between the two buildings. While adding a checkpoint is reasonable from a security perspective, it will add additional delay and difficulty in passing between the two buildings, and might cause problems with the relationship between the two companies. At the very least they will not feel as close, nor be as cooperative.

Infrastructure and network security may protect different things,, but the concepts of network security and infrastructure security are the same.

We can see this same issue in many places every day: between supplier and customer, between two divisions of the same organization, and even between countries, such as the US and Canada or Russia and Finland. There are numerous issues, including productivity, flow of goods and services, trust, sovereignty, costs and security. The difference in security levels makes one partner less desirable and reduces the potential positive impact of working closely together.

National homeland security should also be a consideration of any responsible organization

For an example of national homeland security we will look at Company X who delivers packages to Company Z. The trucks and drivers of Company X are routinely waved through the security gate at Company Z. This is due to the inherent trust and historical reputation of Company X. How much risk is Company Z taking by not making Company X a formal part of their security plan? Have they verifieded that drivers from Company X meet their own rigid standards? Why do they trust Company X so much that they do not at least minimally search Company X's trucks for contraband or additional persons? What would be the effect on Company Z and its' trust levels and reputation if it was learned that Company X had a security problem? And, what if Company X's relaxed security gave its driver's access to secured areas of Company Z's plant or products that might be converted to terrorist use? The bottom line is that all parts of a company's environment must undergo a security evaluation.

Take the First Step

There are, of course, more than four steps, but these are the major categories.

Reading this White Paper will prepare you to take the first step. Once you understand the importance of good security take all four steps: prevention, detection, forensics and response.

The Four Steps to Improved Security

We will draw examples from network, infrastructure and national/homeland security.

After an explanation of why we call the process "The Four Steps to *Improved* Security" we will describe the four steps and why they are important in an overall organizational security program. Examples will be drawn predominantly from network and infrastructure security, as these are the most immediately important to business. Ramifications of any security program in national/homeland security terms should, however, always be considered.

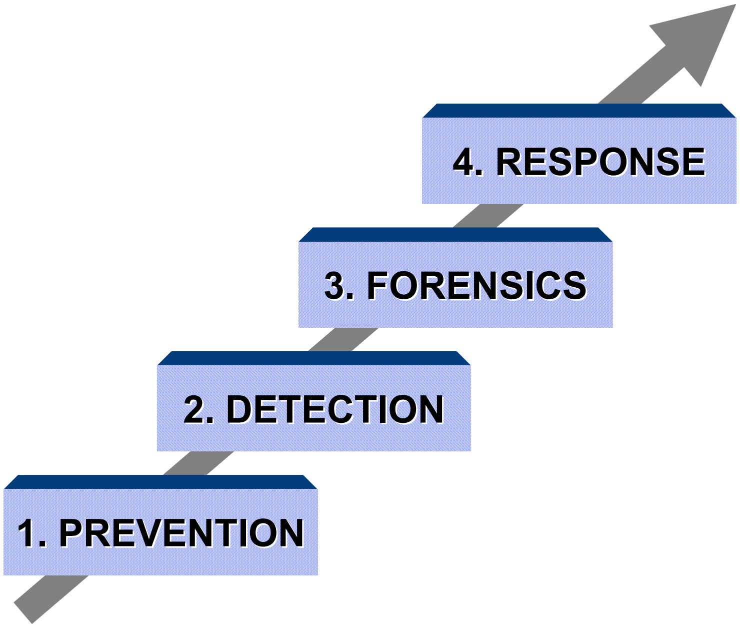

Figure 1
The Four Steps to Improved Security

Improved Security?

Every organization has some security in place. This will be used as the basis for improved security.

In considering the specific approach to organizational security outlined here it is important to consider existing security. The question is not whether "a security system or program is presently in place?", but, "what is the state of the present security program?". There is always an existing system, regardless of how poor or inadequate. A thorough evaluation of the present security program as outlined in The Consultant Registry's Security White Paper *"Security Vulnerability Audit: Assessing Your Organization's Security"*[1] should not be neglected. After such an assessment the focus can be on improving the existing system.

[1] Available from The Consultant Registry at www.consultant-registry.com.

Step One: Prevention

Step One in this four step program is prevention. The objective is to avoid becoming the target of an assault. One very common historical approach to security is called "security by obscurity" and is based upon effectively camouflaging one's identity and presence. Many examples of this approach may be observed if one knows where to look. There is no better example than the windowless concrete telephone company service buildings with a high chain link fence and no sign to identify either their owner or purpose. These buildings are unobtrusive, fit right into most surroundings and draw no special attention to themselves, yet are the nerve center of the neighborhood telephone service. While they can be identified by experts with specialized training (including disgruntled current or former employees, terrorists and others) they are obscure and do not draw undue attention to themselves. They are also not likely to draw opportunistic or ad hoc attacks as neither their purpose nor owner are immediately obvious. Security by obscurity rarely works these days due to a combination of hacker and criminal tools which can readily identify network and physical resources as well as a company's desire to advertise certain things that might become targets, such as web sites and physical office or store locations.

"Security by obscurity" is rarely an effective strategy any more.

If completely hiding resources from would-be attackers is not an alternative, how does an organization prevent attacks? Several possible strategies, depending upon your organizational philosophy, are:

How does an organization prevent attacks?

- Keep a Low Profile
- Stealth Techniques
- Strong Defensive Measures
- Security Discipline and Vigilance

We will discuss each of these possibilities in more depth in the following sections.

Keep a Low Profile

Organizations should determine which areas need a high profile and which need a low profile..

Keeping a low profile might seem inconsistent with sales, marketing and advertising, but the real point is to focus advertising in such a way as to not attract undue or unwanted attention to yourself or your organization.

Keeping a low profile does not run counter to the objectives of marketing and advertising.

For example, you have just come from a trade show where your company has spent millions of dollars advertising to your industry and your company logo is pasted everywhere. Even so, you should not bring undue attention to yourself by displaying a company logo name tag or computer bag at the airport. The attention you will attract at the airport is uncalled for and could put you and your company in jeopardy. It is much more advisable to be 'generic' and disappear anonymously into the crowd. And remember to take off that name badge!

Another example of keeping a low profile in the networking area is the way in which you advertise yourself on the network. Standards require that network servers, the computers that provide information such as web pages or services such as email, identify themselves with a special message often called a banner. A banner basically says "I am version XYZ of this service." Hackers often use this information to determine what vulnerability a system may have, or who has the newest, latest and greatest version of a system so they can try and ascertain how it may be vulnerable. In order to keep a low profile it is possible to program the banner to indicate that you have an earlier version of software, or even the totally confounding version 0.0! This misinformation may keep your network secure from attack due to the extra work required by the hackers to learn the correct information. That is, of course, unless you are the subject of a targeted attack, in which case the attackers are likely to spend whatever resources they need to learn exactly how to attack you.

Keep a low profile by denying attackers of information they need or by making them work harder to get that information.

Stealth Techniques

Stealth techniques are akin to the "security by obscurity" discussed earlier. Stealth techniques can range from not answering telephones with a company's name to using special codes in place of names in emails. The benefits of security must be weighed against issues of ease of use and convenience, however. For very large organizations with a strong need for a public presence stealth techniques may be appropriate, and even mandatory for certain divisions of the company, such as research and development, the security group or certain support areas whose visibility must stay below the radar of potential attackers.

Stealth techniques allow you to hide within the system.

One example of keeping a low profile is to not write your company name, or use obscure initials, when signing in as a visitor at another company. An equivalent stealth technique is to use the name of a completely different, or non-existent company as well as using a fictitious name and/or unreadable signature.

Provide as little information as possible, or misinformation. Don't leave an information trail.

In the network area we already discussed using incorrect or misleading banner messages advertising your servers on the network. In the stealth area an organization can consider not responding to certain network messages. One common message type, PING, for instance, is often exploited by hackers. According to the standards network devices must always respond to a PING message. This is exploited by an attacker sending ping after ping after ping faster than they can be responded to, effectively tying up the resource being PINGed and making in unusable for other purposes. This is called a 'denial of service' attack. It is possible to operate in stealth mode and not even respond to the PING messages at all. Of course, this deprives your system of the diagnostic benefits of PING, but it also deprives potential attackers of a very useful

Reconsider all of the ways in which your organization interacts with the "outside" world.

vulnerability to exploit.

Strong Defensive Measures

The best defense is a good offense.

It has often been said that the best defense is a good offense. This has never been more true than in the areas of infrastructure and network security. Many attacks are those of convenience: during a routine scan a hacker or criminal organization has caught you or your organization in their crosshairs. They have accidentally found some damaging or otherwise potentially exploitable piece of information that they now wish to exploit. Strong defensive measures will reduce or eliminate the accidental leaking of information from the organization.

Security Discipline and Vigilance

Security discipline and vigilance is a people issue.

Security discipline and vigilance is a people issue. Individuals within all levels of the organization must be aware of the environment around them and must be provided with incentives and methodology to report any apparent inconsistencies between what they observe and the established security policy of the organization.

Initial and ongoing training is the key.

Security discipline and vigilance require a combination of good initial new hire training, ongoing training and awareness programs and reward and/or recognition programs. It must be made clear, and also be true, that security is the highest priority of the organization.

Step Two: Detection

Detection involves monitoring at access points and activity inside a building or computer network or system.

Security experts generally agree that the majority of security breaches go completely undetected. One reason for the lack of detection is that a majority, perhaps as high as 70% or more, of security breaches are either insider jobs, or have insider assistance. Very few modern security systems can detect or report violations once the security perimeter has been breached, but they need to.

Many systems are in place but are not used effectively.

For example, many organizations have ID badge systems that will allow or block employee and contractor access to specific buildings. In many cases there are additional security levels such as restricted access of escort requirements. Rarely, if ever, are the internal controls obeyed. To better understand the problems with the escort required restrictions, please see the security discipline and vigilance section above. Otherwise consider that internal checks are complex and expensive and historically have not been seen as important to the operation of the business. That is changing as executive awareness of security issues and the impact on the business bottom line is increasing.

Detection of a violation involves comparing what is being attempted to the policy of acceptable activities.

Detection begins with the organizational security policy. It can be achieved by comparing what is observed to what has been stated in company policy as acceptable. If the organizational security policy states one thing and something different is observed, then some sort of action, or reaction, must be mounted to determine if a violation has occurred.

Let's make the point more understandable with some examples. Consider this policy statement: "all student pilots must learn to take off, fly and land". This is a very good example for several reasons. The first reason is that without the hindsight of the events of September 11th the statement would have seemed too trivial to include in a policy. Another reason this is a good policy statement is it is without exception and is very clear. What is lacking, however, is how compliance will be measured, when, and by whom. This is where management must make some decisions. For the sake of brevity let's say that the complete statement is "all student pilots must learn to take off, fly and land, and that 33.3% of simulator time must be spent on each area, unless otherwise approved by the flight instructor." We now have a way of detecting if there is a discrepancy between policy and practice. A weekly management report can be generated showing distribution of flight simulator hours and any discrepancy can be further investigated. Room must also be made for exceptions, such as a student pilot whose simulator hours are spread across three weeks: week one concentrating solely on taking-off, week two on flying and week three on landing.

Some things seem too basic to include in a specific policy. Not so.

One could argue that there are several ways for a potential terrorist pilot to get around this policy. This policy statement must be only one of a series of related policy statements which, taken together, will detect security violations and trigger further investigation. It is also worth noting that keeping the policy secret, so that a terrorist will not know the detection triggers, combined with periodic updates to the policy is an important part of any effective security program.

Part of an effective policy is to keep certain aspects of the policy secret.

Let's look at another example. Suppose the policy states, as it does in many organizations, that an employee or contractor must not leave their computer terminal/PC logged in when they leave their work area. Violations could be detected by correlating the logged on/logged off status of an individual with their movement through a facility. For instance if they swipe their badge to exit the building and their PC is still logged in they could be detained by the guards and made to go back and log off before they leave. Another, possibly more effective, system would be to log off their device automatically and disable further log-ins until they had reentered the building/work area. This would stop a variety of problems as well as provide an excellent detection mechanism by correlating a number of events.

A silent, automated approach to security is often better than sirens and dogs barking, dependant upon the specific objectives.

One last infrastructure example: the policy statement says that all vehicles parking on company property must have a permanently attached or one-day parking permit issued by corporate security. All parking permits are registered and serial numbered. If a vehicle is discovered either without the appropriate permit, or with a forged, counterfeited or otherwise invalid permit, such as a temporary one day permit, but for

Security systems can be designed to make violations easy to catch.

another date, then some sort of appropriate response may be initiated.

Step Three: Forensics

Management thinking is changing regarding security. The savvy manager understands the importance of good security.

One of the subtle themes of this white paper is the change in management thinking regarding security. We have already established that savvy managers are beginning to realize that good security is not only important to their own success as an island in the business ocean, but also critical to their interconnected partners, suppliers and clients. We have already established that these same savvy managers are beginning to understand the roles played by network, infrastructure and homeland/national security. We have further stated the importance of a clear organizational security policy in detecting violations and causing further investigation. We will now identify one more sea change in the management's security awareness: forensics.

Forensics is done 'after the fact' but can be assisted by information collected earlier.

Forensics has always been thought of as the collection of information that remains at a physical or digital crime scene *after the fact*. And while this is a true statement, it does not mean that nothing can be done before the fact - quite the contrary. An organization can put many systems in place before the crime is committed which aid forensics later.

Every security decision is full of opportunities to aid forensics.

Consider the simple example of building access. During the process of policy development management engages in a dialog regarding the precise building access policy. After finalizing the language regarding access via guarded doors, such as guard booths and reception areas, attention then focuses on the unguarded doors. They decide that the objective is to have employees, contractors and guests use only guarded doors and that a human must verify identity and make the actual decision regarding access. A proposal is made to permanently brick-up all secondary access doors to avoid their use and force compliance with the policy. It is pointed out that this is not possible because fire regulations require the secondary doors for evacuation purposes and permanently closing them could cause dangerous human traffic jams at the main, guarded, entrances in case of emergency evacuation.

Even the consideration of access cameras can improve forensic.

A proposal is made to keep the secondary doors open, but only for exiting the building. A counter proposal is made to equip all doors with card-key access so that any door may be used for entry or exit, and that a permanent record may be kept of all entries and exits. Only persons without a current, active key-card must use the primary guarded entrances. The next question is about monitoring and detection of policy violations. The system of allowing entrances and exits through unguarded doors leaves open the possibility that more than one person may enter or exit at a time. Someone suggests the use of turnstiles that allow only one person to exit or enter per card swipe. Good idea, but this is against fire codes in many of the jurisdictions in which they operate. Next someone introduces the idea of using cameras to monitor the secondary doors for compliance with the policy.

Cameras will provide efficient, low cost monitoring and are easily obtained from a variety of sources, including the present alarm monitoring company, and may be installed at a reasonably low cost,. Management agrees that cameras should be investigated further. The next question is "should the cameras be hidden or obvious?" Management decides that an obvious camera will deter employees and others from breaking the policy and this is good because it is consistent with the first of the four steps: prevention. The next question is, "shall cameras monitor constantly or should they monitor only periodically, and if periodically, how often?" Management decides that cameras will be actuated automatically by motion sensors. This will allow collection of meaningful images and automatic elimination of unneeded video images. The next question: "shall we use sequential video tapes or digital media?" Digital media is chosen because the video images are indexed by time and location and may be retrieved far more easily, *thereby facilitating forensics*. Digital pictures may be retrieved based upon the card key access log, enhanced, printed, archived and otherwise managed the same way any other digital file can be managed. In this case management is making decisions before the fact that will be important for forensics after the fact.

The speed with which a forensics investigation occurs can often reduce or eliminate further damage- the faster the better.

At this point someone asks what the policy is once a violation is detected, reported and had a thorough forensics evaluation. If job termination or criminal prosecution is the objective there are a number of other checks and balances the organization must put into place. For instance, it must be proven that the video evidence has not been tampered with and a chain of possession of the evidence must also be established so that the digital information collected follows the evidentiary rules of the jurisdiction in which any case will be tried. Management decides to hire an expert in forensics to further assure the integrity of digital evidence.

The objective of a security response has a big impact on the type and quality of forensic information which is collected and the proper handling of the forensic information if it is to be used as evidence.

While the decision to put up cameras or not put up cameras, as an example, may seem a simple one, there are many more facets of the decision to consider which will enhance collection of forensic information after a policy violation has been detected. There are similar considerations of all aspects of infrastructure, network and homeland/ national security. How information is collected by network firewalls, Intrusion Detection Systems (IDSs), access logging and similar systems is key to the use of the information for forensics purposes.

Much information is presently gathered that can be put to good forensic use. Its value can be dramatically enhanced with certain changes to the handling procedures and correlation of information.

At this point we have determined that the best possible approach is to prevent any security incursions in the first place. If we do have some incursions, we must be able to react to them and to collect information that will allow us to answer as many of the important questions as possible, and to meet our policy objectives in terms of the response. That response is the next and final step that we will consider.

Prevention is good, but if we are attacked we can detect the intrusion and gather evidence to help in the response phase.

Step Four: Response

After clearly establishing the source of a policy violation the organization may respond in one or more of the following ways:

A carefully considered and measured response is the final of the four steps.

- Do nothing
- Close the vulnerability exploited in the attack
- Take disciplinary or legal action
- Respond (Hack-back)

Organizations will respond in a variety of offensive and defensive ways, depending upon their own objectives.

The actual methodology chosen may vary by severity of violation or identity of the attacker, but the organization should discuss and clearly understand the full ramifications of any response. Filing a police report and prosecuting, for instance, might require public disclosure of information the organization would rather not have revealed. Hack-back attacks on perpetrators might trigger even more severe reactions and escalate problems. Not cooperating with law enforcement or other system administrators might increase legal liabilities and possible penalties. These areas and more should all be considered when evaluating possible responses.

The Four Steps: A Review

Let's review the four steps: Prevention, Detection, Forensics and Response.

Let's briefly review the four steps: Prevention, Detection, Forensics and Response:

	Description
1	**Prevention** To avoid a security problem in the first place by removing possible vulnerabilities and reducing resource visibility.
2	**Detection** Comparing what has been deemed acceptable by an organization's policy guidelines with what is actually observed, and executing a notification process so that security personnel realize the inconsistency exists.
3	**Forensics** Gathering information after a security violation has been detected to form the basis for a response.
4	**Response** Responding to a detected security breach in a manner which is consistent with the organizational guidelines.

Table 1
Four Steps to Improved Security

How can the four steps be implemented cost effectively?.

Now that we thoroughly understand the four steps we will take a look at cost effectively implementing the four steps in a business environment.

The Four Steps on a Budget

Budgetary Considerations

While excellent, world class, leading edge, state-of-the-art security can be very expensive simply improving existing security to reasonable levels can often be done cost effectively.

While it is possible to spend millions of dollars on systems and services to meet the needs outlined in this white paper, achieving a large measure of the benefits from the improvements need not be extremely expensive. Realizing the benefits of the improvements may be more a function of reevaluating how your present security is conducted and making changes in policy and procedures. This can be coupled with a change of awareness of the individuals within your organization and their interaction with your existing or newly updated security policy and systems.

Cost Effective Prevention

Attack prevention can be done by your existing team. Take on the role of the outsider and consider how you would use available information to attack yourself.

Prevention begins with a review of your organization, *from an outsider's perspective*. Become the outsider and ask; "are your signs at the trade show displayed prominently for all (within your trade group) to see? Good. But what about the truck that delivered those signs to the show? And what about the company logo golf shirts your employees will wear to dinner tonight, after the show? And what about the new company logo computer bags that will be sported by your employees and clients at the airport? Maybe not so good. The evaluation of preventative steps can be largely done by you and your staff on the first pass. After you've given prevention your best effort bring in outside help, and get another set of eyes to look at the problem.

Cost Effective Detection

The signs of attack may already be there if you simply train your personnel to read them.

Detection can be an expensive proposition. Hiring a managed security monitoring (MSM) service firm, installing sophisticated Intrusion Detection Systems (IDSs), purchasing and implementing biometric retina scan technology at all access doors and similar steps can quickly crush a security budget. The first step, however, before trying to solve the problem by throwing money at it, is to determine what you have in place already and how it might be improved or leveraged. As an example, when a visitor, or an employee who has lost or forgotten their name badge, passes the guard point do they have to sign in? If so, does the guard verify the information against a piece of other ID, such as a driver's license? Is the sign-in in a paper logbook? Maybe the process could be improved by entering the information immediately into a computer log file that could later be searched more easily. Or maybe a small, personal copier could be used to capture an image of the front and back sides of the identification presented, an inexpensive step which could greatly enhance forensics later on. The solutions can be expensive, but don't necessarily need to be.

Cost Effective Forensics

Forensic information can be routinely gathered and analyzed as a part of detection. This, too, is an area that can be needlessly expensive.

Forensic scientists are used to working with such randomly generated and obscure clues that any additional information that may be used to corroborate their other findings can be very helpful. Simply moving from a VCR system requiring viewing of all footage to a digital image system which can be searched by date, time, employee ID number or other indices can be very helpful. The addition of badge readers to track movement of employees and visitors inside a facility by date and time can be of immense help and a software system, however crude, which can correlate physical movement with computer or network transactions is of extreme value.

Cost Effective Response

How elaborate or expensive the response to an intrusion or attack is can be determined by each organization, but it does not need to be expensive or elaborate Beyond closing the vulnerabilities, what does the organization want or need?.

Response can be costly if you hire or outsource response services. There are, no doubt, existing personnel who are responsible for security response or who can have such actions added to their responsibilities. One of the keys to using existing or modest additional resources for response is to have a system that automatically eliminates false alarms so that the responder is reacting to real alarms in as many cases as possible. In many instances this is a sufficient business cost justification for Managed Security Monitoring (MSM) firms who will filter alarms before contacting your personnel.

The Business Case for Good Security

Savvy managers are increasingly understanding the business case for good security.

Security is beginning to pass the tests of other areas of business operations. We are beginning to see the Return On Investment. Security of a product or service is being seen as a positive differentiator in the marketplace, and often the 'tie breaker' for product or service selection when other factors appear equal. Savvy business people are also beginning to understand their role in the security of their supply chain and network with their clients. The security of the group is impacted by the security of each individual. Each organization is a link in the security chain and any weakness can be exploited to gain access and do damage to other organizations in the group.

The Four Steps and Your Business

Do the four steps apply to your organization? They probably do. If not, why not?

With the foregoing discussion in mind, this is a good time to take a few moments to consider the specific needs of your organization. Do the four steps apply to your organization? Is the information you've read in this white paper actionable? What will be your next step, and when will you make it?

Conclusion

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

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

Threats & Vulnerabilities: Security and Your Business

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

Recent surveys have proven three facts:

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

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

Network Security: The Business Value Proposition

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

Network security is an important part of any business. All too often network security is driven by the operations and technology people, not by the business needs. Network security can, and should, be put to the same tests for cost effectiveness and return on investment 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.

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

Begin, or continue, your organizational security mission keeping the four steps, and the business benefits, of security in mind.

This white paper has identified the four major steps to improved security. Your mission is to consider these steps, modify them as needed, and to begin, or continue, the process of enhancing your own security and that of your business partners. As you make and execute your plans remember that enhanced security insulates your business from many of the worst threats and vulnerabilities facing organizations today as well as making you a more attractive, effective business partner, supplier or customer. We urge you on in your mission and wish you the best success.

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. In the fall of 2001 he 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 C-Level Security Policy Workshops

C-Level 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 acknowledged - in writing - by each and every employee and often contractors and 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. The goal of the C-Level Security Policy Workshops is for the attendee to leave with a completed document.

Audience:

This workshop is designed specifically for senior management at the "C" Level: Chief Executive Officers (CEO), Chief Technology Officers (CTO), Chief Information Officers (CIO), Chief Financial Officers (CFO), and Chief Security Officers (CSO), Vice President of Human Resources (VP-HR) or any other management responsible for providing guidance and leadership to a company on their infrastructure and network security issues.

Prerequisites:

There are no prerequisites for this workshop.

Workshop Description:

Most organizations do not clearly understand the risks and liabilities of bad or incomplete network and/or infrastructure security. In many cases organizations hit by a "hack attack" are operationally crippled, experience direct loss such as loss of business or costs due to damage while many are impacted, often to a bigger extent, by indirect losses such as loss of customer confidence or loss of share value and subsequent loss of shareholder and market trust.

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.

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