# Global Information Assurance Certification Paper

# Risk Assessment ?? Deliverables?? What it's all about.

Abhay Sadwelkar
SANS Security Essentials
GSEC, Version 1.4
06/29/2002

## Executive Summary

The objective of this paper is to provide a high level overview to the security student on the components of Information Security Risk Assessment and some of the various best of breed technologies involved in securing a company's network and information assets. What is Risk Assessment? :

> Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk.[1]

Why do we need to conduct a risk assessment? To identify the potential hazardous situations, which may negatively affect our business processes, and to estimate the likelihood of such an event occurring. A risk assessment would help to provide alternative solutions to reduce the risk, estimate the effectiveness of those solutions and provide information to base a risk management decision.

The paper discusses in brief technical and business risk analysis and touches upon ISO 17799 based Gap Analysis, Disaster Recovery Planning options (DRP), Business Continuity Planning (BCP) and the deliverables therein. We sum up with highlights on leading technologies in antivirus, firewall, intrusion detection, authentication and threat management. These technologies are a part of the defense in depth[2] approach to secure our organization's information assets. Though each technology is a discipline in its own, an attempt has been made to provide the concepts in a nutshell.

ASSUMPTION for Risk Assessment is for a corporate network with a WAN/LAN environment and remote branch offices.

**Scope of Work**

In undertaking any form of risk assessment, scope of the intended work has to be clearly defined as a bottom rule. It means we precisely understand the client network, his business requirements and specify the output reports of this exercise. A step-by-step sign off procedure is recommended to be included in performing the Risk Assessment. Otherwise the exercise would be a never-ending one and we have to think of those budgets/deadlines too.

We will discuss primarily the Technical and Business risks and the recommended technologies to address these. Note exact efforts and recommended technologies for Implementation can only be estimated after completion of the Risk Assessment. For the benefit of this paper we have made a few assumptions on the product implementations.

---

[1] Jack L. Brock Jr, p.6.

[2] SANS Security Essentials Curriculum, Day 2, Threat and the Need for Defense in Depth, p 1-3.

A sample Scope of work for such an assessment for our corporate network would include but not limited to the following:

**Risk Assessment**

1.Technical

- Identify and categorize key information assets and processes
- Perform Threat Assessment
  - Network vulnerability assessment for WAN/LAN including network, hosts, database
  - Penetration testing
- Design Disaster Recovery options
- Design a Secure Architecture

2.Business

- Business Continuity Plan[3] Framework for the IT Operations Center with Business Impact Analysis[4]
- Assess compliance with existing security policies and procedures and Perform ISO 17799 based Gap Analysis[5]

**Recommended technologies for Implementation**

Budgets and business requirement must be considered while proposing the technologies.

- Identify and propose recommended technology/products for implementation.

**Deliverables**

We have clearly defined the scope of work in carrying out a RA for our corporate network and now we look at the deliverables. The deliverables should match the scope of work.

**Risk Assessment Deliverables**

1.Technical

- Critical Information Inventory
- Threat assessment Reports
  - Vulnerability assessment report detailing system flaws and weaknesses with remedial actions
  - Penetration testing report detailing the information leaks and exposures caused by such leaks with remedial actions.
- Disaster Recovery Strategies options
- Recommended Secure Architecture Design

2.Business

[3] The Business Continuity Institute
[4] Information Resources and Technology Security Office, Virginia Tech
[5] Ministry of Communications and Information Technology, India

- BCP framework, Business Impact and Allowable Outage Times report[6]
- Gap Analysis report highlighting differences in the current security management posture against the ISO 17799 recommendations

**Recommended technologies for Implementation**

- Some or all of the below sample products/technologies may be required to secure the network and protect our corporate's Information assets.
  - o Antivirus for the entire Enterprise
  - o Firewall
  - o Intrusion detection
  - o Authentication
  - o Threat Management software

# Details

**Understanding of client Requirements**

It cannot be stressed enough that the client's business requirements are at the center of this Risk Assessment exercise and hence the assessment and the solution should appropriately address these.

By using a security assessment questionnaire template, Information on our corporate's network such as network diagram, number of remote locations, number of servers, clients and their platform, applications, database, firewall, existing security policies and technical security guidelines, remote connectivity and such other relevant info can be gathered. It is important to discuss and understand at this stage the client's pain areas and his priorities in addressing them.

Such information will form the basis of Understanding of Client requirements statement and help mutually define the scope of the engagement.

**Risk Assessment Deliverables (Technical)**

**Identify and categorize Key Information assets and processes**

The objective is to identify IT processes and key Information Assets that are essential for the delivery of output that achieve business goals. Identification of key IT processes and assets that will enable the corporate to achieve it's business objective's is an essential step that will equip our corporate planners with details of those business critical processes and assets that are required to be operational during an adverse event.

This two step activity consists of gathering knowledge of critical processes and assets from business unit managers/ business process owners, reviewing the existing organizational documents that detail IT processes, inventory and process study through site visits.

[6] NIST Special Publication 800-34, p.17.

Interviews with the key business process owners and business heads, or detailed questionnaires that will require them to list key business processes in the order of criticality, that they perceive and link them to the business outputs. Reviewing of organizational documents such as IT Policy, organizational digital/information security policies, agreements with third parties etc will provide the necessary details on the key information processes.

The resultant report is a collection of various key organizational IT processes and Information assets and their respective dependencies.

**Perform Threat Assessment**

This step explores various potential threats to the critical identified information systems and assesses their frequency of occurrence based on vulnerability assessment

This comprises of

- Threat source identification and developing a list of potential threat vectors such as natural, human, environmental
- Vulnerability assessment, both technical and non technical to uncover system flaws which can be exploited by the threat vectors. Vulnerability assessment can be done by using scanners, network mapping, port scan, manual exploit research and such tools.
- Penetration/Perimeter testing[7] to test the security posture of our corporate's network infrastructure. This can be done to reflect on site (disgruntled employee) or off site attack from the Internet (external attacker)

The deliverables of this exercise would consist of

- Vulnerability assessment report that will detail system flaws and weaknesses categorized as high, medium and low risk with corrective action that need to be taken
- Penetration testing report provides details on information leaks, the exposures caused from them and corrective action.
- Threat Assessment report will detail the likelihood of occurrence of exploitation of the found vulnerabilities by the identified threat sources

**Disaster Recovery Strategies Options**

Disaster Recovery Planning[8] is the process of preparing for Disaster and catalogues procedures to be followed during and after a disaster. The two major steps in a DRP process are:

- Data Processing Continuity planning
- Data Recovery Plan Maintenance

**Data Processing Continuity planning**

- This may include mutual aid agreements[9] that is an arrangement with another enterprise having similar business and network infrastructure

[7] Charl Van der Walt, Security Focus
[8] Jeffrey H. Wold, Disaster Recovery Journal

- It could be a third party commercial service providing alternate back-up and processing facility
- It could be one of the following sites[10]
  - Hot-Fully configured computer facility with power and operational file and print servers and workstations. All applications loaded and mirror a regular production environment.
  - Warm-Computer facility with power and hardware, applications is not loaded. Sometimes servers are available but not workstations
  - Cold-Facility with power but no servers/workstations
  - Mobile-Sites are self-contained, transportable shells custom-fitted with specific telecommunications and necessary IT equipment.

DRP may include transaction redundancies such as:

- High Availability Solutions such as data mirroring, vaulting[11], shadowing etc
- Distributed storage network solution namely Storage Area Networks, Network Attached Storages, Centralized Storage Management Solution etc
- Storage solutions such as tape servers, virtual tapes etc

Various parameters such as compatibility with present infrastructure cost involved, processes complexity and personnel skill level required in administration etc will be considered while evaluating the options. The recommended strategies have to be approved by the client

**Data Recovery Plan Maintenance[12]**

DRP can get out of date like any other plan and hence an audit procedure is necessary to ensure that plan maintenance is regular and complete. It is important to test the DRP and the test must encompass every component to instill confidence in it. DRP is too critical not to be tested as its functionality determines the survival of the organization. DRP may include several teams for recovery, salvage and resumption of operations.

The deliverables will include the following

a) Recovery strategies options report will detail the various recovery strategy options along with their advantages and drawbacks
b) Disaster recovery and backup strategies and measures report
c) DRP maintenance plan guidelines

**Secure Architecture Design**

Based on the findings of vulnerability assessment, risk assessment and high-level security policies framed, the secure architecture for the client network will

---

[9] NIST Special Publication 800-34, p22
[10] NIST Special Publication 800-34, p 20-21
[11] Document management, Flow Logic
[12] NIST Special Publication 800-34, p 28

be designed. Various products are available nowadays to fit in the secure architecture design, which we will discuss further on in this paper. The physical security products will include Electronic Door locks, Access cards, Fire suppression systems, Power control and regulatory appliances, alarm systems etc.

The resultant Secure Architecture Design will detail the various security components involved in the design, their functional roles and integration with client network. This also includes recommended products in each category for secure architecture.

**Risk Assessment Deliverables (Business)**

**BCP Framework for IT Operations Center:**

What is Business Continuity?

> A proactive process, which identifies the key functions of an organization and the likely threats to those functions. From this information, plans and procedures that ensure key functions can continue whatever, the circumstances, can be developed.[13]

BCP is designed to protect disruption to normal business activities and to protect business critical processes from natural and man made disasters. BCP aims at preservation of capital, resumption of normal business activities and to minimize cost of business disruptive events and mitigate risks associated with it. BCP for the IT Operations Center would focus on[14]:

- Local and Wide Area networks and servers
- Telecom and data communication equipment and links
- Workstations and workspaces
- Application and system software
- Data, media, storage and records
- Staff duties and production processes

Broadly the elements of BCP are:

- Scope and plan initiation
- Business Impact Assessment
- Business Continuity Plan development

**Scope and plan initiation**

It is important to establish and communicate the need for BCP, obtain management support and manage the project to completion within agreed time and budget limits.

After examining the company's operations and support services we list the activities to be covered by the plan and then approve the list for the resources needed and the management practices to be employed in creating the plan. BCP

[13] The Business Continuity Institute

[14] NIST Special Publication 800-34, p 41

should consider all distributed information processing and storage issues. While it would be a centrally planned and implemented process it should fully cover all aspects of the IT operations of the company. The BCP committee should reflect enterprise wide involvement in this key information security process.

**Business Impact Analysis**
The objective is to determine the magnitude of impact of threats to the critical information systems should any occur. Defined as:

> A management level analysis, which identifies the impacts of losing company resources. The BIA measures the effect of resource loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning[15]

Impact Analysis aims at determining the impact that could occur due to compromise of any critical systems. The impact due to such possibilities are then estimated and measured along the impact timeline. The various parameters that will be considered for impact include financial impact, reputation impact, regulatory/compliance impact etc. The Impact timeline will indicate the possible impacts during different period in time post the disastrous event. The negative impact of a security event could result in the loss or degradation of any or a combination of the following security goals[16]: integrity, availability and confidentiality.

**Business Continuity Plan development**
This is the process of using information collected and analyzed in Business Impact Analysis to evolve a recovery strategy and consists of two phases of Defining a continuity strategy and Documenting the defined continuity strategy.

In defining a continuity strategy, we consolidate the results of BIA and management perception of criticality. All relevant enterprise elements like computing, facilities, people, supplies and equipment are covered while defining the continuity strategy

In the second phase we document all findings and conclusions of the continuity strategy definition phase
It is important that top management approves the BCP and there should be an enterprise wide awareness of the plan. As with all plans the BCP may go out of date and hence it is necessary to periodically review and update the plan.

The deliverables of this entire process are:

[15] The Business Continuity institute
[16] Gary Stoneburner, Alice Goguen, and Alexis Feringa, p. E-2.

a) An Impact analysis report stating the magnitude of impact that could happen due to compromise of various information critical assets of the client systems during various time periods post the disaster forms this report
b) An Allowable Outage Times report is a list of maximum permissible outage times for various critical assets of the client information system.
c) Risk Assessment Report: Based on the impact report and the threat assessment report, risk level of various critical assets will be determined and this report constitutes this risk information ordered according from high propensity critical assets to low propensity critical assets.
d) Business Continuity Planning report that will detail the BCP options for the IT Operations center.

**ISO 17799 Gap Analysis**

No matter how secure and well protected an organization appears to be, sensitive information can be leaked without knowing until it is too late. As the number of reported information security breaches consistently increases, the need to create a management framework for information security intensifies. The Internet is now the most effective form of communication as well as being a convenient platform for transacting business/commerce with a wide range of existing and new customers. Dependence on Information systems and services and interconnecting of public and private networks and sharing of information resources has increased the difficulty of achieving access control.

In today's world customers look for quality, assurance and value for money in the products or services that they pay for. Nowadays standards play a very important role to assure customers and provide confidence in making their investment decisions. In our day to day life we see so many of these standards reassuring us of the quality of the product/services we purchase whether it may be foodstuff, clothes, medicines, insurance, heath care, stock etc. Similarly information security standards play a crucial role in managing and documenting a company's information assets and assuring customers their information would be kept secure and confidential.

It is important not only to follow standards but also adopt an international standard such as ISO 17799 that clearly defines the scope of Information Security management System (ISMS)[17] and the controls applicable to improve overall security and ensure business continuity.

Conducting a Gap Analysis is the first step in this direction. The purpose of a Gap analysis is to assess client's current Information Security Management System against ISO 17799.Gap analysis involves analysis of the existing security management system of client and comparing those arrangements with the

[17] Timothy Stacey, SANS Information Security Reading Room

requirement of the International Standard. This will enable in highlighting weaknesses and making recommendations for necessary controls for ISO 17799 compliance or certification.
The existing security policy and procedural controls are grouped into various sections in line with the 17799 standards. Then the grouped existing controls are checked against the best practices outlined in the respective control section of the standard. The various sections[18] along which the existing controls will be grouped and checked against are as follows.

1. Information Security Policy-A document to demonstrate management support and commitment to the ISMS process
2. Security organization-An established management framework to initiate and control the implementation of information security within your organization and to manage ongoing information security provision
3. Asset classification and control- A comprehensive inventory of assets with responsibility assigned to ensure that effective security protection is maintained
4. Personnel security- Well defined job descriptions for all staff outlining security roles and responsibilities.
5. Physical and environmental security- A clear and concise definition of the security requirements for your premises and the people within them.
6. Communications and operations management- Optimize your communication to facilitate smooth operation of the ISMS.
7. Access control- Network management to ensure that only those with the appropriate responsibility have access to information in the networks and the protection of the supporting infrastructure.
8. Systems development and maintenance- Ensuring that IT projects and support activities are conducted in a secure manner through data control and encryption where necessary.
9. Business continuity management- A managed process for developing and maintaining business continuity plans which protect critical business processes from major disasters or failures.
10. Compliance- A demonstration to clients, employees and the authorities of your commitment to meet statutory or regulatory information security requirements

The resulting output will be a document comprising of the mapping of existing controls to the 17799 standard controls and the details of the shortcomings of the existing controls. Recommendations on the changes required to achieve compliance to ISO 17799 will be a part of this document.

Implementation of this standard helps identify threats, vulnerabilities and risks, and reduces the impact of security incidents. Benefits include improvement in customer confidence and satisfaction, improves overall security, manages and facilitates continuous improvement.

[18] ISO 17799 Security World

## Recommended technologies for Implementation

As mentioned previously during the scoping of work the exact efforts and recommended technologies for Implementation can only be estimated after completion of the Risk Assessment. For the benefit of this paper we assume the following products for implementation and briefly describe each of them.

- Antivirus
- Firewall
- IDS
- Authentication
- Threat Management

**Antivirus**

**Trend Micro** (www.antivirus.com)

Enterprise antivirus solution consists of a suite of products called Trend Enterprise Solution (Neat Suite) and has five components.

**Interscan Viruswall**: This component scans 3 types of Web Traffic (SMTP, FTP, HTTP) and is your first line of defense from Internet based viruses such as Nimda, Code Red,

Supported on Solaris SPARC, HP UX, Win NT/2000,Red hat Linux and Suse Linux

**Scan Mail for Exchange/Lotus Notes**: Heuristic scanning of the Exchange/Lotus mailboxes. Stops viruses from using your Exchange/Lotus Notes environment as a distribution mechanism. ScanMail for Exchange/Lotus Notes detects and removes viruses hidden in databases and email attachments before they can reach the desktop. Supports Exchange server cluster. Available for platforms Solaris SPARC, OS/2, AIX, S/390, AS 400, Win NT/2000.

**Server Protect**: Protect the OS, hard disk data corruption by viruses of your LAN servers, application servers.

Available for platforms Win NT/2000, Novell Netware, Red Hat Linux

**Office Scan Corporate Edition**: Customizable client deployment, company wide policy setting, central virus reporting, and remote management features. For desktop virus scanning on Windows OS such as Win NT/2000, XP, 95,98

**Trend Virus Control System**: Centralized console to monitor configure and update the various antivirus components from a single point.

In addition to the Neat Suite bundle of products, Trend Micro offers various other antivirus products including plug-in modules for spam blocking and content filtering, harmful applet blocking.

DIAGRAM ON TREND UNIVERSE[19]


Viruses and Trojans have caused havoc around the world not to mention the financial losses in billions of dollars. Unless we keep our antivirus current and updated with the latest virus detection pattern files we could possibly be subjected to an attack that may compromise our security dimensions pertaining to confidentiality, integrity and availability. We know the following classic examples[20]:

- where the Melissa virus in March 1999 infected desktop systems running Microsoft's outlook e-mail client. The virus replicated itself by going through the Outlook address book and sending itself to the first 50 outlook addresses.
- W32.Sircam had succeeded in causing an availability attack because it deleted files, an integrity attack by copying malicious code to various locations on the hard drive and the confidentiality attack by mailing random files from the user's machine to various other machines.

Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity. An antivirus is the minimum and yet very necessary component in our approach to defense in depth. Lets take a look at the next important technology for protection.

**Firewall**

**Stonegate** (www.stonesoft.com)

3rd Generation firewall with inbuilt High Availability and Load Balancing.

The loss of a critical network component can mean millions in lost revenue, operational inefficiencies, or lost credibility in the market- place. Stonesoft

[19] Trend Micro Inc

[20] SANS Security Essentials Day 2,Threat and the need for Defense in Depth, p 13-15.

provides the solution for 7x24-network connectivity with the StoneGate High Availability Firewall and VPN.
StoneGate provides the first fully scalable, high security and high performance firewall and VPN solution for business critical applications. StoneGate is the first firewall to provide secure connections and load balancing between multiple ISPs to ensure continuous network connectivity. Some distinguishing features are:

Embedded Firewall Operating System
StoneGate is built on a hardened, streamlined Linux OS eliminating the vulnerabilities often found in firewalls based on off-the-self operating systems.

Multi-Layer inspection
StoneGate's Multi-Layer inspection technology combines the best aspects of both stateful inspection technology and application-level Proxy technology.

The cornerstone of StoneGate is maximum security. It is based on Stonesoft's Multi-Layer Inspection; a firewall technology that is based on the best aspects of stateful inspection and application-level proxy technologies. Multi-Layer Inspection provides security on several communication layers, including the application level.

Firewall Clustering
Firewall Clustering provides for Load Balancing and Fault Tolerance in the firewalls. In addition to Load Balancing and Fault Tolerance clustering offers scalability and enables online maintenance.
StoneGate has dynamic Load Balancing between the firewall nodes for maximized firewall throughput. The Load Balancing is fully transparent to the end users. StoneGate also has Fault Tolerance: if a firewall node fails, the other nodes in the cluster automatically take over the tasks of the failed node without the end users noticing anything.
Clustering enables adding new firewall nodes to a cluster on the fly to increase firewall performance. It also enables online maintenance: a firewall node can be taken offline during normal business hours e.g. for hardware or software upgrade.

Server Load Balancing
StoneGate features Server Load Balancing for e.g. web servers and FTP servers protected by StoneGate.
StoneGate Security Gateways run on standard Intel-based hardware with operating system embedded in StoneGate. Either standard multi-purpose computers or Linux-based appliances can be used. Running the StoneGate Security Gateways on Linux enables the use of a wide range of hardware platforms.
The Management System runs on Windows NT, Windows 2000, Linux and Solaris

Hardware requirements consist of two servers one for the Engine, the other for the Maintenance and Log Server.

A firewall has become a necessity for networks connected to the Internet and play a big role in controlling and monitoring access to your network. Both incoming and outgoing traffic should be monitored. Since a compromised system within your network can be used for a denial of service attack without your knowledge. Using NAT (Network Address Translation) is an effective way to shield your host systems from the Internet and unwanted attention. A firewall is the primary protection point for your network and therefore has to be tightly configured and the logs periodically reviewed to understand traffic flow and detect any attack attempts. The firewall will give you a fair idea of intrusions to your network. However an intrusion detection tool/s with their various attack detection signatures is what will actually tell you in depth is happening in and around your network and block or kill the attacking connection.

**Intrusion Detection**
**Internet Security Systems** (www.iss.net)
ISS offers real time (Sensors) and non-real time (Scanners) tools for threat management and vulnerability assessment of the network infrastructure. The tools help to prevent threats and misuse relating to unauthorized network access, probing attempts, denial of service and DDOS, service exploits (DNS, FTP etc), backdoors (Back Orifice 2000) and such.
An analogy of a Sensor would be a video camera which monitors activity as to who comes in and goes out of a building in real time, while that of a Scanner would be a watchman going around a building and reporting which doors, windows were not secured. We will briefly discuss the various sensors and scanners.

ISS provides following types of sensors
Network Sensor
Server Sensor

**Network Sensor**
Provides for real time intrusion protection and response by monitoring network traffic and comparing against attack signatures. If an attack is detected it can log the event, block or kill the connection and inform the administrator by an SNMP alert or email. The console is called site protector and the alerts can be correlated with the known vulnerabilities found running the scanner and thus a filtered, more meaningful alert stream is achieved.

**Server Sensor**
Provides real time monitoring, detecting and response to inappropriate activity and analyzes network packets to and fro from a critical server. Malicious packets can be blocked, the account suspended and the entire event will be logged and

an alert sent to the administrator. As with network sensor it can correlate the alerts with the vulnerabilities found by the scanner to filter the false positives.
It has the ability to monitor SSL encrypted traffic in addition to IPSEC and SKIP encryption. RealSecure Server Sensor is capable of detecting attacks that have been encapsulated within an SSL session.

The sensors can run on a **switched** network by a strategic deployment method. A close look would reveal strategic locations where a switch can be placed that would provide excellent security coverage. If one switched port were connected to a router that connected to the Internet, then it would make sense to insert a small hub between the router and the switch and connect a RealSecure engine at that point. That would provide protection against attacks coming in from the Internet, regardless of what else was on the network.

The RealSecure sensors operate on the following types of networks.
Ethernet networks (10 Mbps)
Fast Ethernet networks (100Base-T only, 100 Mbps),
FDDI (100 Mbps),
Token Ring networks (4 Mbps to 16 Mbps) on NT only

To assess vulnerabilities in your network infrastructure, ISS offers Scanners. The scans provide a detailed description of vulnerabilities found and classify them according to High, Medium and Low risk status. A corrective action is also suggested to seal the identified gap. It's an ongoing process where you monitor and respond in a continuous cycle to reach the optimum desired security level. Default policy templates are available to perform a scan and also the option to customize on a blank policy template to suit your requirements.

ISS offers tools that provide information on the vulnerabilities in non real time. They have 3 types of scanners for vulnerability assessment:

System Scanner
Internet Scanner
Database Scanner

**System Scanner**
Host based tool to detect security vulnerabilities, misconfigurations and checks policy compliance. The administrator can create system security baselines for users, groups, shares, services and critical system files.

**Internet scanner**
Network based vulnerability assessment tool that is able to scan any network device with an IP address. This includes routers, printers, PC's, firewalls, workstations, etc. The administrator can create a hosts file to specify which

devices need be scanned and exclude others as required. Even though the network may have access control in place by way of a firewall and rules it is recommended to use the Internet scanner to scan the firewall itself for misconfigurations. The network can be scanned both from outside and inside the firewall by using Internet scanner.

**Database Scanner**

Databases are powerful and complex tools that help run e-Business applications effectively and store vital data. However relational databases can be directly accessed by client applications and admin utilities without much thought to the security of the operating system on the host where they reside.

The database scanner is used to detect security exposures in leading database applications. It scans for vulnerabilities in SQL, Sybase and Oracle database. Database Scanner detects weak passwords, checks password expiration, detects login attacks, disables old unused accounts, and tracks login hour restrictions. Database Scanner offers security policy generation and reporting functionality, which instantly measures policy compliance and automates the process of securing critical online business data.

We have seen the various intrusion detection tools and vulnerability assessment solutions available to learn, secure, and tighten the protection around our network. These tools play a significant role by enabling us to take a proactive approach to the security threats we face nowadays. Lets see how Authentication fits our need and approach to defense in depth.

**Authentication**

**RSA Security** (www.rsasecurity.com)

Strong authentication is a must for remote access to corporate network by employees, partners or customers. Whether they need access to RAS, VPN, e-mail, web server or other corporate resource a strong two-factor authentication will ensure only authorized people gain entry to your network. In the case of a corporate VPN, though the tunnel is encrypted the identity of the person at the other end may be questionable. A strong authentication mechanism such as SecureID ensures only authorized persons gain access to designated resources.

Two-factor authentication consists of what you have (e.g. an ATM bank card) and what you know (your PIN code). In our case it is an Authenticator commonly known as key fob.

Each key fob has a unique symmetric key combined with a powerful algorithm that generates a 6 digit code every 60 seconds. This code is random and dynamic and hence extremely difficult to guess at any given point in time.

The components involved in the two-factor authentication setup are few and consist of ACE agents, ACE Server and the key fobs.

**ACE Agents**

RSA ACE/Agents function much like security guards, standing between the user and a protected resource or device to enforce two-factor authentication via using RSA ACE/Server software.

**ACE Server**
It is the management component of the RSA SecurID solution, used to verify authentication requests and centrally administer authentication policies for enterprise networks. The ACE server maintains a record of all the ACE agents and the key fobs.

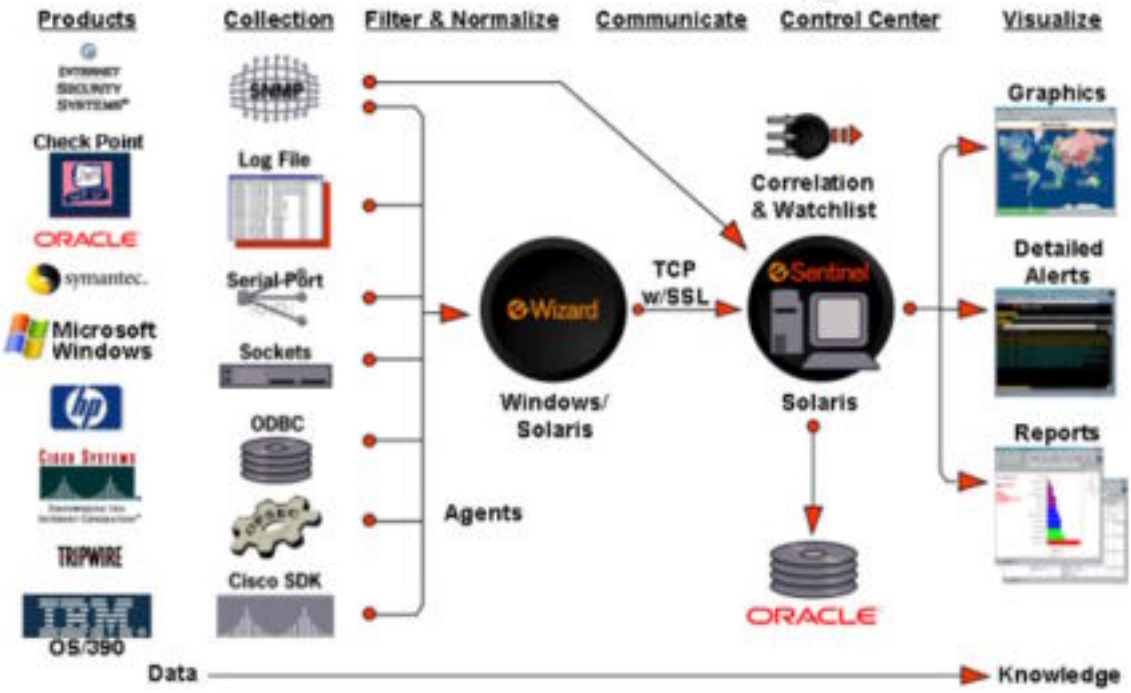
**Key Fob**
This is a hardware token, which is used by the user along with a PIN while accessing corporate resources.

A brief mention at this juncture on Authorization is necessary. With e-Business vast business opportunities open up for creating new revenues and cutting costs. Business processes are put on the web where they can be accessed by employees, partners and customers. This is where the organization has to do a delicate balance between enabling users to achieve their business objectives and providing the necessary security for these resources exposed to the Web. Authorization establishes and enforces policies that control user privileges.

We started by the simplest yet most needed protection in the form of an antivirus and moved on to successive protection layers of firewall, intrusion detection, and authentication. Now we take a look at a technology that will help make our job of understanding and responding to all this heterogeneous, complex information consisting of logs, reports, alerts etc easier and better.

**Threat Management**
**e-Security** (www.esecurityinc.com)
These days Corporates invest a significant amount of money in security hardware and software such as firewalls, intrusion detection systems, antivirus products and more. Mostly these come from different vendors. These products have very little integrated functionality and inter-communication and though they provide vast amounts of information, it is practically impossible to monitor and meaningfully analyze this data in real time with the few resources that IT departments have these days. Most network and system administrators are handling the corporate network security portfolio along with their regular job descriptions. It is not uncommon to see organizations spend thousands of dollars beefing up information security by buying technologies and yet subjected to damaging attacks to their information assets. Having only policies and security devices is not enough but you need to properly manage and monitor the heterogeneous security technologies to derive the optimum benefit of these.

To address this concern an emerging category of security software has been developed called Real time threat Management. **e-Security Inc** offers such tools for real time threat management.
e-Security's products gather information from all existing heterogeneous security products and filter, centralize, prioritize event information, in real time enabling security teams to respond to threats effectively. Real-time threat management systems contain two primary elements: agents and a manager.
Agents are applications that access, filter, acquire, and transform audit log information from the security devices and applications distributed throughout the network to the manager. Lets look at the different components provided by e-Security of this technology. The below diagram[21] will illustrate this concept.



e-Sentinel™ 1

The manager, part is called **e-Sentinel** and is the software process that monitors the security agents to determine and report on the status of security devices. e-Sentinel provides a powerful central processor and database that links to various security point sources through rule-based e-Security Agents. The data is collected from various sources such as SNMP, log files, OPSEC, Cisco SDK, sockets, serial ports. Information is communicated to the console via industry standard secure messaging protocols.

[21] e-Security Inc

Another element is the **e-Wizard** which is a Windows drag-and-drop GUI with tools for creating rule-based e-Sentinel agents that enable fast integration of the heterogeneous products into the e-Sentinel centralized security monitoring environment These agents use the standardized SNMP protocol to link multi-vendor security products with e-Sentinel for monitoring and responding to security events in distributed security systems.

**Agent** connects an IT asset to e-Sentinel. Agents collect and parse security data from the heterogeneous devices and are also responsible for normalization of this security data. This is crucial for event correlation and accurate reporting.

e-Sentinel administration and configuration applications have various tools that allow security personnel to use the reporting tool of their choice to create customized reports.
Scene Builder- that creates graphical representations of scenes that depicts the security network.
Text Alerts -provides the ability to view and interface with textual alert messages using color-coded alert lists.
Log Reviewer- is a report generation tool that allows security analysts to view network statistical data and historical alert data.
e-Reporter- is a Web-based reporting framework.

**e-Sentinel Security Operations Console**
The e-Sentinel Security Operations Console offers, through its menu, an efficient method to start and stop e-Sentinel operations applications. Users simply select the desired application from a single pull-down menu. Applications can be started or stopped with the click of the mouse. Alternatively, applications may be accessed and controlled using command-line entries.

## Conclusion

We have discussed the components of a risk assessment had a look at the deliverables and understood the necessity of a standards based Gap Analysis. We've highlighted the various options for DRP and explored further, on a high level only to see what BCP for the IT operations center would involve. We sum up with a brief discussion into the various technologies available in the market today to assess, deploy, monitor and manage the security threats to our information assets.

The risk assessment process will facilitate and enable the organizations business objectives, provide managers with necessary information on the critical departmental business processes so as to focus their resources on the primary objectives. Designing and implementing security into an organization's business processes can enable business strategies that would otherwise be too risky or technically infeasible.

The subsequent information obtained from such an assessment will assist and back up the action required whether it be implementing policies and procedures or products/technology.This will also help to prevent and reduce loss, rather than cleaning up after the damage has been done.This ensures a proactive approach to addressing risks.

## References


1. Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas, "Contingency Planning Guide for Information Technology Systems", SP 800-34, NIST Technology Administration, US Department of Commerce, June 2002. URL:
http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

2.Jack L. Brock, Jr, " Information Security Risk Assessment -Practices of Leading Organizations", United States General Accounting Office, Accounting and Information Management Division, November 1999.URL:
http://www.gao.gov./special.pubs/ai00033.pdf

3.KPMG, Treasury Board of Canada Secretariat, Best Practices in Risk Management: Private and Public Sectors Internationally.URL:
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rm-pps1_e.html#_Toc456660315

4.Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems", SP 800-30, NIST Technology Administration, US Department of Commerce, October 2001.URL:
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

5.Charl Van der Walt, "Assessing Internet Security Risk, Part One: What is Risk Assessment?" June 11, 2002, Security Focus Online. URL:
http://online.securityfocus.com/infocus/1591

6.Information Resources and Technology Security Office, "Business Impact Analysis/Risk Assessment for Information Assets", Virginia Tech, December 2000. URL:
http://www.security.vt.edu/playitsafe/riskanalysis/RA-Dept01-Inst.doc

7.Ron La Pedis, "Ensuring survival", Business Continuity Planning Strategy Brief. URL:
http://www.cert.org/research/isw/isw2001/papers/LaPedis-supporting-02-08.pdf

8.Jeffrey H. Wold, "Disaster Recovery Planning Process", Disaster Recovery Journal. URL: http://www.drj.com/new2dr/w2_002.htm

9.Electronic Vault, Data Shadowing and Replication, Flowlogic. URL: http://www.flowlogic.com/solutions_document.html

10."Gap Analysis" Department of Information Technology, Ministry of Communications and Information Technology, India. URL: http://www.mit.gov.in/stqcit/Gapanalysis.htm

11. The ISO 17799 Made Easy.URL: http://www.iso17799-made-easy.com/

12.ISO 17799 Security World. URL: http://www.iso-17799-security-world.co.uk/what.htm

13.Fred Cohen and Associates, Summary of Controls Used in BS 7799 http://all.net/books/audit/bs7799.html

14.Jerry Isaacson, "MIT BUSINESS CONTINUITY PLAN", Massachusetts Institute of Technology, Copyright 1995 http://web.mit.edu/security/www/pubplan.htm

15. DRI International, Professional practices for Business Continuity Planners http://www.dr.org/ppcont.htm

16.Visor Consultants Ltd, "Business Continuity management-Preventing Chaos in a Crisis", BC Planning Guides, The Business Continuity Institute. URL: http://www.thebci.org/frametrial.html

17.The Institute of Internal Auditors http://www.theiia.org/

18.Trend Micro http://www.trendmicro.com/download/datasheets/

19.Stonesoft http://www.stonesoft.com/products/literature/StoneGate

20.Internet Security systems http://www.iss.net/products_services/enterprise_protection/

21.RSA Security http://www.rsasecurity.com/products/securid/index.html

22.e-Security: The Leading provider of Real Time Threat Management Software http://www.esecurityinc.com/products/main.asp

23.SANS Security Essentials Curriculum, Day 2,"Threat and the Need for Defense in Depth", p 1-3,1-13,1-14,1-15.

24.Timothy Stacey, "Toward Standardization of Information Security: BS 7799", SANS Information security reading Room. URL: http://rr.sans.org/policy/standardization.php

Last Updated: May 23rd, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| 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 |