

# TECHNOLOGY OF INFORMATION SECURITY

Ram Swaminathan, Baljinder Sandhu, Nita Goel, Pulak Dhar, Vineet Srivastava.  
Cistel Technology Inc, 210 Colonnade Road, Suite 200, Nepean, ON K2E7L5.  
[rswami@cistel.com](mailto:rswami@cistel.com)

## Abstract

*As opposed to other assets, information is something that can be stolen without being lost. Security administrators have a complicated and hostile environment, where data need to be available for those who need it and must be denied to unauthorized access. As both internal and external connectivity challenges become complex, security efforts become daunting to IT system administrators. Being aware of and paying attention to the key elements of IT security will protect the information assets against majority of the security threats. The paper focuses on steps to achieve workable IT security policies by concentrating on risk assessments, prevention of vulnerabilities, detection, implementation of resources to defend investments, quick and effective response to compromises and attacks and a constant vigilance. The set of rules we propose to extract will determine the factors to use to balance security and other societal interests. Having a security policy document in itself is not enough. The contents must be delivered effectively to have the desired results.*

**Keywords:** *IT Security; Vulnerability; Assessment;*

Security Managers need a reliable solution for defending the organization against constantly evolving attacks. Internet based threats are getting faster, stealthier and more and more dangerous. Technologies that alert about potential threats are extremely good to have. However, if a system depends on manual response to secure against these threats it is considered useless, because of the very nature of these attacks and also the amount of false positives. Our approach is to build on the basics and then go on to protect against possible unknowns, minimize the false alarms and automate the response to an alert.

## Rule No. 1: Protect the Perimeter.

Any amount of preparedness and defense is often inadequate as new attacks propagate very quickly. There has to be a proper methodology to keep these defenses up to date. Every security measure will have inherent weaknesses and special care has to be taken to address them.

Perimeter protection is by far the best protection strategy for corporate assets. Firewalls have to allow certain kinds of traffic in and out of the network. This gives an attacker a chance to gain control of one of the hosts in the network, if it is vulnerable. A proper configuration can make penetration very difficult, even for skilled attackers. Policy errors and misconfiguration can some times make the firewall very permissive.

## Rule No: 2 Implement IDS

IDS (Intrusion Detection System) can identify malicious traffic patterns and drops such network packets and hence avoiding compromise of the network resources. A good implementation of IDS involving content monitoring techniques and protocol analysis should be capable of alerting the security professionals of any type of attack. Many of these IDS implementation are based on a set of threat profiles or signatures against which the traffic is compared. Suspicious network packets are handled as per the pre-defined policies. IDS has some weaknesses too. It generates a large number of false alarms and hence is very heavy on maintenance requirements. Also, a rapidly propagating attack can penetrate the system before the IDS has been hardened by reconfiguration using the new signature profiles. An emerging technology known as "Anomaly-based detection" overcomes the shortcoming of signature based detection. The new technique avoids the dependency of requirement of new signatures. An organizations network patterns are baselined and variations are flagged.

### **Rule No. 3: Prepare against the Unknown**

Conventional methods of IT security which discover attacks after they happen, is not good in this age of fast Internet access. It is inadequate to depend totally on the security community to prevent against unknown attacks as there is a big time lag between identification of a new threat and fixing it. Hence it is a good practice to implement technologies for intrusion detection, alerting and prevention that work with minimum human intervention. This technology focuses on detection and thwarting attacks before they impact the corporate environment. Typically such products sit outside the firewall and use pre- attack scanning and reconnaissance activity to detect potential attacks, tries to shut down all traffic coming from a malicious host and integrate traffic prohibition policies. These products can implant flags in regular attack patterns and will be able to identify them when an actual attack takes place. Further, these all business partners can benefit from the knowledge base it creates.

### **Rule No. 4: Secure the Core Systems**

Constant monitoring of the network, checking and analyzing the security logs and setting up honey pots help to understand what is being targeted. Service packs, patches, bug fixes and hot fixes should be applied as an ongoing effort against preventing attacks.

Security will always be breached without direction, completeness and consistency. Security policies are not to impose restrictions. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues. It is the responsibility of every computer user to know these guidelines. The following are general guidelines for use.

- a. All confidential and valuable information be encrypted as per guidelines for encryption.
- b. Only authorized people should be allowed access for network traffic measurements.
- c. Classification of information as Public and Privileged will be great help in deciding what needs to be protected.
- d. A sound password policy is a very effective security measure. Users are responsible for the security of their passwords and accounts. System level passwords should be changed every 45 days; user level passwords should be changed every two months.
- e. All individual workstations should be protected by auto-locking, password protected screen savers. Mobile computers should be protected with special care. Antivirus with the current updates and Intrusion

detection programs should be used at all times to protect against Trojans, viruses and spyware.

- f. Disallow port scanning or security scanning, network monitoring unless authorized by the company.

### **Rule No. 5: Develop a Methodology for Vulnerability Assessment**

Various tools can be used to identify specific vulnerabilities in systems. The purpose of vulnerability analysis is to take what was identified in the gathering of information and test to determine the current exposure, whether current safeguards are sufficient in terms of confidentiality, integrity or availability. It will also give an indication as to whether the proposed safeguards will be sufficient.

The vulnerability analysis phase also includes penetration testing with the objective of obtaining something of value, such as a text file, password file, classified document etc. It is important to note that this should be pre-determined with senior management. The specific vulnerabilities can be graded according to the level of risk that they pose to the organization, both internally and externally. A low rating can be applied to those vulnerabilities that are low in severity and low in exposure. Vulnerabilities would receive a high rating if the severity was high and the exposure was high.

Identify technical vulnerabilities by making use of automated scanning tools. A security scanner is software which will audit, even remotely, a given network and determine whether hackers may break into it, or misuse it in some way.

A good security scanner should be able to detect services running on any port and test its security and attempt to exploit the vulnerability, without assuming anything.

The following are some of the recommended tools.

Nessus ( [www.nessus.org](http://www.nessus.org) )

Nessus has *posix* tools (Solaris, FreeBSD, GNU/Linux and others) and also for windows platform.

Nmap ( [www.nmap.org](http://www.nmap.org) )

Nmap is a utility for network exploration or security auditing. It supports *ping* scanning (determine which hosts are up) and TCP/IP fingerprinting (remote host operating system identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more.

Netcat ( [www.astake.com/research/tools/index.html](http://www.astake.com/research/tools/index.html) )

TCP/IP Swiss army knife is a simple UNIX utility which reads and writes data across network connections using TCP or UDP protocol.

The reports generated after the Security Audit explained in the previous step, gives a good indication of health of the network. Any weakness detected has to be rectified immediately.

Security measures and policies merely lessen the chances of misuse of the system that damages caused by certain common incidents. It helps discover and limit any misuse and/or damages promptly, and makes it easier to recover from various types of accident and misuse. It does not completely prevent such breaches.

Default settings tend to have security settings at the most permissive levels to make their networks perform most impressively. As vendors often deliver systems with default levels, security tends to be intrusive and constraining in various ways.

Untested server security will be expensive for the company in the event of a disaster. Mistakes can happen in creating server security policies and in implementing them because of the human errors. Full security aspects should be tested to see that it conforms to your security policies. Not only this should be done when you design and implement your security, but also should be done on a reasonable periodic basis. It is preferred to hire an external agency for such audits.

### **Rule No. 6: Implement Total Physical Security and Disaster Recovery Measures.**

Over eighty percent of the computer system attacks are perpetrated by insiders. Ensure that servers are located in a locked room with tight access controls to the room and the building. If an attacker gets physical access to a computer, they can easily access all the information.

#### **6.1. Physically securing the hardware**

Keep any computers which have sensitive information away from the general public. Keep them locked using specialist devices available for attaching computers to desks. The computers which store the sensitive information should be kept in a special computer room.

#### **6.2. Physical security of networks**

Networks can be easier to secure if all computers that hold the sensitive information are physically secured. Other computers can be left less-secure, provided the network itself is secure and the unsecured computers don't have sensitive information on them.

Network access, such as Internet access, tends to be at the mercy of Internet Service Providers. It is important to have reliable access and build redundancy into the system. The reliability of your local providers can be a significant factor depending on the nature of business.

### **6.3 Disaster Recovery**

A good disaster recovery plan should include the administration and maintenance procedures. Maintenance of the Disaster Recovery plan is the responsibility of Technical Support team. The steps the coordinator should take to maintain this plan are as follows:

- a. Ensure that the plan is updated at least once per year.
- b. Ensure that the plan is tested at least once per year.
- c. Ensure that the plan is signed-off by the Director or Finance Manager.
- d. Update the plan at the earliest convenient time after significant network or business changes have occurred that affect the plan.
- e. Make sure that the plan is stored in a secured area accessible to the Disaster Planning Coordinator and ensure that at least one copy is kept at the client location.

### **Rule No. 7: Constantly Re-Assess and Overhaul Security policies (Risk Management)**

The process of identifying, prioritizing and addressing risks is called risk management. A risk is any threat that can disrupt the organization's access to services or data. The risks can be internal or external, either preventing access or delaying access. Every organization needs to identify the risks that it faces and prioritize the risks, and determine how it should address the possibility of the risks materializing by following the steps outlined below.

Risks and their impact vary from organization to organization and according to geographical locations. This document concentrates on the security related aspects of risk factors and its impact on an organization and users. The important issue is a good understanding of the service classification based on critical and desirable services. To identify security efforts, it is essential to analyze vulnerabilities in the existing infrastructure and determining what needs to be protected and what can be done to minimize exposure to the threat.

Once the security efforts are identified, a cost/benefit analysis is carried out and required changes are implemented in the business setup.

### **Rule No. 8: Train IT Security personnel**

Managing Security is very difficult, so also to find appropriately skilled personnel to defend against

attacks. The shortfall is reported to exceed a million workers within a few years. In the best interests of its investments, companies should not only identify skilled working professionals but also train them. They should also arrange for internal training sessions for distributing the skills learned. Considerations should be given for specialization in various aspects related to IT security. In-depth security training should not be a choice but a necessity.

There is no substitute for certified professionals who have undergone training from organizations such as SANS and International Information Systems Security Certifications Consortium Inc. These institutes offer diverse and specialized trainings which embrace all aspects of IT Security. Experience plays a crucial role in defending against attacks. It is important to measure the level of competence of the IT security professional and his/her dedication to the task. It is essential to conduct "Security Drills". This will provide a training ground for the analysts to prepare for fundamental concepts. A conceptual approach should be well designed to provide adequate results, where it becomes too expensive to stage realistic security situations.

Information security conferences such as USENIX and DEF CON provide a good opportunity to expose security staff to new trends in the field as well as network with peers. Vendor-hosted classes and certification tracks, such as those offered by Cisco or Checkpoint, often provide employees with the opportunity to sample newer products and understand the security concepts behind them. To help employees obtain data to tune devices, stay abreast of current technology, and otherwise update their general security knowledge, encourage them to conduct research and study security resources such as newsgroups, websites, and security periodicals.

## Conclusion

The selection of a standard in any area impacts the application developers and the security personnel during design of the organization's security policy. Emerging technology enhancements in Biometrics and combination of several methods like general face matching surveillance technology ( deployed during the Super Bowl) as well as Iris and finger print scans ( being used at major airports in the US ) will reduce vulnerability, minimize the risk of hoaxes and provide high usability.

Wireless technology is expected to become the new arena for attacks and exploits. Many products are being developed for threat monitoring, response and mitigation by consortium of top security researchers at

various organizations and these are combined with in-house talent. A good example is the National Infrastructure Protection Center at the FBI.

We will be seeing a flood of self patching software, making the life of administrators simple. One good example is Microsoft XP. Major improvements are being done and Linux kernels are getting stronger and better at security management thanks to a big support from IBM.

System security sentries will be setup that block access by systems that have not been hardened. Buyers specifying that a system meet a minimum set of requirements will become commonplace. Rule and profile based intrusion detection will start becoming more dominant. Large scale infrastructure and configuration based security improvements will be seen as cost savers in the long run. Businesses and Government will intensify their coalition, as security problems can not be resolved by any one setup.

## Acknowledgements

We gratefully acknowledge useful discussions and advice from our colleagues Dr. Nishith Goel and Ron Church of Cistel Technology Inc, Hugh Baldwin, Dr. Alok Patnaik and Alok Saxena of Tecsis Corporation and Prof. Chung-Hong Lung of Carleton University.

## References

- [1] James Bayne, An Overview of Threat and Risk Assessment, January 22, 2002. <http://www.sans.org/rr/audit/overview.php>
- [2] Kurt Garbars, Implementing an Effective IT Security Program , August 28, 2002 [http://www.sans.org/rr/audit/IT\\_sec.php](http://www.sans.org/rr/audit/IT_sec.php)
- [3] Jennifer Vesperman , Introduction to Physical Security and Security of Services ,Feb 24, 2002. <http://www.tldp.org/REF/INTRO/PhysSecurity-INTRO.pdf>
- [4] Cistel Internal Report TR-01, Technology Of Trust, Dec 31, 2002. <http://www.cistel.com>
- [5] Lamont Granquist , NMAP Guide. <http://www.insecure.org/nmap/lamont-nmap-guide.txt>
- [6] Mark King, Security Lifecycle – Managing the Threat February 19, 2002. <http://www.sans.org/rr/securitybasics/lifecycle.php>
- [7] ForeScout Technologies, The First 15 Minutes, An Intrusion Prevention White Paper. [www.forescout.com](http://www.forescout.com)
- [8] 5 Steps to Enterprise Security , An eWEEK White Paper. <ftp://ftp.eweek.com/pub/eweek/pdf/printpub/White/whitpaper.pdf>