

RGTS

Rockefeller Group Technology Solutions™



**Information Security in
Today's Business World**



**YOUR PROVEN PARTNER IN
COMMUNICATIONS SOLUTIONS™**

Overview	1
What Is the Field of Information Security?	2
The Business Impact of Security Issues	4
The Cornerstone of Information Security – The Security Policy	5
Components of a Security Policy	5
Purpose	5
Roles and Responsibilities	5
Enforcement	5
Physical Security	5
Access Controls	6
Technology	6
Communications Mechanisms	6
Data Security and Retention	7
Legal Considerations	7
Importance of a Security Policy	7
Information Security Technologies	7
Technology Overview	8
Perimeter Protection	9
Firewalls	9
Intrusion Detection Systems	12
Secure Communications	12
Virtual Private Networks (VPNs)	12
Secure Remote Access	13
Encryption Systems	13
Public Key Infrastructure (PKI)	13
Auditing and Monitoring	14
Scanning Tools	14
Logging and Log Analysis	14
Alert Reporting Systems	15
Host Security Tools	15
Virus Protection	15
Access and Authentication Mechanisms	15
Simple Password Systems	15
Directory Services	16
Smart Card Technologies	17
TACACS, TACACS+, RADIUS	17
Messaging Services	17
Unsolicited E-mail	17
Information Security Technologies – A Practical Example	20

In today's world we are bombarded from all angles with stories of increased security precautions, high-visibility security breaches, identity theft, corporate sabotage, and all sorts of other disturbing and distracting security bulletins.

So what does it all mean to today's businesses? Many large-scale organizations have entire departments devoted to security and risk management, but for the rest of the business world a comprehensive Information Security strategy has not been something that fit in as a high priority. Until now.

In today's world, taking precautions to protect your business is not just important, it is imperative.

The focus of this paper is to discuss Information Security as it relates to a large part of the business world, the companies that don't maintain full-time security groups. The goal here is to explain the different aspects of Information Security and outline some of the basic starting points for building an effective security strategy.

Many industry groups have identified Information Security as a hot item for the upcoming year. Why now?

For most businesses in the post-September 11th world, 2002 was spent reviewing and updating their Disaster Recovery policies and procedures. A key component of a DR review is assessing the risks to the operation of the business. A DR strategy develops contingency plans in case of an incident. The next logical step is to develop a strategy to avoid incidents. This leads us into the heavily interrelated areas of Information Security and Risk Management.

Let's begin by defining the field of Information Security.

We will build a definition from the inside out. One of the most fundamental aspects of Information Security, and the most often overlooked, is internal security. How do we protect our organization from risks inside our own walls? This doesn't always imply malicious or mischievous intent, because in many cases we simply need to ensure that we've built safeguards to protect us from ourselves.

Looking at how most businesses work, the next step to address is how we communicate with the outside world. Remote offices, partners, vendors, clients, suppliers, potential clients, competitors, and so on all create different types of communication that require different mediums and levels of security.

Conversely, we then have to look at how others communicate with us. The method we choose to communicate with a vendor may differ in its medium and security level from a method we want others to use when communicating with us.

Next we need to look at our perimeter. How are the "walls" of our business protected? This is where we look at deflecting mischievous hackers, viruses, service interruptions, sabotage, and all the other perils that abound in today's electronic world.

Now that we have secured the access to our data, we must look at the data itself. Our definition of Information Security must include the steps we take to ensure that the data we have in our systems, on

backup tapes, in storage facilities, and in people's positions is secure. Many businesses have implemented all the security mechanisms available to protect their perimeter and communications, only to have to scramble to recover from data contained on a stolen laptop.

Our definition is still not complete. We have put protection mechanisms into our definition, but another important aspect of Information Security is knowing who did what and when. Maintaining an audit trail of logs, communications records, security systems, and system changes is critical to having an effective security strategy. In many industries it is now required by regulatory agencies that security and communication records be maintained for long periods of time, sometimes years.

Another component of our definition of Information Security is less tangible but far the most important to today's businesses. It is actively managing risks. The implementation of an effective Information Security strategy follows the axiom – a chain is only as strong as its weakest link. In our case, this means that we must constantly be reviewing and updating our security practices to ensure that they are dynamic and change with our business.

Active risk management is an important aspect of any Information Security practice. It is very easy to say we must implement every security protection technique known to man, but when you look at the dollars and cents of it, we quickly get into discussing acceptable risk.

WHAT IS THE FIELD OF INFORMATION SECURITY?

The last part of our definition is one that has been around in business for a long time but has come more to the forefront in today's "connected" workplace. That is the legal aspect of Information Security. There are legal considerations across all areas of our security strategy. Managing risk from a legal point of view, ensuring that possibly questionable content is kept out of the workplace, privacy issues, copyright and licensing compliance, and policy enforcement are all critical elements in implementing an effective Information Security strategy. HIPAA (Health Insurance Portability and Accountability Act) is a good example of this in practice. This recent government regulation requires Information Security compliance with how individual health-care records must be treated.

So let's look at the definition of Information Security that we have built so far. It includes:

- Protection from internal risks
- Protection from external threats
- Secure communications
- Safeguarded information
- Maintenance of an audit trail
- Management of risk
- Addressing of legal ramifications

Now that we have defined what Information Security is, what does it mean to our businesses?

To draw a parallel in simple terms, let's think of the safeguards we have in place with our cars. We have locks on our doors, a spare tire in the trunk, an alarm system, an ignition key, seatbelts, airbags, bumpers, turn signals, and even something as simple as windows that roll up from the inside. All these are mechanisms we use to protect the security of our cars. Some devices protect the car itself, some protect us as the driver, and some protect the others out there on the road. Each serves a different function and offers its own options and mechanisms for implementation.

In terms of our businesses, we need to review each function and determine what level and what method we want to use to meet our business needs.

In our example and in the world of Information Security, the final checkpoint of the effectiveness of our strategy is legal review. If something happens as a result of which we have to go to our insurance provider, financiers, partners, or a client, the question that is going to be asked is, "Did we take all reasonable measures to ensure the safety, security, and integrity of our resources?"

Our Information Security strategy boils down to a business decision regarding acceptable risk: What is the amount of money we can justify spending versus the risks we are willing to accept? This is where the idea of active risk management becomes very important to today's business. As businesses and technologies rapidly change, what is acceptable today may be entirely unacceptable tomorrow. If we are managing our risks carefully by reviewing our security practices regularly we will be able to adapt our strategies to meet the challenges of ever-increasingly difficult times.

The business decision-making process is based on a combination of industry best practices that serve as baseline security functions, industry-specific regulations such as HIPAA or regulatory guidelines, legal strictures, and technology considerations for the specific systems and services that your business uses.

The common perception of Information Security as a purely technology field meant to keep hackers out of our networks is not entirely correct. From a business point of view, Information Security is more accurately defined as a risk management function. Incidents will happen; it is the job of the effective security strategy to provide the foundation and guidelines to keep a minor incident from becoming a major catastrophe.

THE CORNERSTONE OF INFORMATION SECURITY – THE SECURITY POLICY

The pen being mightier than the sword, there is no area where this holds true more than in the world of Information Security. In building our definition of what Information Security is, we identified a wide set of criteria involved in building a security strategy. The most effective security plan is rendered immediately useless, however, by the employee who doesn't know about it.

The cardinal rule in the field of Information Security can be summarized in three words: WRITE IT DOWN!!!

The secret to deploying an effective security strategy is ensuring that everyone in your organization knows that it exists, what it means, and how it is enforced. Effectively communicating your security policy to your team is the first and most important step in making security an integral part of the culture of your business. To borrow another old axiom, when it comes to security a stitch in time saves nine.

Also, when it comes to enforcement and legal considerations, if a policy has not been clearly communicated, it becomes extremely difficult to enforce.

Components of a Security Policy

In many large organizations, you will find entire departments dedicated to the development and enforcement of security policies. In an organization where there are no dedicated security resources, having a binder of security policies the size of a phone book may not make sense. Let's look at some of the common components of a security policy and how businesses can build a manageable security plan.

Purpose

The first thing that must be communicated to your team is why the policy is important. The importance of the security policy to the business must be stressed. The overall integrity of the security strategy will come down to the diligence and practices of each individual in the organization.

Roles and Responsibilities

Clearly defining who is responsible for each component in a security policy will ensure that the policy and how it is carried out are integrated into the organization. The whole organization must know who to contact with questions, how to address potential issues, and where to go for help.

The policy should define who is the corporate security officer, security technical contact, backup contacts, the hierarchy of escalation points, and the like.

Enforcement

How a policy is to be enforced is a key component of the policy. Individuals must know what their specific responsibilities are under the policy and be aware of the ramifications of noncompliance. Each person involved must review and acknowledge receipt of the policy.

Physical Security

How a business's locations, offices, computer rooms, files, communication equipment, and other physical resources are secured is a matter of physical security. Procedures for updating locks, codes, and such are also involved here.

In a basic policy we simply state that all company resources must be in a locked space, with keys kept by the office manager, who maintains a logbook of who comes and goes.

Access Controls

The access controls section of a security policy defines who and how people are to gain access to your facilities, systems, files, and communications. It also defines what and how information is logged regarding access to your company's resources.

Things like building passes, security cards, and entry and exit logs are some of the simpler aspects of access controls. On the technology side, password policies, access methods and restrictions, and who can access what are all important aspects of a security policy that should be clearly documented. Even a simple thing like requiring users to change their passwords on a regular basis can avoid major exposures.

Technology

The technology section of your security policy will vary widely, depending on your business. The basic idea of the technology section is to look at and address the risks associated with the technology you use to run your business. Some areas usually covered in a technology security policy are

- **Policies for accessing the network and installing new equipment**
- **Standard equipment configurations (passwords, access restrictions, etc.)**
- **Acceptable Use Policies**
 - Internet usage policies
 - E-mail and instant messaging policies

- Use of company resources (phone, fax, etc.)

- **Perimeter Protection Policies**

- Firewalling requirements
- What is permitted and restricted from the network
- Phone and fax fraud protection

- **Change Control Requirements**

- **Logging Mechanisms and Retention**

- **Approved Secure Communications Technologies**

- Encryption Standards
- Remote Access and VPN (Virtual Private Network) Standards

Technology policies can become very involved as your business relies more and more on technology. A general guideline to follow is that if you need it to do business, you need to develop a security policy to ensure the safety, security, and stability of that item as a business tool.

Communications Mechanisms

Many companies will create a separate section to document the approved methods for holding secure communications.

Connecting remote locations, providing access to remote or traveling employees, communicating with vendors, and communicating with current and prospective clients are all areas that must be defined in a security policy.

By defining the methods to use to communicate securely you establish a baseline standard that can be incorporated in all your new business ventures.

Data Security and Retention

You maintain a tremendous amount of data about your company, your clients, your partners and vendors, and everyone else you deal with. What are you doing to protect this data? In today's world, where business and personal information is being sold to third parties at an alarming rate, defining what you will do with data you collect and how you will keep it can go a long way toward maintaining strong relationships with your partners, vendors, and clients.

You may also choose to document what information you will provide to others. If it is clear in your security policy what can and cannot be shared with others, the risks associated with having sensitive information end up in the wrong place can be minimized.

Legal Considerations

What much of an effective Information Security policy boils down to is building a legal document that we can manage our business from. In it we are setting out the policies and procedures for our organization to follow and the methods we will use to enforce them. This means we must include a legal section in our policy document. It should delineate what methods we will use to enforce our policy, how infractions will be dealt with, and what the ramifications for noncompliance are to be.

In today's electronic age, cooperation and coordination with law enforcement agencies is an everyday reality for many businesses. Once an incident happens, if

the proper procedures are not followed, the law enforcement agencies will not be able to provide much assistance in finding the culprit.

Importance of a Security Policy

While these examples are some of the fundamental areas that go into a security policy, this is by no means a complete list. Security policies vary from industry to industry and business to business. Best practices provide guidelines, but ultimately a security policy document is the record for your business of where and how you are managing risk.

There are many resources available for businesses looking to develop a security policy. Experience counts, and in many cases an experienced security consultant can put together a basic policy document in a very short time.

The key to a security policy's being effective is a two-step process: update, and communicate. The policy must first be a living document that evolves with your business. Then a message of security and company policies must be communicated clearly to your team on a regular basis.

A security policy will serve as a roadmap for developing your business with security in mind. It will serve as a guide for your organization to ensure an organized, common security strategy and provide a mechanism for minimizing and managing security-related risks.

Before getting into the specifics of each technology area, it is important to discuss their use as part of a greater security strategy. Technology provides tools for supporting a security policy. Implementing technology for technology's sake does not make much business sense. By defining in our security policy first what we are trying to protect, we can be much more effective in selecting the right technology for the job, at the right cost.

A great historical example of making the mistake of building technology for technology's sake can be seen in the Maginot Line of World War II. The Maginot Line was a huge and costly defense system set up by post-World War I France to defend their eastern border, which had potential invasion routes from Germany.

The Maginot Line was essentially a giant wall that stretched along almost four hundred miles of France's eastern border. It was extensive, modern, well-equipped, and considered by most to be impenetrable. But, in 1940 the German army found a very effective way to exploit a weakness in the Line – they simply found the end of the Line and went around it!

A Maginot mentality often exists in today's IT community when a new technology is built as a silver bullet to meet all our security needs. Without having a comprehensive policy in place we are simply placing rocks in the path of a river instead of building a solid dam. In building our technology plan, we have to ensure that we are using technology to support and reinforce our plan, not putting it in place of an overall plan.

As in all other industries, technologies in the security field are being developed at a breakneck pace. Information Security technology is one of the few areas in today's economy where investment dollars are still plentiful. As a result, with all the development out there, the product and technology landscape can at times be pretty confusing.

Technology Overview

For the sake of this discussion, we will break down the areas of security-related technologies into six basic categories:

- **Perimeter Protection**
 - Firewalls
 - Intrusion Detection Systems (IDSs)
- **Secure Communications**
 - Virtual Private Networks (VPNs)
 - Secure Remote Access
 - Encryption and Public Key Infrastructure (PKI)
- **Auditing and Monitoring**
 - Scanning Tools
 - Logging and Log Analysis
 - Alert Reporting Systems
- **Host Security Tools**
- **Access and Authentication Mechanisms**
- **Messaging Tools**

There are many vendors in today's market delivering hybrid systems that group several of these functions in a single solution. The security "appliance" approach has become a popular method of providing clients simple "black box" solutions to meet many of their security technology needs.

Since we are looking at the fundamental aspects of Information Security, we will focus on the functions of each area, with the understanding that many vendor implementations may contain varying degrees of multiple functions in a single product.

Perimeter Protection

Firewalls

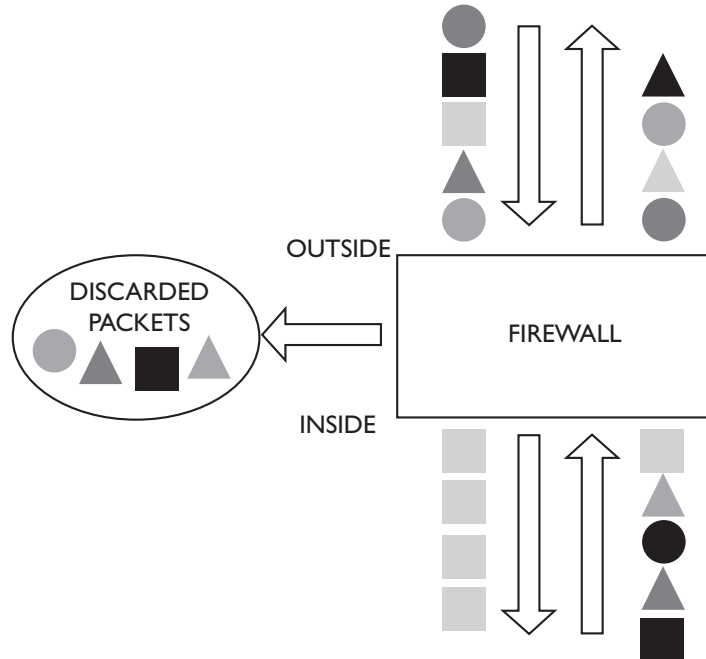
Firewalls are one of the most fundamental security technologies in use. Firewalls have been around for longer than they have been called by that name. Basically, a firewall is a computer system with two or more network interfaces and some software. Early firewalls were simply IP routers or UNIX systems with firewall functions built into the software.

The software allows the administrator to create lists of rules to apply to data packets as they pass through the firewall. The different rule sets work on a simple permit-or-deny scheme. Different levels of granularity can be obtained in different products, but all firewalls work on the same principle.

An example of a simplified firewall and its associated rule set is illustrated on page 10. There we have set up a firewall to manage the flow of circles, squares, and triangles into our site. The firewall has an inside and an outside interface and will apply the rules in numerical order.

In this example we have created several rules to manage the traffic to and from our network. One is that we only want to allow squares into our network. And we want to be able to send triangles and circles from our network. We have also achieved an additional level of granularity by filtering the shapes by color. Finally, we have narrowed the criteria for what we will allow in, to include only yellow squares.

Simplified Firewall

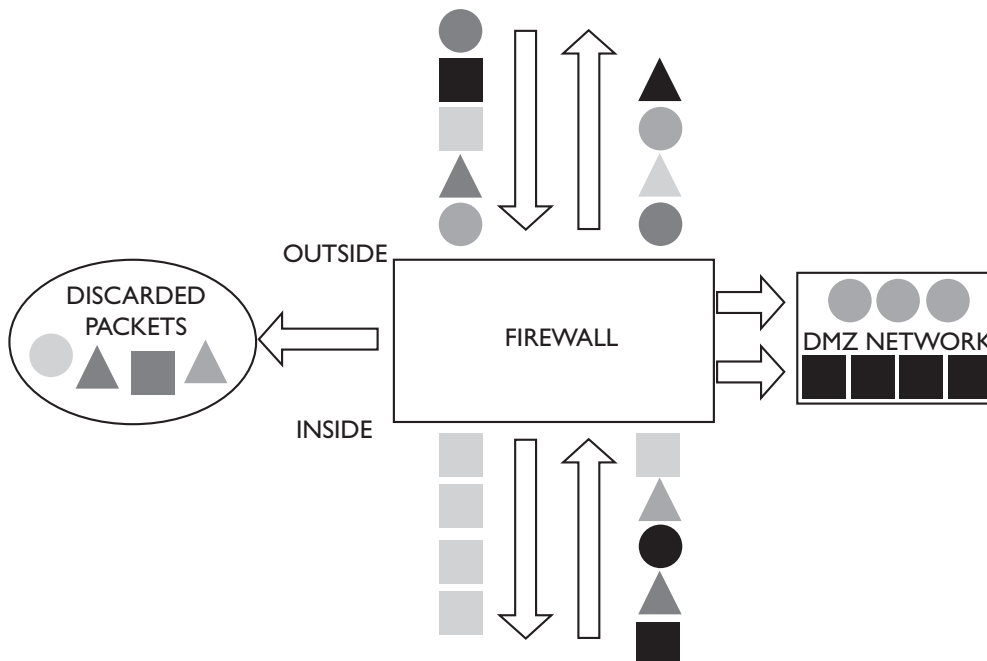


Rule #	Action	Object	Object Color	From	To
1	Permit	Squares	Yellow	Outside	Inside
2	Permit	Triangles	Any	Inside	Outside
3	Permit	Circles	Any	Inside	Outside
4	Deny	All	Any	Outside	Inside
5	Deny	All	Any	Inside	Outside

As you can see, this firewall lets us control carefully how information flows in and out of our network. Many companies will set up a sort of Demilitarized Zone (DMZ) interface on their firewalls to allow an additional level of security.

In our next example on page 11, a DMZ allows green circles to pass through the DMZ from the outside and permits red squares to exit from the inside. In business, this would be the equivalent of allowing clients on the outside to access resources on our network, but not let them inside our “trusted” perimeter.

Firewall with DMZ Interface



Rule #	Action	Object	Object Color	From	To
1	Permit	Squares	Yellow	Outside	Inside
2	Permit	Triangles	Any	Inside	Outside
3	Permit	Circles	Any	Inside	Outside
4	Permit	Circles	Green	Outside	DMZ
5	Permit	Square	Red	Inside	DMZ
6	Deny	All	Any	Outside	Inside
7	Deny	All	Any	Inside	Outside

Firewalls and TCP/IP

Data on the Internet and in most modern networks is carried by a transmission protocol called TCP/IP, usually referred to as IP for short. IP communications can be seen as parallel to those of the postal system. Each data “packet” has an address that goes from the general to the specific in identifying where the packet should be delivered. In the post office system this is like the state, city, zip code, address, and suite number, in descending order.

IP communications work in the same fashion. All data packets on the network have a source address (where they came from) and a destination address (where they are going). Services are identified by what are called ports. To access a particular service, the source system sends a packet to the destination system identifying the port it wishes to communicate with.

Each of these packets and its path provides us with the criteria for building our firewall rule set. We can filter on its source address, destination address, and port in any number of combinations.

Modern firewalls add additional features to address other aspects of securing inbound and outbound communications, but all basically work on the same principle, applying rules to data packets as they pass through a firewall.

Intrusion Detection Systems

Intrusion Detection Systems (IDSs) have also been around for quite some time in one form or another. Only recently, however, have they started to come to the forefront for a typical comprehensive security strategy.

Where firewalls are designed to stop traffic at the network entrance point, the function of an IDS is to inspect that traffic as it passes, to determine if it matches an existing pattern of suspicious activity, impermissible actions, or restricted access.

The IDS monitors traffic and logs statistics about the patterns it sees, and many systems can take action on specific items. Some systems will allow you to drop the suspect packet, notify an administrator, display a message to the end user or even redirect it to a so-called "honey pot" system.

A honey pot system is a mirror image of a production system set up with special security software to allow system administrators and law enforcement officials to track what is done and catch the person behind the attack. To the hacker, the honey pot system looks like they have gained access to a live

production system. Little do they know they are being tracked, logged, and will ultimately be prosecuted.

An IDS allows us to get a much deeper and detailed view of traffic patterns as they are occurring on our networks.

Secure Communications

Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) have become very prominent in today's communications field. And for good reason. A VPN offers a much more cost effective and easier to manage solution than traditional point-to-point dedicated circuits, frame relay networks, or insecure remote access mechanisms.

A basic definition of a VPN is:

A method of providing a secure, private link between locations over a public network.

The term *VPN* is sometimes used in a very broad context. Vendors will sometimes use *VPN* to refer to any product that allows some sort of authenticated service.

The generally accepted implementation of a true *VPN* is to use the Internet as its transport mechanism. *VPN* technologies allow a secure, encrypted connection between two points to be set up across the Internet. A *VPN* simply establishes a "security agreement" between two systems and encrypts all the traffic transmitted between them. Modern *VPN* systems can support hundreds and even thousands of such secure communication sessions.

VPNs are being used to extend the reach of corporate networks and change the way many work. With high-speed Internet

access available in more and more places, people are able to work from wherever they are. The company office can now be extended into homes, hotels, and even coffee shops.

Secure Remote Access

Remote Access is an area of security that has been revolutionized by VPNs. The VPN has allowed businesses to deploy solutions for remote access that provide the same capabilities as if you were sitting in your office.

Ssh

Ssh is an abbreviation for Secure Shell. Secure shell is an important technology, as it provides a secure mechanism of accessing network and systems infrastructure. Traditionally the "telnet" protocol has been used to access and administer network and systems infrastructure. Telnet is an open protocol that does not incorporate any security mechanisms outside of a password that is passed in the clear. Ssh addresses this weakness by providing an encrypted session to the system you are attaching to.

A good general guideline to follow is to ensure that ssh is enabled on your entire network and systems infrastructure and telnet is disabled.

Internet VPN

As we have discussed, Internet VPNs have changed the way remote workers connect to the corporate network. They are not only used as mechanisms to connect remote offices in replacing point to point or frame relay networks but are also extremely effective tools for providing secure access to mobile users.

Encryption Systems

The early predecessors of the modern VPN were encryption systems. Hardware-based encryption systems have been in use on dedicated communications links by banks since the 1970s. Hardware- and software-based encryption systems are still in use today, serving as effective tools in supporting security policy.

Hardware Based

The simplest solution to providing an encrypted link is a hardware solution. In this technique encryption devices are put on each end of the communications medium, making it impossible to hijack the communication.

Https

In today's Internet environment we see a very simple, effective implementation of encryption. It is implemented in the https protocol used to browse the web. When you point your browser at a Web site that uses the more secure https protocol, an encrypted session is set up between your browser and the Web server.

Public Key Infrastructure (PKI)

PKI Systems

PKI is a term that has been talked about in the industry for some time, but its potential has yet to be fully realized. Simply put, PKI systems are distributed encryption systems that allow secure communication across an enterprise. For many businesses the complexity and management required to maintain PKI systems puts them out of reach. As the field is developed and refined, we will see more PKI systems moving into most businesses.

PGP Encryption

A public key encryption mechanism that has been in use for some time is PGP. PGP, or Pretty Good Privacy, was developed in the Internet community as a common method of using public and private keys to secure e-mail communications.

Public and private key encryption can be very complex from a technical standpoint. A simplified analogy can be drawn using the example of a lockbox.

To send a secure message using a public and a private key, think of it as giving a lockbox to your friend (the public key). You give it to your friend with the lid open, but only you have the key to open it (the private key). Your friend places a message in the box and closes the lid. Once the box is locked, only you can open it with your key.

Sending a secure e-mail using a public/private key pair works in a similar fashion. Your friend gets your public key (the lockbox) from a key server. Together they encrypt a message to you using your public key (close the lid on the lockbox). They then send the message to you, which you open using your private key (the key to the lockbox).

Auditing and Monitoring

Auditing and monitoring provide us the mechanisms for ensuring the ongoing security and stability of our networks and systems. They provide the forensic evidence required to follow up on an incident. Their review and analysis of logs

and security records provides valuable insight into what is going on with the networks and systems critical to our businesses' success.

Scanning Tools

As discussed earlier, systems that communicate over the Internet use the TCP/IP protocol and "ports" to identify the systems and services they are trying to reach. The first step someone looking to gain access to a network will take is to "scan" the network.

Basically what this means is that a potential intruder will use a tool to query all of the IP addresses in a network range and, when a live address is found, the tool will query all of the ports available on that system. This will now provide a list of active systems and the services they are supporting. There are scans like this running constantly across the Internet.

The best way to counter this tactic is to run scans of your own. By getting a view of what others can see from the outside of your network, you can more effectively implement mechanisms to protect your business resources. The results of a scan provide a good starting point for an audit of your perimeter security.

Logging and Log Analysis

Almost all network infrastructure and security systems keep logs. All too often, though, these logs are simply thrown out or are overwritten. There are very powerful tools available to collect, store, and digest logs. They can give you a great deal of insight into what is going on in your enterprise and allow you to adapt your security strategy.

Many log analysis tools will send alarms and alerts when a suspect activity is identified. They can analyze log data as it is being written and at times identify a suspect activity as it is in progress.

Log files also provide you with key pieces of forensic data to track down and prosecute potential offenders.

Alert Reporting Systems

Security bulletins are released constantly. The volume and scale of their releases and notifications can be overwhelming. A new area that vendors are beginning to address is to compile and summarize security alerts for your specific business.

For businesses that do not maintain a full-time security team, these services provide a great opportunity to stay on top of breaking security updates without having to stretch already limited resources. Security services allow you to determine which bulletins and alerts you wish to receive, based on the systems and policies in use in your organization.

As you implement your security policy, you will quickly see how many and how often vendors release security fixes, patches, and updates. Having a method to address the volume of updates will make your security strategy much more manageable and effective.

Host Security Tools

Virus Protection

Virus protection is an aspect of Information Security that many are familiar with. The production and proliferation of viruses and hostile programs has reached all-time highs and continues to grow exponentially.

Virus protection programs often use an analysis technique called heuristics.

Heuristics in information technology is the study of patterns in computer code. What virus packages, and IDS systems also, do is look at the code being executed on a system to determine if it matches the pattern of a suspect code that has been seen before.

Because new viruses are produced all the time, the virus protection game is a constantly reactive one. As soon as a tool to block a particular virus is deployed, a variant of that virus is published that gets around the fix.

Operating system and software vendors are working to develop more secure systems that are more virus-proof. The problem is that as long as people can access computer systems on a network, there will be those out there who will try to damage, destroy or manipulate them.

The best defense is ensuring that you regularly update all your systems with the latest patches and fixes, virus definition files, and vendor-recommended upgrades.

Access and Authentication Mechanisms

Simple Password Systems

The most basic security system, which has been around since computer systems were invented, is the user name and password procedure. In today's world, simple user name and password systems are widely used.

Many of the limitations of simple password systems are becoming more and more evident. The days of using your birthday or your cat's name as your

password are quickly passing. The simplest password-guessing program, tied with the incredible processing power of today's PC, can run through password guesses of all of the words in the dictionary, plus most common combinations, such as using a 1 in place of an l, in a very short time.

The common practice today where simple password systems are used is to put some requirements around a password's length, usually at least six to eight characters, a password life that forces users to change their password every so often, usually every 30 to 90 days, and a password guess check that requires random characters, numbers, and combinations to try to fool password-"cracking" programs. Even with all these preventive measures, the simple password system is still breakable.

There are other limitations to the simple password system. People are sometimes their own worst enemies. The first thing many security auditors will do is look at monitors, under keyboards, and in top desk drawers, where they will typically find a notepad with user names and passwords written down.

This is entirely understandable. In today's connected world, users have to remember an incredible number of passwords for various work and home computer systems, Web sites, bank codes, voicemail, security systems, and a host of other applications. With that many passwords it is understandable that users would need a method of keeping track of them. This has led to the development of the next type of security technologies, directory systems.

Directory Services

The idea behind Directory Services is to provide a central repository for storing user and system information. The first obvious application for this is that it provides a central method of authenticating and supplying access to users. Directories are also used as management tools for administering and maintaining networks and systems from a central point.

The Lightweight Directory Access Protocol (LDAP) is an industry-standardized directory system heavily used in Internet systems. Active Directory (AD) and Novell Directory Services (NDS) are directory strategies developed by Microsoft and Novell respectively. AD and NDS extend the capabilities of LDAP and provide additional management features and functions. The limitation of both AD and NDS is that they are proprietary technologies. Getting LDAP, AD, and NDS to work together can be a complex and, in many cases, monumental task.

The importance of Directory Systems is that they are beginning to move toward the goal of a "single sign-on." Single sign-on has been a sort of holy grail in the security industry for a long time. Allowing users to sign on only once and then be automatically authenticated across any system they wish to use is the goal. The actual technical implementation of this goal is still under development. Early implementations have worked in some circumstances but fallen apart in other, more open, scenarios.

Newer development on the technique of Internet-based single sign-on can be seen in Microsoft's Passport logon service and

the Liberty Alliance single sign-on effort led by Sun Microsystems and Netscape. Both are striving toward a single log-on to an Internet service that will automatically provide authentication to other Internet-based services. These efforts are still under development as well and have seen varying degrees of success.

Smart Card Technologies

As mentioned, simple password systems have a lot of weaknesses. Passwords can be guessed, written down and put in the wrong place, or cracked by using simple tools found on the Internet.

One answer to this problem has been to look at the passwords themselves. The idea of “single use” passwords has become a popular method to address password weaknesses. Single-use passwords are implemented using smart cards. A smart card is simply a small chip that constantly calculates a complex algorithm in sync with a password server on the corporate network.

When a user wants to log in to the network, instead of a simple password, they refer to their smart card and enter the password generated by it, usually in combination with a personal secret code. This constantly changing password system makes it nearly impossible to guess a password.

TACACS, TACACS+, RADIUS

There are also several mechanisms out there that address the problems of simple passwords from a protocol point of view. All of them implement a centralized repository for storing user authentication and access information. They provide levels of encryption, better

“challenge/response” methods, and increase the level of security behind the password scheme. Most can work in conjunction with a smart card system to provide secure passwords on the user end and secure authentication systems on the back end.

Messaging Services

Unsolicited E-mail

One of the biggest Information Security problems facing businesses today is unsolicited e-mail, or spam. Unsolicited e-mail is simply e-mail that you didn’t ask for that is sent to you or your organization. Industry studies estimate that unsolicited e-mail is anywhere from 25 percent to upward of 50 percent of the e-mail that most organizations receive. In terms of traffic management, storage, processing power, bandwidth, and sheer aggravation, the unsolicited e-mail problem has gone from a nuisance to an outright epidemic.

By simply registering a domain name on the Internet you will almost immediately start receiving unsolicited e-mail.

Currently there is no simple solution for this problem. E-mail was designed as an open communication system, which is the true power of the medium. But as long as there are unscrupulous parties out there, bulk unsolicited e-mail will remain a problem that we must deal with.

So how do they do it, and how do we address the problem?

Originally, e-mail servers used for sending a message were open to anyone. You attached to a server to send a message, told it who to send it to, and identified

who you were. Bulk e-mail companies, or spammers, exploit this function. They will attach to an e-mail server and send messages to huge lists of e-mail addresses with bogus information in the Sent From field. If you've received unsolicited e-mail, you have seen this: a strange-looking user name with a domain name from a respectable e-mail provider.

The solution for this aspect of unsolicited e-mail is the responsible administration of e-mail servers. Early e-mail servers were "open" relays for mail. If you wanted to send a message, you attached to the server and relayed your message. In today's world, however, responsible mail servers must be "closed." This means that you forward messages only from people you know, specifically your company or clients. Any other type of forwarding is restricted. Implementing the technical measures to authenticate who is sending and receiving, to make sure they are who they say they are, is critical.

There is another danger of having an "open" relay. There are several watchdog groups on the Internet who maintain a list of open relays, called a blacklist. If your mail server is an open relay and ends up on the blacklist, your mail may not be forwarded, your Internet Service Provider may restrict mail traffic to and from your

company, and ultimately it may drop your connection to the Internet. This can have a serious business impact and is a very real aspect of doing business on the Internet. Think about how much your business relies on e-mail as a communications forum. Open relays dropped from a provider's network can take days or weeks to get back into service. That's a pretty dramatic outage for today's businesses.

The next aspect of addressing the unsolicited e-mail problem is user education. Once your e-mail address is on a junk mailing list, the chances of its ever coming off are slim and the odds of the list expanding to include your entire organization are high. And responding to an unsolicited message to be removed in many cases has the opposite effect. Your e-mail address is thus verified as a valid address and added to even more lists.

End users must understand that their business e-mail address is for business purposes and should never be put on any type of mailing list without first verifying who it is run by, what their policy is regarding sharing your information with others, and laying out how to be removed from the list. There are many reputable mailing and discussion forums on the Internet that provide valuable business information and dialogue via e-mail.

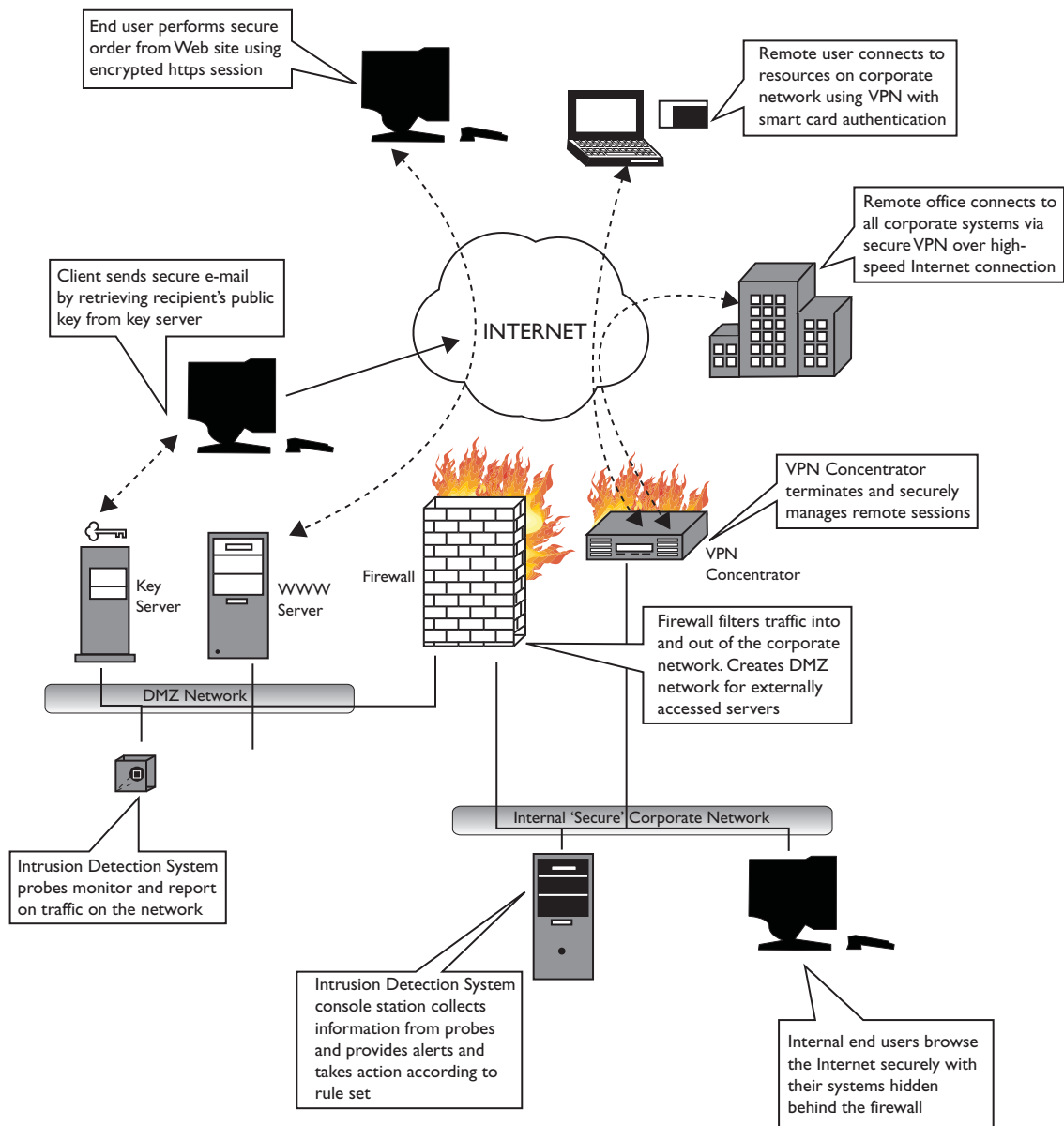
Unfortunately, there are just as many unscrupulous characters who do not value privacy and information security.

The third aspect of addressing unsolicited e-mail is a developing aspect of the Information Security technology field. There are several vendors on the market with products and strategies for filtering and processing junk mail. There are a variety of strategies, but most simply act as an e-mail firewall. If you remember the function of a firewall, it inspects data packets and applies rule sets to them. An e-mail firewall works in a similar way, by looking at the message headers, content, and source to determine if the message meets the criteria for a valid message or is spam. They look for suspect source addresses, questionable content, and compare the message with databases of known junk mail.

The problem of unsolicited e-mail has developed into a field of its own within the umbrella of Information Security. This problem poses one of the largest issues affecting businesses today. If the problem continues to develop and expand, the effectiveness of e-mail as a business tool may change or be eliminated altogether.

As we have seen, Information Security is a complex and diverse field. There are many facets and approaches to making security a part of today's business. We have also looked at how and why having a comprehensive Information Security strategy is critical for today's business.

The following diagram shows where some of the security technologies we have discussed fit in the role of supporting a security policy.



Rockefeller Group Technology Solutions (RGTS) technology team is well versed in the tools and techniques available to support your business objectives in deploying a security strategy. RGTS engineers can develop comprehensive technology solutions to meet your business needs.

The first step in building a security strategy is understanding critical resources and potential vulnerabilities. An Information Security audit is a good way to get a handle on the current state of your organization from a security perspective and develop an action plan for next steps.

CONTACT INFORMATION

Richard Gross, RPA, FMA

Vice President
rgross@rgts.com
(212) 282-2632

Michael Salz

Chief Technology Officer
msalz@rgts.com
(212) 282-2841

Robert Newburger

Vice President of Sales
rnewburger@rgts.com
(212) 282-2233

Rockefeller Group Technology Solutions

1221 Avenue of the Americas, New York, NY 10020
(212) 282-2000 www.rgts.com



Rockefeller Group Technology Solutions™

Rockefeller Group Technology Solutions

NEW YORK – HEADQUARTERS

1221 Avenue of the Americas

New York, NY 10020-1095

Tel: 212-282-2200

www.rgts.com