Global Information Assurance Certification Paper

The Need for Enterprise Network Security:

By
Rajeev Sukumaran
Dated: 1/3/2001

There was a time in the Information Technology (IT) world, not too many years ago, when "security" was the last thing discussed, and something rarely planned for. The Internet, its growth, and the publicity surrounding the accompanying attacks from cyber-vandals have raised interest in and awareness of computer and network security. In the early to mid 1990s, this was reflected in the growth of the antivirus (AV) software and firewall industries. Typical of our society, one looked for the quick fix to the problem of internetwork security. AV software and firewalls became an answer to the computer security question, allowing one to make a check mark in the box and move on.

Antivirus software, firewalls, authentication tokens, intrusion detection software, and locks on the computer room door are all important, but they come on the scene at the end, rather than the beginning, of a computer and network security scheme. This article discusses the starting points – the foundations – of enterprise network security. Firewalls, etc. are not enough.

The Reason for Network Insecurity

What makes enterprise networks insecure? First on the list, and typical, is the lack of an up-to-date computer and network (or more generally, an information) security policy. Really, in many cases one would be hard pressed to find *any* security policy. One reason for this is that often the task seems very difficult. Perhaps it has been put off for too long. Perhaps the policy one has was from before connection to the Internet and no one remembered to update it. Perhaps one does not know how to begin.

Often it is one or more of these reasons, coupled with the second thing that makes networks insecure: a lack of commitment to security by management. In an organisation, commitment expresses itself in the forms of funding and the allocation of people. Some may give lip service to the importance of computer and network security, but often nothing is done to show commitment – to exhibit its importance – until an accident occurs.

A third reason for network insecurity is decentralised system or network administration combined with a lack of co-ordination. One company suffered from this problem. The company, call it XYZ industries, had a security policy; nothing to get excited about, but it did exist, and it was current. Additionally, there was a commitment to security, up to the chairman's office. XYZ also had an office in the north of India and a office in the West of India, the networks and computers connected via a Virtual Private Network (VPN) over the Internet. What XYZ industries lacked, was a centralised system administration and co-ordination of administrative activities.

There are three security questions to ask – rules to live by – when connecting networks together. The first question is:

1. Are these networks secured in the same way, using functionally equivalent security devices, and sharing the same security policy? In other words, are the

same devices are used to secure the networks, and are they secured according to the same rules.
2. Second, do people on each network report to the same authority? That is, do they have the same upper management?
3. Are they managed in the same exact way (perhaps by the same group of people) in both locations? .

Before going on it is best to define some terms. These are not universal definitions, but they are how these terms will be used in this article.

Threat. A threat is a potential for harm. Just because a threat exists does not mean that it will actually happen or cause harm. Threats exist because of the very existence of the system or object, not necessarily because of an identifiable weakness. For example, a threat against an automobile is the threat of theft. This is because 1) the car exists, and 2) the car is made for mobility.

Vulnerability. A vulnerability is a weakness in a system or object that may cause harm. If a particular automobile model was manufactured in error with identical ignition locks on every one built, it would be more vulnerable to theft than other models.

Risk. Risk is the probability that a vulnerability will be exploited. Every car is vulnerable to theft, some more than others are (due to type or ease of theft). A car parked in some sections of a city is statistically more prone to being stolen than the same car parked in another part of the city. The risk is greater in Baltimore.

Each individual enterprise network has unique threats and vulnerabilities. However, the general kinds of threats, the nature of the vulnerabilities, and the causes for concern are similar across the board.

The number one agent of threat to network security is the inside employee. Year after year, studies continue to find that the insider constitutes the threat agent in over 50 percent of computer security events. These are primarily employees, but also include business partners and contractors with direct or network access to a company's computer and network facilities. Still today, most "bad guys" on the outside are just bored high school students who are just poking around. Some individuals trying to break into your site may be hard core hackers, or even industrial (or government) spies, and members of the media. The likelihood (i.e., the risk) of anyone in any of these groups attempting a break-in, either physically, electronically over a network, or socially through going through garbage in a dumpster or "social engineering" the network staff, is directly related to the type of business at an enterprise. Small numbers of things of small value are less interesting than many things of a very high value, and so the risk of attack is subsequently lower.

Usually, an organisation will be concerned about most, if not all, of the following:

- Data Loss. If information is power, then information is also money, and the loss of information can be equated to the loss of power and money. Data can be electronically destroyed or altered.
- Disclosure of confidential information. Information available to workers – to legitimate users of a network – may also be available to someone who has broken in. The theft and then disclosure of confidential corporate information can lead to loss of sales, loss of market position, and, so, loss of corporate valuation. The disclosure of personal and private information about

individuals can lead to civil or criminal liability for a company — not to mention problems for the individuals affected.

- Damage to reputation. This may at first glance seem a minor thing, but most organisations have a concern about this, and rightly so. Reputation, or image, indirectly affects how effective an organisation can be as well as affecting the bottom line. A computer or network break-in negatively modifies the image outsiders have of a company's competence, trustworthiness, effectiveness, resourcefulness, and worth. Customers, potential customers, investors, and potential investors are all influenced by a security incident.
- Downtime. Dealing with security events is expensive. A security incident can shut an organisation down, either by direct action of a cyber-attacker, or as part of the resulting investigation and damage control. After a lot of time spent investigating the incident — either internally only, or with the aid of law enforcement — there is public relations and investor relations to think of, as well as system and network cleanup time.

Anything and everything that touches the computers and the network are considered vulnerable to attack. Every server computer, desktop computer, desktop "Internet gateway" (desktop machines on the network that also have a modem for outside access), each network device, communication facility, and all remote or mobile PCs are vulnerable to attack. Individuals are not immune. System personnel as well as every user of a computer network are points of vulnerability – avenues or agents an attacker might exploit to gain access.
In establishing a network security perimeter you need a security policy that then dictates the mechanisms and methods used to enforce that policy. The order is important.

SECURITY POLICY DEVELOPMENT

STEP 1 — Risk Analysis

A security policy and the related methods and mechanisms are bridged by both a risk analysis and a business needs analysis. The first step, the risk analysis, is the process where we identify assets and evaluates their worth, both to the organisation and to a potential attacker. Assets are anything that might have worth. When looking at a computer network one might list the computers, routers, network, as well as the information stored on the network. One should be very specific in this exercise. People are (usually) considered assets.
Next, postulate threats. Threats come in all shapes and sizes and from every direction. They will cover the entire range of probability, from the obvious and probable to the nearly impossible. They will also cover the entire range of costs to counter, from free to very expensive. Ask a lot of questions at this point. "What am I trying to protect?" "What is it worth?" "What are the threats?" "What are the risks?" There are many "What if...?" questions as well as "What would happen if...?"
An organisation will not be vulnerable to all threats, and part of the analysis is reviewing the system, methods, and mechanisms already in place on the network and in the organisation to see where vulnerabilities to the threats exist. When threats to which an organisation is vulnerable are found, propose countermeasures. There are countermeasures to nearly every threat.
Countermeasures will, no doubt, already exist. While it was stated above that few

organisations have a security policy, what was really meant is that few have security policies that are consistent, relevant, up-to-date, or even written down. Thus, organisations usually have some security policy, often just "allow us to do our business, and keep the bad guys out." Where there is some security policy already existing, part of the risk analysis is to review existing countermeasures, methods, and mechanisms. They are assessed for effectiveness and relevance. Then decide to replace, augment, or keep them.
A cost/benefit analysis can be done as part of the risk analysis, then reviewed against the business needs analysis. As stated earlier, countermeasures exist for every threat. Some are free. Some are very, very expensive. A cost/benefit analysis in the risk analysis allows one to decide what countermeasures are "worth it" to implement. Free or nearly free countermeasures of serious (high-risk) vulnerabilities will usually be implemented. Free or nearly free countermeasures of very low risk vulnerabilities might not be (since nothing is truly free, if we count system management time, installation time, reading log files, etc.). Very expensive countermeasures of very high-risk vulnerabilities may be implemented; it depends on the value of what we protect.

STEP 2 — Business Needs Analysis

Gathering business needs from members of the organisation is easy in that all it entails is a verbal or written interview with individuals from different parts of the organisation. Simply ask, "what is the business need?" The difficult part is sorting needs from wants, and working with these individuals to hone down the list to include only needs.
For example, a first pass through an organisation might produce the following list (for purposes of this paper, this list is abnormally short)

- E-mail in and out for communication with customers, potential customers, business partners and potential partners, suppliers, etc.
- File transfers from outside customers for patch kits.
- Access to the World Wide Web.
- External Web page marketing.
- Push technologies, such as a popular desktop news information service.
- Internet Relay Chat.
- Internet carried audio and video conferencing.

Here is that same list, now with the next step of questions or comments.

- E-mail in and out for communication with customers, potential customers, business partners
  and potential partners, suppliers, etc.
  This will require antivirus software on each desktop, but is generally acceptable.

- File transfers from outside customers for patch kits.
  This would have to be on a computer outside the network security perimeter. One must draw up system management procedures and other safeguards before allowing this. Also, only system staff will be allowed to put things on this server. Within these bounds, FTP access for patch kits in a controlled

directory on a controlled server is acceptable.

- Access to the World Wide Web
  Java, Javascript, and ActiveX are useful but still considered dangerous. We intend to screen
  These at our firewall .Is this acceptable?

- External Web page marketing.
  Acceptable on a webserver controlled and secured by system administration.

- Push technologies, such as a popular desktop news information service.
  These can impose a large burden on Internet gateways. What is the business requirement for this service?

- Internet Relay Chat.
  IRC is not securable. The business need for this would have to be extraordinary. A discussion about this requirement is needed.

- Internet carried audio and video conferencing.
  Some such services can be secured and others are not. We should meet to discuss this further. Would normal audio conferencing be more suitable?

And so it would go. The business needs and the security needs come together, are negotiated, and co-ordinated in the next section.

THE SECURITY POLICY

The security policy is where the business needs and security needs come together and differences are resolved. As stated earlier, everyone has a security policy, but most are not well thought out, not written down, and in an organisation of more than one person, there is usually more than one security policy, with some overlaps and some collisions. It states what to allow, what to deny, what to do, and how to do it. It identifies the kinds of uses of resources that are regulated. The identified resources must be tangible and either controlled by or required by an organisation. For example, an Internet connection might be in the hands of an Internet Service Provider, but may still be correctly listed as a regulated resource if the connection is required for business.

A security policy, to be useful, must match reality, which is why one starts with analyses of business needs and risk. This is also why it must be relevant and up-to-date.

A security policy declares:

- How an organisation handles information
- How people may access information
- Permitted behaviour
- Prohibited behaviour
- Existing assurances
- Auditing practices
- Control practices

As one can imagine by a few of these, parts of the security policy should be restricted on a need-to-know basis.

In laying this out, the author's intention is not to drive the reader to despair. Most security policies evolve. Usually, they start with a Swiss cheese kind of consistency that matches the security perimeter and posture, both of which are also full of holes. The next step, after some work, is an inconsistent or unbalanced security policy, like putting an iron door on a grass hut. Organisations then move to what Internet firewall expert and author Bill Cheswick of Bell Labs called "a crunchy shell around a soft, chewy centre." Eventually, they hope to get to systematic information security. This systematic security is built on architectures, strategies, and standards, rather than on what firewall won the latest award or which product supports the newest Internet service. Security must be treated like any other investment. We focus on the customer, minimise life cycle costs, and maintain flexibility and responsiveness.

Security policy planning entails starting with the mission needs. Identify the mission critical information through data classification. Classifications might include "don't care," sensitive, financial, competitive, legal, privacy-related, etc. List the identified threats and vulnerabilities from the risk analysis. As stated above, these may include people — employees, partners, customers, and suppliers — and access points, equipment, mobile computers, and critical applications. Also, as implied above, there will be some residual risks — vulnerabilities that will not or cannot be countered. Identify these in a security policy.

A good security policy matches the corporate culture, defines rules of behaviour and individual responsibilities, matches responsibility and authority, details consequences of misuse or abuse, and lists services supported and controls to be employed.

METHODOLOGY AND MECHANISMS

The technology and methods employed as countermeasures are dictated by the security policy, and are part of the policy, but deserve special highlighting. These must match the policy, and therefore the threats. Methods and mechanisms employed will include things like firewalls, intrusion detection devices, biometric authentication devices, antivirus software, and the like. The general practice is:

1. Securing PC with antivirus software
2. Putting firewalls on the connection to the Internet
3. Putting web servers on the Internet (without real security)
4. Deploying web servers internally (without real security)
5. Deploying firewalls internally
6. Adding Virtual Private Networking (VPNs)
7. Securing "Internet side" web servers and other servers (hardened systems, behind a firewall, etc.)
8. Securing internal servers

Many organisations do not get past step 4. Most do not get past 6. Most understand the need for all eight steps (or at least the first seven steps).

Equally important, are the procedures in place for system management and monitoring. Things such as the proper installation of systems (often this means changing the default settings), backups, reviewing audit logs, physical access to servers, and security education are vital security measures.

The security policy should spell out what an organisation will do should an intrusion

be discovered. An incident response plan (part of the security policy) should be like a disaster recovery plan — it must be done in advance, not during a crisis. The following questions should be answered:

- Who should be notified?
- What will you do if you catch someone in the act? Let him continue? Cut him off?
- Will you call the police?
- What do you tell the press? Who talks to the press?
- What do you tell customers, clients, and investors?
- What do you tell your users? Your patients?

The methods and mechanisms employed must be based on the security policy, meet the business needs, counter identified vulnerabilities, and reduce the risks resulting from threats

Conclusion:

All of these elements – the risk analysis and business needs analysis, the security policy, and the security mechanisms and methods – work together to establish a company's corporate security approach. An essential fact, however, that can't be overlooked is that threats change, vulnerabilities change, business requirements change, and the available countermeasures change. All of these must be periodically and routinely re-evaluated.

The results of neglecting any one of the steps — risk analysis, business needs analysis, security policy, and the instituting and deploying the resulting methods and mechanisms — can be disastrous.

References:

http:\\www.securityfocus.com
http://www.w3.org/Security/Faq/
http://www.cert.org/

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event